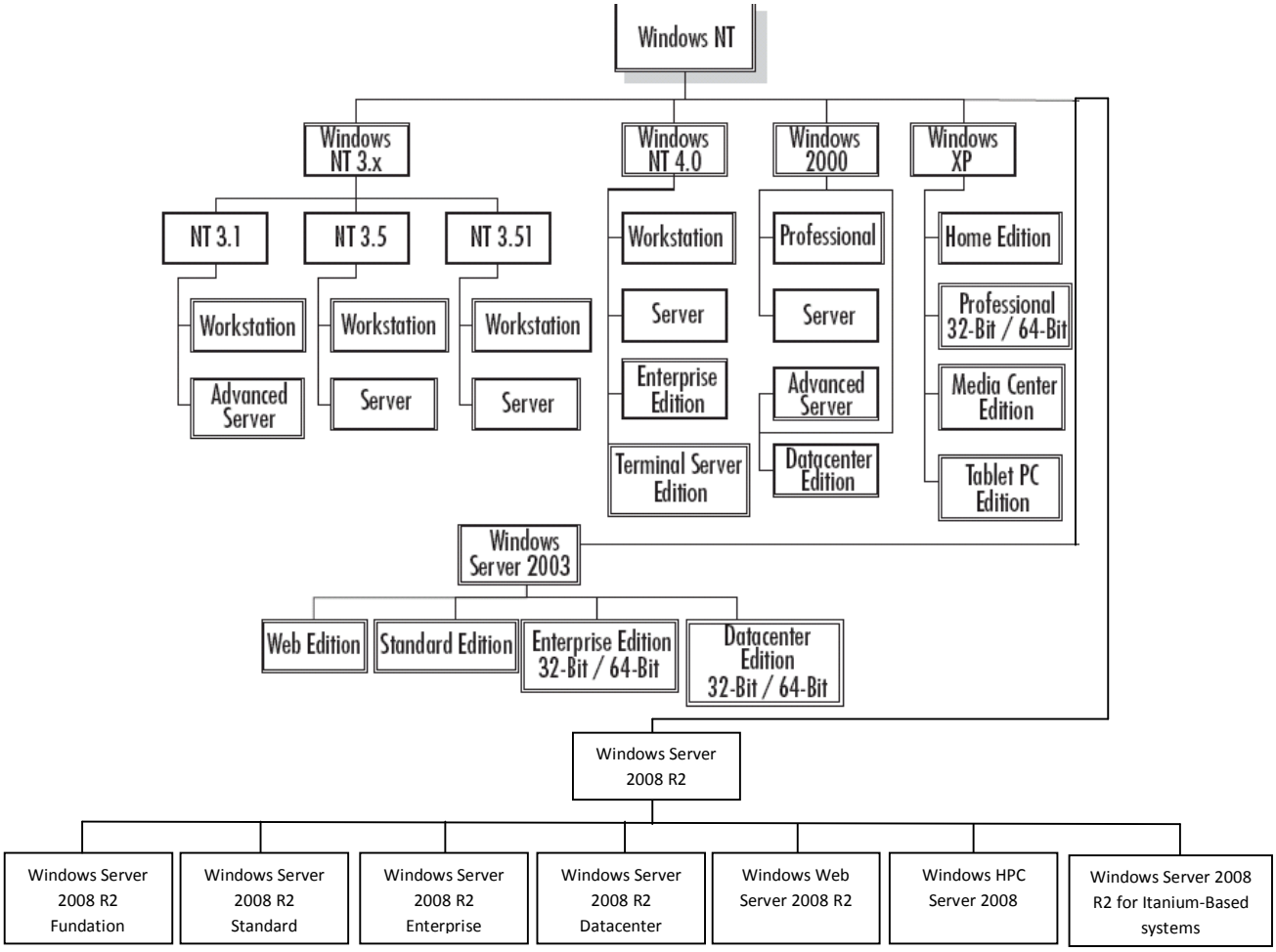
Tartalom

1. Windows Server 2008 R2 áttekintése

A történeti alapok:

- A Microsoft 1980-ban kezdett operációsrendszert gyártani először.
- DOS alapú rendszerek
    a. Kezdetben az operációsrendszerek MS DOS alapú rendszerek voltak. Erre az alapra fejlesztettek egy GUI-t: Graphical User Interface. (felhasználó barát, multi task üzemmód)
    b. Kezdetben verziószámok alapján nevezték el a termékeket (1.0, 1.1), a későbbiekben, pedig az évjárat alapján.
    c. Az utolsó DOS alapú fejlesztés a ME volt.
- NT alapú rendszerek
    a. Egy új operációsrendszer kifejlesztésén az IBM és a Microsoft együtt dolgozott és létrehozták az OS2-t.
    b. Majd a Microsoft „kiszállt" ebből a fejlesztésből és létrehoztak egy új 32 bites operációs rendszert a WIN NT-t.
    c. Ez az operációs rendszer alkalmas először domain létrehozására, központi erőforrás kezelésre.
    d. Létezik kliens és szerver verziója is.



Windows Server 2008 R2 termékismertető

A Windows Server 2008 R2 kiadása a díjnyertes Windows Server 2008 alapjaira épül, és a létező technológiák továbbfejlesztése mellett olyan új funkciókat kínál, amelyek révén az informatikai szakemberek növelhetik kiszolgálói infrastruktúrájuk megbízhatóságát és rugalmasságát. Az új virtualizációs eszközöknek, webes erőforrásoknak, a kezelhetőség terén megvalósított fejlesztéseknek és a Windows 7 rendszerrel való integrációnak köszönhetően időt és pénzt takaríthat meg, továbbá megfelelő platformot biztosíthat a dinamikus, hatékonyan felügyelt adatközpontok számára. A hatékony eszközök – egyebek között az Internet Information Services (IIS) 7.5-ös verziója, a frissített Kiszolgálókezelő és Hyper-V platform, valamint a Windows PowerShell 2.0-s verziója – együttesen nagyobb fokú felügyeletet és megnövelt hatékonyságot biztosítanak az ügyfelek számára, továbbá lehetővé teszik, hogy minden korábbinál gyorsabban reagáljanak a vállalatuk tevékenységével kapcsolatos üzleti igényekre.

Továbbfejlesztett webalkalmazási platform

A Windows Server 2008 R2 számos olyan fejlesztést tartalmaz, amelyek együtt a Windows Server e kiadását a legszilárdabb webalkalmazási platformmá teszik. A megújult webkiszolgálói szerepkör mellett a rendszer tartalmazza az Internet Information Services (IIS) 7.5-ös verzióját, és a korábbinál szélesebb körben támogatja a .NET-keretrendszer használatát Server Core konfigurációban. Az IIS 7.5 kialakításakor azok a fejlesztések kerültek előtérbe, amelyek révén a webes rendszergazdák könnyebben üzembe helyezhetik és felügyelhetik a webalkalmazásokat, és amelyek fokozott megbízhatóságot és méretezhetőséget biztosítanak. Az IIS 7.5 emellett korszerűbb, egyszerűbben használható felügyeleti funkciókat nyújt, és több lehetőséget kínál a webkiszolgálói környezet testreszabására. Az IIS és a Windows webplatform alábbi fejlesztései érhetők el a Windows Server 2008 R2 rendszerben:

- A webalapú alkalmazások egyszerűbb felügyelete és támogatása
- Egyszerűbb terméktámogatás és hibaelhárítás
- Továbbfejlesztett fájlátviteli szolgáltatások
- Lehetőség a funkciók és szolgáltatások bővítésére
- A .NET-keretrendszer tökéletesebb támogatása
- Biztonságosabb alkalmazáskészletek
- IIS.NET közösségi portál

Méretezhetőség és megbízhatóság

A Windows Server 2008 R2 minden eddiginél jelentősebb munkaterhelések ellátására alkalmas, továbbá dinamikus méretezhetőséget és minden téren magasabb fokú rendelkezésre állást és megbízhatóságot biztosít. A rendszer számos új és továbbfejlesztett jellemzőt kínál, ilyen például a korszerű processzorarchitektúrák jobb kihasználása, az operációs rendszer összetevőkre bontásának magasabb foka, valamint az alkalmazások és szolgáltatások nagyobb teljesítménye és méretezhetősége.

- Korszerű processzorarchitektúrák jobb kihasználása
- Az operációs rendszer összetevőkre bontásának magasabb foka
- Az alkalmazások és szolgáltatások nagyobb teljesítménye és méretezhetősége
- Továbbfejlesztett tárolási megoldások
- A belső hálózati erőforrások tökéletesített védelme

Továbbfejlesztett energiagazdálkodás és egyszerűsített felügyelet

Napjainkban egy adatközpont kiszolgálóinak folyamatos kezelése és felügyelete az informatikai szakemberek egyik legtöbb időt igénylő feladata. Bármely rendszerbe állított felügyeleti stratégiának támogatnia kell mind a fizikai, mind a virtuális környezetek kezelését és felügyeletét. Az ezzel kapcsolatos problémák megoldása érdekében a Windows Server 2008 R2 egyes új szolgáltatásai csökkentik a Windows Server 2008 R2 folyamatos felügyeleti igényét és a mindennapos üzemeltetési feladatokkal járó adminisztratív teendők számát. E szolgáltatások közé tartoznak az alábbiak:

- Az adatközpontok energiafogyasztásának továbbfejlesztett kezelése
- A fájlszolgáltatások továbbfejlesztett kezelése
- Továbbfejlesztett távoli felügyelet
- Kisebb adminisztrációs igényű, interaktív módon elvégezhető adminisztratív feladatok
- Bővített parancssor és automatizált felügyelet a PowerShell 2.0-s verziója révén
- Tökéletesített identitáskezelés
- Az elterjedt szabványoknak és gyakorlati eljárásoknak való nagyobb fokú megfelelés

Lehetőségek a kiszolgáló és a munkaállomás virtualizációjára

Napjaink adatközpontjaiban igen fontos szerep jut a virtualizációnak. A virtualizáció révén lehetővé váló hatékonyabb üzemeltetésnek köszönhetően a szervezetek jelentősen csökkenthetik működési költségeiket és energiafogyasztásukat. A Windows Server 2008 R2 a következő típusú virtualizációs lehetőségeket kínálja: ügyfél kiszolgáló virtualizációt a Hyper-V platform révén, valamint megjelenítési virtualizációt a Távoli asztali szolgáltatások révén.

- **Hyper-V**: A Windows Server 2008 R2 rendszerben bemutatkozik a Hyper-V platform új verziója. A Windows Server 2008 R2 részét képező Hyper-V platformot több kulcsterületen is továbbfejlesztették a dinamikus, virtuális adatközpontok létrehozása érdekében, így nagyobb rendelkezésre állást és teljesítményt biztosít, tökéletesített felügyeleti és egyszerűsített rendszerbe állítási eljárásokat kínál, és új szolgáltatásokat is tartalmaz, ilyen például a működés közbeni, élő áttelepítés.
- **Távoli asztali szolgáltatások** (korábbi nevükön Terminálszolgáltatások): A Távoli asztali szolgáltatások biztosítják azt a funkciókészletet és rugalmasságot a felhasználók és a rendszergazdák számára, amely nélkülözhetetlen a tetszőleges telepítési környezetben elérhető, robusztus hozzáférési élmény megvalósításához. A Távoli asztali szolgáltatások funkciókészletének bővítése érdekében a Microsoft jelentős beruházásokat tett a virtuális munkaállomás-infrastruktúra (Virtual Desktop Infrastructure – VDI) terén. A VDI egy olyan központosított munkaállomás-szolgáltató architektúra, amely lehetővé teszi a Windows és más munkaállomás-környezetek futtatását és felügyeletét a központi kiszolgálón található virtuális gépeken.

Nagyobb felhasználói élmény a Windows 7 rendszerrel együtt

A Windows Server 2008 R2 számos olyan funkcióval rendelkezik, amely kifejezetten a Windows 7 rendszert futtató ügyfélgépekkel való együttműködéshez készült. A Windows 7 a Microsoft ügyfélgépekre szánt Windows operációs rendszerének legújabb verziója. Az alábbi lista néhány olyan szolgáltatást tartalmaz, amely csak akkor érhető el, ha a Windows Server 2008 R2 rendszert futtató kiszolgálókat Windows 7 rendszerrel működő ügyfélgépekkel használják:

- Vállalati számítógépek egyszerűbb távoli csatlakoztatása a DirectAccess funkció használatával
- Személyes és nyilvános számítógépek biztonságos távoli csatlakoztatása
- Nagyobb teljesítmény a fiókirodák számára
- Továbbfejlesztett biztonsági szolgáltatások a fiókirodák számára
- Továbbfejlesztett virtualizált munkaasztali integráció
- A telephelyek közötti összeköttetések nagyobb hibatűrése

Windows Server 2008 R2 termékcsalád bemutatása

A Windows Server 2008 R2 mindegyik kiadása kulcsfontosságú funkciókat tartalmaz tetszőleges méretű vállalatok számára az üzleti és informatikai kihívások leküzdéséhez. A megfelelő emblémára vagy hivatkozásra kattintva részletesen olvashat az egyes kiadásokról.

A Windows Server 2008 R2 Foundation gazdaságos, belépő szintű technológiát kínál elsősorban kisvállalatok tulajdonosai és kisvállalatok támogatásával foglalkozó informatikusok számára. A Foundation kiadás egy költségkímélő, egyszerűen telepíthető, bevált és megbízható technológiai csomag, amely biztosítja a szervezetek számára a leggyakoribb üzleti alkalmazások futtatásához, valamint az információ és az erőforrások megosztásához szükséges alapokat.

A Windows Server 2008 R2 Standard a valaha megjelent legrobusztusabb Windows Server operációs rendszer, amely továbbfejlesztett beépített webes és virtualizációs szolgáltatásai révén fokozza a kiszolgálói infrastruktúra megbízhatóságát és rugalmasságát, ugyanakkor segít az időráfordítás és a költségek csökkentésében. A rendszer hatékony eszközei segítségével a kiszolgálók fokozottabban ellenőrizhetők, a konfigurációs és felügyeleti feladatok pedig egyszerűbben elláthatók. A továbbfejlesztett biztonsági funkciók emellett fokozzák az operációs rendszer szilárdságát, ami nemcsak az adatok és a hálózat védelmét segíti elő, hanem szilárd, rendkívül megbízható alapot biztosít a vállalat működése számára.

A Windows Server 2008 R2 Enterprise egy korszerű kiszolgálói platform, amely gazdaságosabb és megbízhatóbb támogatást nyújt az üzletmenet szempontjából létfontosságú feladatok ellátásához. Innovatív szolgáltatásokat kínál a virtualizáció, az energiatakarékosság és a felügyelet terén, és egyszerűbbé teszi a mobil munkatársak számára a vállalati erőforrások elérését.

A Windows Server 2008 R2 Datacenter nagyvállalati kategóriájú platformot biztosít az üzletmenet szempontjából létfontosságú alkalmazások rendszerbe állításához és a nagyarányú virtualizációhoz kisebb és nagyobb kiszolgálókon egyaránt. Javítja a rendelkezésre állást, továbbfejlesztett energiagazdálkodási lehetőségeket kínál, és a mobil és fiókirodai alkalmazottak munkáját segítő megoldásokat is tartalmaz. A korlátlan virtualizációs licencjogosultságok révén az alkalmazások összevonhatók az infrastrukturális költségek csökkentése érdekében. A rendszer 2, de akár 64 processzorral is üzemeltethető. A Windows Server 2008 R2 Datacenter kiadása megfelelő alapot nyújt a nagyvállalati kategóriájú virtualizációs és vertikálisan méretezett (scale-up) megoldások kiépítéséhez.

Windows Web Server 2008 R2

A Windows Web Server 2008 R2 egy hatékony webalkalmazási és -szolgáltatási platform. Ez az Internet Information Services (IIS) 7.5 rendszert tartalmazó, kifejezetten az internet felé néző kiszolgálóként kialakított kiadás tökéletesített felügyeleti és diagnosztikai eszközökkel segíti az infrastrukturális költségek csökkentését számos népszerű fejlesztési platformmal való használata esetén. Az integrált webkiszolgálói és DNS-kiszolgálói szerepköröknek, valamint a javított megbízhatóságnak és méretezhetőségnek köszönhetően ez a platform lehetővé teszi a legnagyobb kihívást jelentő környezetek kezelését is, legyen szó akár egy dedikált webkiszolgálóról, akár egy teljes webkiszolgálói farmról.

Windows HPC Server 2008

A nagy teljesítményű számítástechnika (HPC) következő generációját jelentő Windows HPC Server 2008 nagyvállalati kategóriájú eszközöket kínál a kiemelkedően hatékony HPC-környezetek megvalósításához. A Windows HPC Server 2008 akár több ezer processzormagra is hatékonyan méretezhető, és a rendszer állapotának és stabilitásának proaktív megfigyelésére és fenntartására szolgáló felügyeleti konzolokat is tartalmaz. A feladatütemezés terén megvalósított együttműködő-képesség és rugalmasság lehetővé teszi a Windows és a Linux rendszerű HPC-platformok integrációját, továbbá biztosítja a kötegelt és a szolgáltatásorientált alkalmazási (SOA) jellegű munkaterhelések támogatását.

Windows Server 2008 R2 for Itanium-Based Systems

Az Itanium-alapú rendszerekhez készült Windows Server 2008 R2 nagyvállalati kategóriájú platformot biztosít az üzletmenet szempontjából létfontosságú alkalmazások rendszerbe állításához. Méretezési adatbázis, üzleti és egyéni alkalmazások szolgálják a növekvő üzleti igények kielégítését. A magas rendelkezésre állást segítik a feladatátvételi fürtszolgáltatások (failover clustering) és a dinamikus hardverparticionálási lehetőségek.* A Windows Server korlátlan számú virtuális példányának futtatására feljogosító licenceknek köszönhetően a rendszerek virtualizáltan is üzembe helyezhetők.** Az Itanium-alapú rendszerekhez készült Windows Server 2008 R2 biztosítja az alapokat a kiemelkedően dinamikus informatikai infrastruktúrák számára.

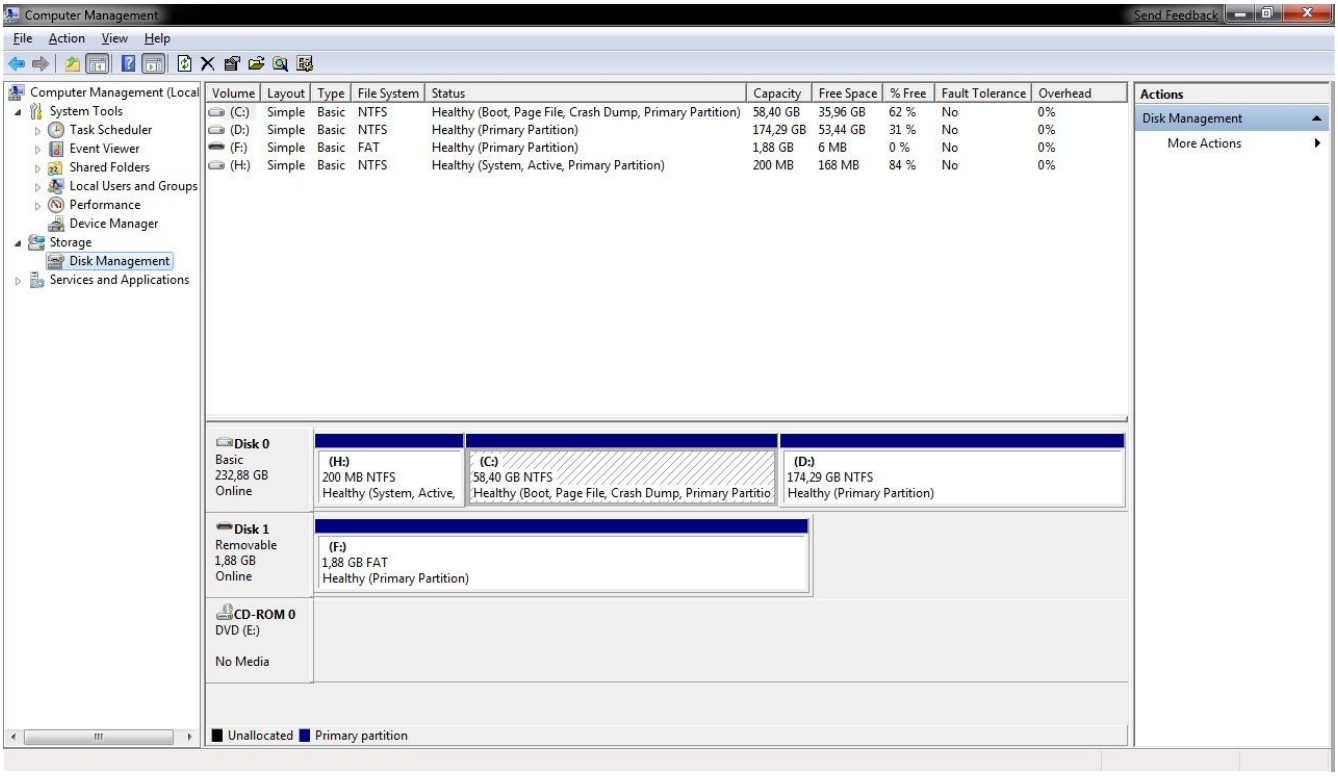
*A szolgáltatást támogató kiszolgálói hardver szükséges hozzá.

**Harmadik fél által biztosított virtualizációs technológia szükséges hozzá. A Hyper-V platform nem érhető el Itanium-alapú rendszerekhez.

Technologies	Windows Server 2008 Web	Windows Server 2008 Standard	Windows Server 2008 Enterprise	Windows Server 2008 Datacenter	For Itanium-based Systems
Sockets – x86	4	4	8	32	●
Sockets – x64	4	4	8	64	●
Sockets – IA64	●	●	●	●	64
RAM – 32-bit OS	4 GB	4 GB	64 GB	64 GB	●
RAM – 64-bit OS	32 GB	32GB	2TB	2TB	2 TB
Hot Add Memory	●	●	●	✓	✓
Hot Replace Memory	●	●	✓	✓	✓
Hot Add/Replace Processor	●	●	✓	✓	✓
Node Failover Clustering	●	●	16	16	8
Fault Tolerance Memory Synchronization	●	●	✓	✓	✓
Cross-file RDC	●	●	✓	✓	●
Network Access Service Connections (RRAS)	50	250	Unlimited	Unlimited	2
Network Access Service Connections (IAS)	●	50	Unlimited	Unlimited	●
Terminal Server Connections	250	250	65,535	65,535	2
Advanced Identity Management Features	●	●	✓	✓	●
ADFS Server	●	●	✓	✓	●
Advanced Certificate Services	●	●	✓	✓	●
Certificate Authority Web Proxy	●	●	✓	✓	●
Network Device Enrollment Service	●	●	✓	✓	●
Online Responder Service	●	●	✓	✓	●
Media Server	Basic	Basic	Full	Full	●
Virtualization (Viridian)	●	✓	✓	✓	●
Quick Migration	●	●	✓	✓	●
Host Clustering of Virtual Images	●	●	✓	✓	●
Virtual Image Use Rights	Guest	Host + 1 VM	Host + 4 VM	Unlimited	Unlimited

Fontosabb beépített management eszközök

Computer Management



I. SYSTEM TOOLS (RENDSZERESZKÖZÖK)

1. Task Scheduler (Feladat ütemező):

2. Event Viewer (Esemény napló):

Ha probléma van egy rendszerrel, ajánlott először ránézni az Eseménynaplóra, mely könnyen kezelhető, és az egyik leginformatívabb eszköz az NT alapú Windowsokban. Hiba esetén nagy esélye van, hogy naplózva lett az esemény, és utólag talán ez az információ segít a hibakeresésben.

Alkalmazás-napló: a számítógépre telepített alkalmazásokkal kapcsolatos információkat tekinthetjük meg itt. A programoktól származó üzenetek és hibák ide kerülnek bejegyzésre

Biztonsági-napló: a sikeres és sikertelen események kerülnek ide.

Rendszer-napló: ebben a részben a rendszerrel kapcsolatos vagy által generált eseményeket találhatjuk meg. Pl. beléptetési hiba, valamelyik szolgáltatás nem indult el, esetleg egy-egy hotfix vagy Service Pack telepítése.

Bejegyzések fajtái:

- **Információ**: egy esemény sikeres végrehajtása, pl. egy szolgáltatás elindítása.
- **Figyelmeztetés**: nem túl jelentős, de hibához vezethet.
- **Hiba**: jelentős probléma, mely veszélyes lehet a rendszerre.
- **Sikeres események**: ha a biztonsági naplózás be van kapcsolva, ide kerülnek a sikeres események.
- **Sikertelen események**: ha a biztonsági naplózás be van kapcsolva, ide kerülnek a sikertelen események.

Lehetőség van a bejegyzések szűrésére, hogy csak a minket érdeklő információkat lássuk. Ehhez a megfelelő napló (alkalmazás, biztonsági, rendszer) nevén jobb klikk, majd Tulajdonságok / Szűrő fül. Az öt lehetséges szempontot a neve melletti check-boxban jelölhetjük ki.

Egyéb műveletek:

- Megnyitás
- Mentés
- Export
- Logolás beállítása.
    a. Log fájl méretének beállítása
    b. Logolás módjának beállítása

3. Shared Folders (Megosztott mappák):

- Megosztások / Shares: milyen megosztásaink vannak a szerveren
- Munkamenetek / Sessions: mely userek csatlakoznak a megosztásainkhoz
- Nyitott fájlok / Open Files: mely fájlok vannak megnyitva.

4. Local Users & Groups (Helyi felhasználók és csoportok):

- *Felhasználók* / Users: A számítógépet használó userek felsorolása.
  Installáláskor létrejött felhasználók:
    a. Administrator (enable)
    b. Guest (disable)
    c. Support_xxxxxxxx (disable)
- *Csoportok* / Groups: A felhasználók csoportokba rendezhetők, ami a jogosultság kezelést megkönnyíti.
  Néhány a beépített csoportok közül:
    a. **Administrators:** A rendszergazdáknak teljes és korlátozás nélküli elérésük van a számítógéphez/tartományhoz.
    b. **Backup Operators**: Felhasználók, akik a "Biztonsági másolat" ("Backup") programján keresztül hozzáférhetnek a rendszerfájlokhoz is a mentés ideje alatt. Más esetben nem.
    c. **Guest**: A vendégek hozzáférése alapértelmezés szerint azonos a Felhasználók csoport tagjainak hozzáférésével, kivétel a vendégfiók, amelynek korlátozottabb a hozzáférése.
    d. **Power Users**: A kiemelt felhasználók néhány megszorítással birtokolják a rendszer felügyeleti jogait. Telepíthetnek olyan programokat, amelyek nem módosítják az operációs rendszerhez tartozó fájlokat, és nem telepítenek rendszerszolgáltatásokat.; Testre szabhatják a rendszer közös erőforrásait, például a Nyomtatók, a Dátum és idő, az Energiagazdálkodási lehetőségek beállításait és a Vezérlőpult egyéb erőforrásait.; Létrehozhatnak és kezelhetnek helyi felhasználói fiókokat és csoportokat.; Leállíthatnak és elindíthatnak olyan rendszerszolgáltatásokat, amelyek alapértelmezés szerint nem indulnak el.; Nincs engedélyük ahhoz, hogy felvegyék magukat a Rendszergazdák csoportba, és nem férhetnek hozzá más felhasználók NTFS-köteten levő adataihoz, kivéve, ha ehhez megfelelő jogosultságot kaptak az adott felhasználótól.
    e. **Print Operators**: Kezelhetik a nyomtatók beállításait, illetve hozzáférési jogaikat, de újat nem telepíthetnek.
    f. **Remote Desktop Users**: Ennek a csoportnak a tagjai megkapják a távoli bejelentkezésre vonatkozó engedélyt.
    g. **Users**: A felhasználók sem véletlenül, sem szándékosan nem tudnak a rendszerre kiterjedő változásokat végrehajtani. Futtathatják a hitelesített alkalmazásokat, de a régi típusú alkalmazások többségét nem. A Felhasználók csoport a legbiztonságosabb környezetet biztosítja a programok futtatásához. A felhasználó nem módosíthatja a rendszerleíró adatbázis egész rendszert érintő

beállításait, az operációs rendszerhez tartozó fájlokat vagy a programfájlokat. A felhasználó leállíthatja a munkaállomást, de a kiszolgálót nem. A felhasználó létrehozhat helyi csoportokat, de csak az általa létrehozott helyi csoportokat kezelheti. A felhasználó teljes hozzáféréssel rendelkezik saját adatfájljai eléréséhez (%userprofile%) és a rendszerleíró adatbázis saját részéhez (HKEY_CURRENT_USER). A felhasználó nem telepíthet más felhasználók által is használható programokat (így elkerülhetők a trójai faló programok). Nem férhet hozzá más felhasználó saját adataihoz és Asztal-beállításaihoz sem.

5. **Performance (teljesítmény):**

A Teljesítménynaplók és riasztások eszköz segítségével részletesen megfigyelhető az operációs rendszer erőforrás-hasznosítása.

- *Számlálónaplók* (counter logs): Időközönként adatokat gyűjt, csak nem a képernyőn jeleníti meg, hanem egy naplófájlban rögzíti a merevlemezen, ezzel lehetővé válik hosszabb távú elemzések készítése, kiértékelése. A naplófájlt később fel lehet dolgozni és grafikusan megjeleníteni.
- *Nyomkövetési naplók* (trace logs): A számlálónaplóval ellentétben nem úgy működik, hogy bizonyos időközönként menti a kijelölt számláló állapotát, hanem egy esemény bekövetkezte váltja ki a naplózást.
- *Riasztások* (alerts): Beállítható, hogy bizonyos esemény bekövetkezésekor riasztás „hajtódjon" végre.

6. **Device Manager (Eszközkezelő):**

Lehetővé teszi a telepített hardvereszközök és a hozzájuk kapcsolódó meghajtó programok áttekintését és beállítását.

II. STORAGE (TÁROLÁS)

1. **Disk Management (lemezkezelés):**

A Lemezkezelés rendszer segédprogram a merevlemezek, valamint az azokon található kötetek és partíciók kezelésére szolgál. A Lemezkezelés segédprogrammal lemezeket inicializálhat, köteteket hozhat létre, köteteket formázhat.

III. SERVICES AND APPLICATIONS (SZOLGÁLTATÁSOK ÉS ALKALMAZÁSOK)

A szolgáltatás egy háttérben futó alkalmazási típus. A Szolgáltatások beépülő modul az alábbiakra használható: Szolgáltatások indítása, leállítása, felfüggesztése, folytatása vagy letiltása távoli és helyi számítógépeken. A szolgáltatások indításához, leállításához, felfüggesztéséhez, újraindításához vagy letiltásához rendelkeznie kell a megfelelő engedélyekkel.

A Microsoft Management Console

A Microsoft Management Console (MMC) segítségével felügyeleti eszközök csoportjai, úgynevezett konzolok hozhatók létre, menthetők és nyithatók meg. A konzolok többek között a következőket tartalmazzák: beépülő modulokat, bővítményeket, figyelésvezérlőket, feladatokat, varázslókat, valamint a Windows hardver-, szoftver- és hálózati összetevőinek kezeléséhez szükséges dokumentációt. A meglevő MMC-konzolok további elemekkel egészíthetők ki, vagy új konzol hozható létre és állítható be adott rendszerösszetevő felügyeletéhez.

2. Active Directory, domain

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 2008 R2 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

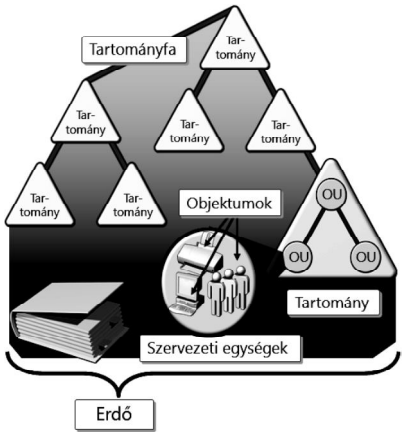
Természetesen ahhoz, hogy kiaknázhassuk az Active Directoryban rejlő lehetőségeket, először be is kell fektetnünk (nemcsak anyagi értelemben), vagyis meg kell szereznünk a hatékony használathoz és üzemeltetéshez nélkülözhetetlen tudást. Minél mélyebben ismeri a rendszergazda az általa üzemeltetett rendszert, 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.



- **Fa** *(Tree)* – Ha az erdő több tartománya összefüggő DNS-tartományneveket 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.

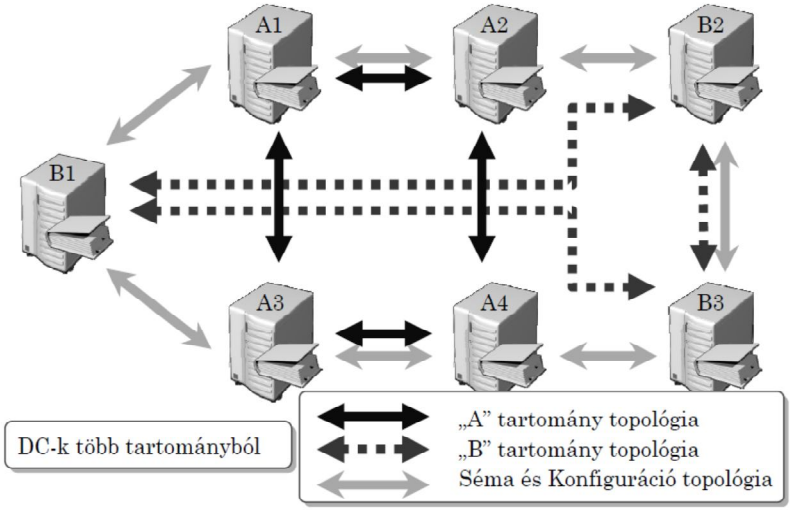
- **Szervezeti egység** *(Organizational Unit, OU)* – A szervezeti egységek az Active Directory-objektumtárolói, amelyekbe felhasználók, csoportok, számítógép-objektumok, illetve más szervezeti egységek helyezhetők. A szervezeti egységek rendkívül fontos szerepet játszanak a csoportházirend érvényesítésével 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.



Replikációs topológia több tartomány esetén

A replikációs topológia

Az összes tartományvezérlőn megtalálható konzisztencia-ellenőrző (Knowledge Consistency Checker, KCC) az Active Directory Sites and Services (Active Directory – helyek és szolgáltatások) beépülő modulban megadott hálózati adatokra alapozva automatikusan létrehozza a leghatékonyabb replikációs topológiát. Bármikor bekerül tehát egy új tartományvezérlő, a KCC a módosítás figyelembevételével újraszámítja a korábban kialakított topológiát (15 perc az időzítése).

A konzisztencia-ellenőrző minden címtárpartícióhoz (séma, konfiguráció, tartomány, alkalmazás) külön replikációs topológiát hoz létre. A konzisztencia-ellenőrző minden tartományvezérlőn kétirányú, gyűrűsreplikációs topológiát alakít ki, vagyis megpróbál legalább két kapcsolatot létrehozni minden tartományvezérlő esetében (a jobb hibatűrést érdekében), a jelentősebb késés elkerülése miatt pedig arra törekszik, hogy két tartományvezérlő között legfeljebb három lépést alakítson ki. A topológia közvetlen kapcsolatokat is tartalmazhat, ha a három lépésnél hosszabb replikációs út elkerülésének érdekében ez szükséges.

Az Active Directoryban a **telephely** (site) olyan számítógépek csoportját jelenti, amelyek között nagy sebességű, megbízható hálózati kapcsolat (jellemzően LAN) van. A telephelyhez tartozó számítógépek általában egy épületben találhatók, vagy közös helyi hálózathoz csatlakoznak. Egy telephelyen belül természetesen több IP-alhálózat is lehet.

Replikáció telephelyen belül

Egy telephelyen belül állandó és nagy sebességű hálózati kapcsolat van a tartományvezérlők között, így itt a KCC a minél gyorsabb szinkronizációt lehetővé tevő topológia kialakítására törekszik. A címtárfrissítések automatikusan mennek végbe, ha a Change Notification Mechanism (változásértesítés) segítségével értesítés érkezik egy változásról. A telephelyek közötti replikációval ellentétben a helyi címtárfrissítések átvitele tömörítetlen formában történik.

Replikáció a telephelyek között

A telephelyek közötti replikáció megvalósítása jelentősen eltér a helyi replikációtól, mivel a telephelyek közötti sávszélesség általában korlátozott, sőt esetleg nincs is állandó kapcsolat. A telephelyek közötti replikáció a sávszélesség minél hatékonyabb kihasználását próbálja elérni; a címtárfrissítések automatikusan mennek végbe egy beállítható ütemezés alapján (alapértelmezés szerint háromóránként). A telephelyek közötti replikációval kapcsolatos adatforgalom alapértelmezés szerint tömörített, a sávszélesség jobb kihasználásának érdekében.

Címtárpartíciók

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

- **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 2008 R2 rendszert futtató tartományvezérlők a fentieken kívül egy vagy több alkalmazás-címtári partíciót is tárolhatnak.

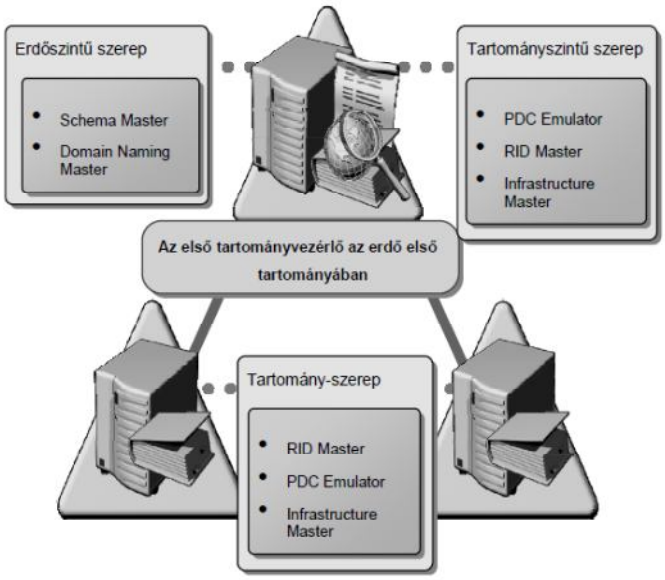
Az egyedi főkiszolgáló-műveletek (FSMO)

A Windows Server 2008 R2 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.



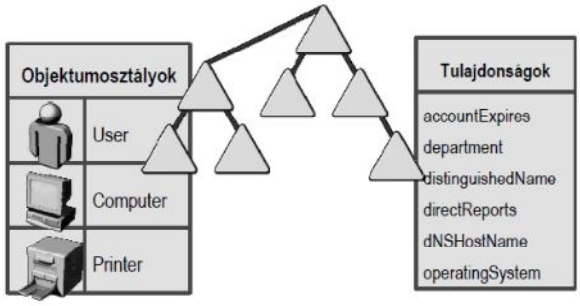
- **Infrastruktúra-főkiszolgáló** *(Infrastructure Master)* – Szintén tartományszintű műveleti főkiszolgáló szerepkör, amelyből szintén egy lehet a tartományon belül, de csak akkor van rá szükség, ha a hálózat több tartományból áll. Feladata a saját tartományának objektumai és a többi tartományban található 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.

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.



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.

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

Működési szint (tartomány)	Támogatott tartományvezérlők	Leírás
Windows 2000 vegyes mód (Windows 2000 mixed mode)	Windows NT Server Windows 2000 Server Windows Server 2003	Vegyes módban Windows NT BDC-ket (Backup Domain Controller) is csatlakoztathatunk a tartományhoz. A címtár legfeljebb 40000 objektumot tartalmazhat.
Windows 2000 natív (Windows 2000 native)	Windows 2000 Server Windows Server 2003 Windows Server 2008 (sémabővítéssel)	Univerzális csoportok; a csoportok típusai változtathatók; egymásba ágyazható csoportok; SID history; RAS házirendek; a méretezési problémák megoldása.
Windows 2003 köztes mód (Windows 2003 interim mode)	Windows NT Server Windows Server 2003	A tartományi köztes mód az erdő első Windows NT tartományának frissítésekor használható, nem automatikus módon. Inkább csak átmenetileg, NT→2003 migrációkor használatos, ha biztosan tudjuk, hogy nem fogunk Windows 2000 tartományvezérlőt használni.
Windows 2003 natív mód (Windows 2003 native mode)	Windows Server 2003 Windows Server 2008 (sémabővítéssel)	Netdom.exe eszköz (tartományvezérlő átnevezése); frissíti, de nem replikálja a LastLogonTime attribútumot; replikálja a nem túl pontos LastLogonTimeStamp-et (mindkettő bejelentkezési időbélyeg); a Users és Computers tárolók átirányítása; az Authorization Manager az AD-ban képes tárolni funkció-alapú házirendjeit; Kerberos Secure Delegation az alkalmazások részére.
Windows 2008 natív mód (Windows 2008 native mode)	Windows Server 2008	Csak olvasható tartományvezérlők (RODC); DFS-R replikáció a SYSVOL megosztás számára – a különbségi replikációs módszerrel magasabb tömörítési hatásfok érhető el; a Kerberos támogatja az AES 128/256 algoritmusokat; Last Interactive Logon Information, mely kijelzi a felhasználó utolsó sikeres interaktív belépésének idejét, az ehhez használt munkaállomást és a sikertelen belépések számát; finomhangolt jelszóházirend (a korábbi verziókban tartományonként, a 2008-tól akár szervezeti egységenként beállítható – de csak felhasználókra, nem számítógépekre vonatkozhat).

Az erdők között kisebb a lehetséges működési szintek száma: Windows 2000 (default), Windows Server 2003 köztes (interim), Windows Server 2003, Windows Server 2008.

Kezelés és eszközök

A következőkben megismerkedünk az Active Directory felügyeleti eszközeivel, sorra vesszük azokat a grafikus felülettel rendelkező eszközöket, amelyekkel elérhetjük a címtárban tárolt objektumokat, illetve megadhatjuk az Active Directory működésével kapcsolatos egyéb paramétereket. A grafikus felülettel felszerelt eszközök mindegyike MMC-konzol, és (majdnem) valamennyit a Start menü Administrative Tools (Felügyeleti eszközök) mappájából indíthatjuk el:

- A leggyakrabban használt konzol **Active Directory Users and Computers** (Active Directory – felhasználók és számítógépek) névre hallgat. Segítségével kezelhetjük a címtár objektumait, felhasználói és számítógépfiókokat, csoportokat, szervezeti egységeket, megosztott mappákat és nyomtatókat hozhatunk létre, illetve beállíthatjuk ezek tulajdonságait. Ugyancsak ezt a konzolt használhatjuk a tartomány szintű egyedi főkiszolgálói-műveleteket (FSMO) végző számítógépek megadására (RID Master, PDC Emulator, Infrastructure Master), a felügyeleti jogok delegálására és a tartomány működési szintjének megváltoztatására is. A felügyeleti jogok delegálása azt jelenti, hogy tetszőleges felhasználónak, vagy biztonsági csoportnak jogosultságot adhatunk bármely Active Directory-tárolón (jellemzően szervezeti egységen) belül meghatározott felügyeleti jogok gyakorlására. A felügyeleti jog jelentheti például a felhasználói fiókok létrehozásának, számítógépfiók hozzáadásának, vagy a csoporttagság módosításának lehetőségét, a jogosultsági kör igen részletesen meghatározható. Ilyen módon, a szervezeten belül „kis" rendszergazdákat hozhatunk létre, akik rendelkeznek a rendszergazda bizonyos jogosultságaival, de ez csak szigorúan meghatározott műveletekre, és az objektumok pontosan meghatározott körére vonatkozik.
- Az **Active Directory Sites and Services** (Active Directory – helyek és szolgáltatások) a telephelyek kialakítására és a tartományvezérlők közötti replikáció beállítására szolgál (lásd később). Ugyancsak ezzel az eszközzel jelölhetjük ki azokat a tartományvezérlőket, amelyek a globális katalógus szerepkört fogják tartalmazni.
- Az **Active Directory Domains and Trusts** (Active Directory-tartományok és bizalmi kapcsolatok) konzol, amint a nevéből sejthető, 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. Ezzel a konzollal lehet továbbá a tartománynévnyilvántartási főkiszolgáló (Domain Naming Master) szerepet megvalósító kiszolgálót kijelölni.
- Az **Active Directory Schema** (Active Directory Séma) beépülő-modul a séma kezelésére szolgál, és ennek segítségével mozgathatjuk másik tartományvezérlőre a Schema Master szerepet is. A szerep új számítógépre való áthelyezésére például az eredeti Schema Master meghibásodáskor, vagy cseréjekor lehet szükség

Active Directory Users and Computers tipikus objektumai

Az Active Directory objektumai két csoportba sorolhatók; a konténer típusú objektumok más konténereket, és levél típusú objektumokat tartalmazhatnak. Konténer típusú objektumok tehát azok, amelyek más objektumokat tartalmazhatnak, ilyen például maga a tartomány, a szervezeti egységek stb. A levél típusú objektumok a hálózat különféle funkcióval rendelkező elemeit reprezentálják, ilyenek például a felhasználói- és számítógépfiókok, vagy a nyomtatók. A következőkben áttekintjük azokat a címtárobjektumokat, amelyeket a telepítés után létre kell hoznunk, hogy az Active Directory szolgáltatásait a felhasználók és a rendszergazdák is hatékonyan vehessék igénybe.

A szervezeti egység

A szervezeti egységek az Active Directory-szolgáltatás tárolói, a tartományok alapegységei. A szervezeti egységek tagjai felhasználói- és számítógépfiókok csoportok, és más szervezeti egységek lehetnek. Idegen tartományba tartozó objektumokat azonban nem tehetünk a szervezeti egységekbe. A szervezeti egységek használatának egyik legfontosabb előnye, hogy azok a tartományhoz hasonló tulajdonságokkal rendelkeznek, így alkalmazásuk csökkenti a szükséges tartományok számát. A szervezeti egység az Active Directory legkisebb objektuma, amelyhez csoportházirend objektumokat rendelhetünk, illetve amelyhez felügyeleti jogokat delegálhatunk. Az Active Directory-objektumokhoz tartozó jogosultságok és a csoportházirend is a szervezeti egység hierarchián keresztül öröklődnek.

A szervezeti egységek a tartományon belül szabadon áthelyezhetők, mozgathatók. A szervezeti egység-hierarchia megtervezése rendkívül fontos, mivel a jól kialakított hierarchia alapvető feltétele a csoportházirend hatékony működésének. A következőkben áttekintjük azokat a szempontokat, amelyeket figyelembe kell vennünk a szervezeti egységek kialakításakor.

A szervezeti egység-hierarchia kialakításnak alapvető szempontja az, hogy a létrehozott szerkezet minél jobban tükrözze a szervezet valódi felépítését, de nem feltétlenül a szervezeti hierarchia, hanem inkább a rendszerfelügyelet szempontjából. Azok a felhasználók, illetve számítógépek tartozzanak egy szervezeti egységhez, akikhez várhatóan azonos csoportházirend beállításokat szeretnénk majd rendelni, illetve azonos személyek fogják majd a delegált felügyeleti jogokat gyakorolni felettük. Természetesen a szervezeti egységek egymásba ágyazása bonyolítja a helyzetet, de a legfontosabb kérdés mégis ez legyen: melyek azok a felhasználók és számítógépek, amelyek többé-kevésbe azonos beállításokat igényelnek majd. Az alábbi táblázat a szokásos stratégiákat tartalmazza:

- **Földrajzi:** A struktúra kialakítása a különböző helyek, helyszínek alapján történik.
- **Szervezeti**: A struktúra a cég szervezeti felépítését tükrözi.
- **Feladatkör szerinti:** A hierarchia kialakítása a cég különböző osztályai, csoportjai alapján történik.
- **Vegyes:** A hierarchia legfelső szintjének kialakítása a helyszínek alapján, az alacsonyabb szintek felosztása viszont például a cég szervezeti felépítése alapján történhet.

A fiókok típusai

A felhasználói fiók

A felhasználói fiók (user account) az Active Directory alapú rendszer felhasználóját reprezentálja. Az objektum tárolja a felhasználó adatait (nevét, e-mail címét, telefonszámát stb.) és lehetővé teszi, hogy a rendszer különféle elemeihez hozzáférési jogosultságokat definiáljunk az objektum által reprezentált felhasználó számára. A központi tárolás és hitelesítés miatt a felhasználók a hálózat tetszőleges pontján azonosíthatják magukat és hozzáférhetnek a számukra engedélyezett erőforrásokhoz. Az Active Directory beépítetten tartalmaz néhány felhasználói fiókot (például az Administrator (Rendszergazda) felhasználót).

A felhasználói fiókok létrehozására és tulajdonságaik beállítására az Active Directory Users and Computers (Active Directory – felhasználók és számítógépek) konzol szolgál. Új felhasználó létrehozásakor csak néhány alapvető tulajdonságot kell megadnunk (például a bejelentkezési nevet és a jelszót), a többi beállítási lehetőséget a felhasználó tulajdonságlapján találhatjuk meg.

Itt az informális adatokon (telefonszámok, címek stb.) túl beállíthatjuk a jelszó kezelésével kapcsolatos különféle opciókat, meghatározhatjuk a felhasználói fiók lejáratát (a megadott időpont után a felhasználó már nem fog tudni bejelentkezni), azokat a számítógépeket, amelyeken az adott felhasználó bejelentkezhet stb. Ugyanitt adhatjuk meg azokat a csoportokat, amelyeknek tagja a felhasználó, ez a jogosultságok kiosztásának legegyszerűbb (és legcélszerűbb) módja.

A számítógépfiók

A számítógépfiók (computer account) az Active Directory-tartomány erőforrásainak használatára jogosult számítógépet reprezentál. Az objektum a számítógép számos tulajdonságát tartalmazza (DNS-név, operációs rendszer stb.) és lehetővé teszi, hogy a számítógépen megadott felhasználói adatokat a címtár hitelesítse.

A számítógépfiókok nem jönnek létre automatikusan (kivéve a tartományvezérlőkét), az objektumok létrehozásához az egyes ügyfélgépeket be kell léptetnünk a tartományba. (Természetesen létrehozhatjuk az objektumot az ügyfélgéptől függetlenül is, de ez nem elegendő ahhoz, hogy a számítógép valóban a tartomány tagjává váljon.) A tartományba való belépéshez az ügyfélgépen rendszergazdaként kell bejelentkeznünk, és a folyamat során meg kell adnunk egy olyan tartományi felhasználó hitelesítő adatait is, akinek joga van számítógépfiókokat létrehozni az adott konténerben.

A tartományba való beléptetés két fontos változással jár az ügyfélgépre való bejelentkezéssel kapcsolatban. Egyrészt a belépés után a helyi felhasználók mellett valamennyi engedélyezett tartományi (vagyis az Active Directoryban tárolt) felhasználó is be fog tudni jelentkezni a gépre. Ez azért lehetséges, mert gép helyi Users (Felhasználók) csoportjának tagja lesz a tartomány egyik alapértelmezett csoportja, a Domain Users (Tartományfelhasználók) csoport, vagyis a tartományi felhasználók a helyi Users csoporton keresztül kapnak jogot a gép helyi erőforrásainak elérésére. A másik lényeges változás pedig az, hogy a helyi Administrators (Rendszergazdák) csoportba bekerül a tartományi Domain Admins (Tartománygazdák) csoport, vagyis a tartomány rendszergazda jogú felhasználói rendszergazdaként jelentkezhetnek be a tartományhoz tartozó valamennyi számítógépen.

A csoportfiókok

A csoportfiókok (group account) az adminisztráció egyszerűsítését szolgálják, mivel a csoportokba helyezett felhasználó- és számítógépfiókok a csoporttagságon keresztül kaphatnak hozzáférési jogokat (biztonsági csoport esetén), vagyis, ha egy objektum hozzáférés-vezérlési listájában csoportfiók található, akkor a jogosultság a csoport minden tagjára vonatkozik.

A **terjesztési csoport** (distribution group) csak emailek terjesztésére használt, biztonsági szolgáltatásokkal nem rendelkező csoport. A terjesztési csoportok nem szerepelhetnek a különféle erőforrások és objektumok hozzáférés-vezérlési listáiban, (Access Control List, ACL), vagyis a terjesztési csoportnak nem adható semmiféle jogosultság. A terjesztési csoportok az elektronikus levelezőalkalmazásokkal használhatók elektronikus levelek felhasználócsoportoknak való elküldésére. Ha egy csoportnak nem akarunk jogosultságokat adni, hozzunk létre terjesztési csoportot biztonsági csoport helyett.

A **biztonsági csoportok** (security group) kifejezetten a jogosultságok kiosztásának megkönnyítésére szolgálnak, így hozzáadhatók az objektumok hozzáférésvezérlési listáihoz, és egymásba is ágyazhatók. A biztonsági csoport elektronikus levelezési egységként is használható. A csoportnak küldött elektronikus levelet a csoport összes tagja megkapja. A biztonsági csoport kategórián belül is több különböző csoportot különböztethetünk meg. A különbségtétel alapja egyrészt az, hogy kik lehetnek a csoport tagjai, másrészt pedig az, hogy milyen objektumokhoz adhatunk engedélyt az adott csoport számára, vagyis a csoport mely objektumok hozzáférés-vezérlési listáiban szerepelhet. A fenti két szempont szerint a biztonsági csoportoknak négy típusáról beszélhetünk:

- **Helyi csoport** (Machine Local Group) – Olyan biztonsági csoport, amely csak annak a számítógépnek az erőforrásaihoz kaphat jogokat és engedélyeket, amelyen a csoportot létrehozták. A helyi csoportok tartalmazhatják bármely megbízható hely, például a tartomány, vagy más megbízotti kapcsolatban álló tartományok és erdők felhasználói fiókjait és csoportjait. Fontos szabály, hogy helyi erőforráshoz csak helyi csoportnak adjunk közvetlenül jogosultságot, vagyis például egy ügyfélgép NTFS-jogainak kiosztásakor egyetlen hozzáférés-vezérlési listába se kerüljön felhasználói fiók, illetve tartományi csoport (az egyes felhasználók profilját tároló mappákon kívül). A tartomány szintjén definiált csoportok mindig a helyi csoport tagjai közé való felvétellel szerezzenek jogot az erőforrások használatára.
- **Tartományon belüli csoport** (Domain Local Group) – A tartományon belüli csoportok tagjai a Windows Server 2008, a Windows Server 2003, Windows 2000 és Windows NT alapú 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 saját tartományában található felhasználók, csoportok és számítógépek. A globális biztonsági csoport 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. Univerzális hatókörű csoportnak 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.

A tartomány és az erdő működési (funkcionalitási) szintje határozza meg, hogy milyen csoportok létrehozására van lehetőségünk.

3. A csoportházirend

A csoportházirend technológia segítségével a tartomány számítógépeinek különféle operációs rendszer-, alkalmazás-, és felhasználószintű beállításait a rendszergazda nem egyenként, hanem meghatározott csoportok számára együttesen adhatja meg. A csoportházirend alkalmas a rendszergazda által előírt, a számítógépekre és a felhasználókra vonatkozó beállítások kikényszerítésére is, az így szabályozott opciókat a felhasználók akkor sem módosíthatják véglegesen, ha egyébként a jogosultságaik ezt megengednék.

A létrehozott házirendeket (vagyis beállításcsoportokat) úgynevezett Group Policy Objectek (csoportházirend objektum, GPO) tárolják, ezeket az objektumokat lehet a kiválasztott Active Directory-tárolókkal (telephely, tartomány, szervezeti egység) összekapcsolni.

A csoportházirend objektumokban tárolt beállítások az ügyfélgépeken registryértékek formájában jelennek meg, az operációs rendszer és az alkalmazások pedig ezeket a registryértékeket használják fel működési paraméterként. Bár gyárilag is számos csoportházirend jár az operációs rendszerhez (az XP/Windows 2003-ra mintegy 1700, a Vista/Windows 2008 párosra legalább 2700, a Windows 7/Windows 2008 R2-re több mint 3000 házirend vonatkozik[3]), ez a szám tetszőlegesen bővíthető további sablonok (admin templates, .ADM, illetve .ADMX) hozzáadásával. Ezek egyszerű szöveges állományok, amik a beállítások hierarchikus rendjét, a beállítható értékekre vonatkozó megkötéseket és az egyes beállítások alapértelmezett értékét tartalmazzák. A Microsoft is kiad bővítéseket pl. a Microsoft Office szabályozásához, de más gyártók termékeihez is készülnek ilyenek. Egyedi .ADM-fájlokkal szinte bármit meg lehet tenni, amihez egyébként a beállításjegyzék módosítása szükséges.

A helyi házirend és a csoportházirend

A helyi házirend működési elve megegyezik a csoportházirendével, de az itt megadott beállítások csak egyetlen gépre vonatkoznak, ráadásul lényegesen kevesebb opcióból választhatunk. A helyi házirendet a gpedit.msc konzollal módosíthatjuk, ennek segítségével megadhatóak a számítógépre és a felhasználókra vonatkozó különféle beállítások.

Ha a beállításokat a gpedit.msc konzol segítségével módosítjuk, akkor gyakorlatilag közvetlenül írunk a registrybe, így a beállítások azonnal életbe lépnek, de előfordulhat, hogy nem lesznek hosszú életűek. Tartományi tagság esetén a beállítások ugyanis csak addig maradnak ténylegesen érvényben, amíg a csoportházirend biztonsági opcióinak következő frissítése meg nem érkezik a gépre, ekkor ugyanis a csoportházirend beállításai felülírják azokat a helyi beállításokat, amelyekkel ütközésbe kerülnek.

A csoportházirend esetében a beállítások az Active Directory tárolóihoz (telephely, tartomány, szervezeti egység) kapcsolhatók és az adott tárolóban lévő összes számítógép-, illetve felhasználó objektumra érvényesek lesznek. A helyi házirendben is szereplő beállítások mellett a csoportházirend számos más opciót is kínál, amelyek segítségével a kiszolgáló által biztosított különféle szolgáltatásokkal kapcsolatos beállításokat határozhatjuk meg.

Mire használjuk?

A csoportházirend igen széles körben használható, alig van olyan fontos beállítási lehetőség, ami nem érhető el ilyen módon. A következőkben áttekintjük azokat a tipikus feladatokat, amelyekre a csoportházirend alkalmas:

- **Szoftvertelepítés** – A csoportházirend segítségével Windows Installer (msi) csomagokat teríthetünk a hálózaton automatikusan. A telepítendő alkalmazások a számítógépekhez és a felhasználókhoz is csatolhatók, telepítésük a számítógép induláskor, illetve a felhasználó bejelentkezése után történik meg. Lehetőség van az alkalmazások automatikus frissítésére és javítására is.
- **Mappák átirányítása** – A felhasználókhoz tartozó Dokumentumok mappát a lokálisan tárolt profilból átirányíthatjuk egy hálózati megosztott mappába. A központilag tárolt dokumentumok megkönnyítik a felhasználók adatainak biztonsági mentését, és lehetővé teszik, hogy a felhasználók különböző gépeken bejelentkezve is elérjék a Dokumentumok mappa tartalmát. A felhasználók számítógépén a Dokumentumok mappa gyorsítótárba helyezett példánya található, így a fájlok akkor is elérhetők, ha a gép éppen nincs kapcsolatban a hálózattal. Minden esetben, amikor a felhasználó be-, vagy kijelentkezik, a rendszer szinkronizálja a Dokumentumok mappa ügyfélszámítógépen lévő példányát a kiszolgálón lévő példánnyal.
- **Szkriptek** – Minden számítógéphez és felhasználóhoz két-két szkriptet rendelhetünk. Az egyik szkript a gép indításakor, illetve felhasználó bejelentkezésekor, a másik leállításkor, illetve kijelentkezéskor fog lefutni. A szkriptek lehetnek hagyományos parancsfájlok (cmd.exe), vagy VBScript és PowerShell nyelvű szkriptfájlok is, bár a PowerShell szkriptek közvetlen indítása nem lehetséges. A szkriptek a tartományvezérlők SYSVOL megosztására kerülnek, innen töltik le őket az ügyfélgépek.
- **Biztonsági beállítások** – a csoportházirend megszámlálhatatlanul sok biztonsági beállítást kínál, ezek közül csak a legfontosabbakat említjük: A jelszóházirend segítségével meghatározhatjuk a használható jelszavak minimális hosszát, bonyolultságát, a jelszó minimális és maximális élettartamát stb. A fiókzárolási házirend meghatározza a hibás bejelentkezések maximális számát, és a túllépés esetén alkalmazandó szankciót. Beállíthatjuk a naplózásra és a felhasználói jogokra vonatkozó opciókat, és az eseménynapló takarítási paramétereit is. A biztonsági beállítások hangolását ráadásul sablonok segítségével is elvégezhetjük. Indokolt azonban az óvatosság, mivel egy meggondolatlan mozdulattal olyan biztonságossá tehetünk mondjuk egy távoli telephelyen lévő tartományvezérlőt, hogy a házirend letöltődése után többé mi magunk sem érjük el azt a hálózatból, és így nem is tudjuk visszabillenteni túlzottan biztonságos állapotából.
- **Az Internet Explorer karbantartása** – megadhatjuk az internetkapcsolatra (például proxy használat), a böngésző biztonsági beállításaira és felhasználók környezetére vonatkozó beállításokat, például tetszőleges elemeket adhatunk hozzá a Kedvencek (Favorites) listához.
- **Felügyeleti sablonok** – a csoportházirend rendszer külső bővítményei jelennek meg ebben a szakaszban, így itt találhatjuk meg az operációs rendszer számtalan elemére (Start menü és tálca, Asztal, Vezérlőpult, Médialejátszó, lemezkvóták stb.), a hálózatra (DNS-beállítások, tűzfal stb.), vagy például a nyomtatókra vonatkozó beállítási lehetőségeket.

Hogyan működik a csoportházirend?

A csoportházirend beüzemeléséhez tehát először is létre kell hoznunk a telephely, a tartomány, vagy a szervezeti egység szintjén a megfelelő csoportházirend objektumokat (GPO), amelyben megadjuk azokat a beállításokat, amelyeket az adott objektum fog szállítani az ügyfélgépekre. Minden GPO két elkülönített szakaszból áll, az egyikben megadott beállítások a számítógépekre (bármelyik felhasználó is jelentkezik be), a másikban megadottak pedig a felhasználókra (bármelyik gépen is jelentkeznek be) fognak vonatkozni. A csoportházirend objektumokban megjelenő beállítási lehetőségeket a csoportházirend sablonok (group policy templates), vagyis .adm kiterjesztésű fájlok határozzák meg, ezekből a Microsoft időről időre frissített verziókat ad ki az új komponensek támogatására, de egyedi célra akár mi magunk is készíthetünk ilyen sablonfájlt.

A beállítások megadása után az adott tárolóban lévő felhasználó objektumokra a felhasználó szakaszban megadott, a számítógép objektumokra pedig a számítógép szakaszban szereplő beállítások fognak érvényesülni. Természetesen egy GPO-t több tárolóhoz is hozzárendelhetünk, és egy felhasználóra, illetve számítógépre is érvényesülhet több csoportházirend objektum. A csoportházirend objektumok létrehozásakor két, egymásnak bizonyos mértékben ellentmondó szempontot kell figyelembe vennünk, vagyis meg kell találnunk a helyes egyensúlyt:

- Lehetőleg minél kevesebb csoportházirend objektumot hozzunk létre. Természetes, hogy kevesebb objektummal kevesebb baj van, a beállítások jobban áttekinthetőek stb.
- Másrészt hozzunk létre lehetőleg külön csoportházirend objektumot minden összetartozó beállításcsoport számára, mert így finomabban tudjuk adagolni, kiosztani a GPO-kat a számítógép-, illetve felhasználócsoportoknak.

Az öröklődés

A magasabb szintű (szülő) konténerekhez rendelt GPO-k beállításai alapértelmezés szerint öröklődnek a gyermektárolókra és kombinálódnak (összeadódnak) az ide csatolt GPO-k beállításaival. Ha több GPO eltérő értékkel tartalmazza ugyanazt a beállítást, akkor azok felülírják egymás hatását az öröklési lánc mentén.

Minden konténeren lehetőségünk van azonban a fentről érkező öröklődés megszakítására, ha bekapcsoljuk a Block Inheritance (öröklődés megszakítása) opciót. Ez a lehetőség nagyon jól használható, ha például olyan GPO-t kell beüzemelnünk, ami egyetlen OU kivételével a teljes tartományra vonatkozik. Ekkor hozzáköthetjük a GPO-t a tartományhoz, a kivételes OU-n pedig egyszerűen megszakíthatjuk az öröklődést.

Problémát okozhat azonban, hogy ebben az esetben a tartomány szintjén megadott egyetlen GPO sem ér le az adott szervezeti egységhez. Ennek megoldására szolgál egy másik öröklődéssel kapcsolatos beállítási lehetőség. Minden GPO-n beállítható az Enforce (kikényszerítés) tulajdonság. Az ilyen GPO-k egyszerűen nem veszik figyelembe, hogy az alacsonyabb szintű tároló meg akarja szakítani az öröklődést, és ettől függetlenül is érvényre jutnak.

A csoportházirend objektumok prioritása

Nagyon fontos, hogy figyelembe vegyük az egyes GPO-k kiértékelésének sorrendjét, ami egyben azok prioritását is jelenti, mivel ütközés esetén a később érkező beállítások felülírják a korábbiakat. A sorrend tehát:

- Helyi házirend
- A telephely szintjén megadott házirend objektumok (a rendszergazda által megadott sorrendben). A feldolgozás a legnagyobb sorszámú (Link order) GPO-val kezdődik, vagyis mindig az egyes sorszámú GPO a legerősebb, ennek prioritása a legmagasabb.
- A tartomány szintjén megadott házirend objektumok (a rendszergazda által megadott sorrendben).
- A szervezeti egység szintjén megadott házirend objektumok a nagyobb (szülő) szervezeti egységtől kezdve a kisebb (gyermek) szervezeti egységekig sorban, az egyes OU-k esetében pedig a rendszergazda által megadott sorrendben.

Ez tehát azt jelenti, hogy ütközés esetén az utolsó (tehát a legkisebb, a felhasználót vagy számítógépet közvetlenül tartalmazó szervezeti egység legkisebb sorszámú házirendje) győz, vagyis ennek prioritása a legnagyobb. Természetesen, ha nincs ütközés a beállítások között, akkor a sorrendnek nincs jelentősége, vagyis minden megadott beállítás érvényesülni fog az adott felhasználóra, illetve számítógépre.

A csoportházirend végrehajtásának sorrendje

- Az operációs rendszer indulása közben elsőként a számítógépre vonatkozó csoportházirend objektumok töltődnek le és értékelődnek ki. Ekkor történhet meg például a számítógéphez rendelt szoftverek telepítése is.
- Ezután következik a számítógép számára megadott **startup (indítási) szkript** futása (mindkét említett folyamat befejeződik még a bejelentkezési ablak megjelenése előtt).
- Következik a felhasználó bejelentkezése, természetesen eddig a pontig semmiféle felhasználói beállítás, szkript stb. érvényesítésére nincs lehetőség.
- A bejelentkezés után érvényre jutnak a csoportházirend felhasználói beállításai, például a felhasználóhoz rendelt szoftverek telepítése.
- Ezután fut le az a **logon (bejelentkezési) szkript**, amelyet a csoportházirend segítségével rendeltünk a felhasználóhoz.
- Végül lefut a felhasználói fiókhoz közvetlenül hozzárendelt logon szkript.

Alapértelmezett csoportházirend objektumok

Az Active Directory telepítésekor alapértelmezés szerint létrejön két csoportházirend- objektum.

- A **Default Domain Policy** (Alapértelmezett tartományi házirend) a teljes tartományhoz tartozik, és az öröklődés révén a tartományba tartozó valamennyi felhasználóra és számítógépre (így a tartományvezérlőkre is) érvényes.
- A **Default Domain Controllers Policy** (Alapértelmezett tartományvezérlői házirend) a tartományvezérlőket tartalmazó Domain Controllers (Tartományvezérlők) szervezeti egységhez tartozik, ezért csak a tartományvezérlőkre hat.

A csoportházirend frissítése

A csoportházirend objektumokon végrehajtott változások nem érvényesülnek azonnal a számítógépeken, illetve felhasználókon. Az automatikus frissítés az ügyfélgépek esetében 90, a tartományvezérlőknél pedig 5 percenként történik. A türelmetlenebbek azonban kézzel is kikényszeríthetik a frissítést a **gpupdate** (esetleg a mindent frissítő gpupdate/force) használatával. Ilyenkor sem futnak le azonban a gépindításhoz, leállításhoz, illetve ki-, bejelentkezéshez kötött események (szkriptek), ezek futtatásához újra kell indítanunk a számítógépet, illetve újra be kell jelentkeznünk. A gpupdate parancs csak a Windows XP operációs rendszerben jelent meg, korábban (Windows 2000) a secedit parancs megfelelő paraméterezésével érhettük el ugyanezt a hatást.

A Group Policy Management Console

A **Group Policy Management Console** (Csoportházirend-felügyeleti konzol, GPMC) a csoportházirend objektumok kezelésének új eszköze. A konzol felületén mindent megtalálhatunk, ami a házirendek kezelésével kapcsolatban elképzelhető, felülete nagyon jól elrendezett, segítségével könnyen megérthető és felügyelhető a csoportházirend működésének minden aspektusa. Használata mindenképpen javasolt még a régebbi rendszerek felhasználóinak is, mivel a konzol Windows 2000 és Windows 2003 tartományban is működik. A Windows 7 operációs rendszerben a konzol beépítetten megtalálható a Features között.

A GPMC segítségével az alábbi feladatokat végezhetjük el:

- Létrehozhatunk új házirend objektumokat, és az egyes objektumokra meghívható csoportházirend-objektum szerkesztő (ez nem a GPMC, hanem az operációs rendszer része) segítségével megadhatjuk az abban szereplő beállításokat.
- A létrehozott házirend objektumokat hozzáköthetjük (link) a megfelelő Active Directory konténerekhez.
- Könnyen áttekinthető listában megjeleníthetjük az egyes csoportházirend objektumokban lévő beállításokat, nem kell azokat a szerkesztő alkalmazás felületén megkeresni.
- Delegálhatjuk az egyes GPO-k felügyeleti jogait felhasználók, illetve biztonsági csoportok számára.
- Menthetjük és helyreállíthatjuk a csoportházirend objektumokat (akár valamennyit egy lépésben).
- Ellenőrizhetjük az öröklődést, beállíthatjuk a blokkolást és kikényszerítést, illetve beállíthatjuk az egy konténerre ható csoportházirend objektumok közötti prioritási sorrendet.
- A Group Policy Results eszköz segítségével lekérdezhetjük az egyes felhasználókra, illetve számítógépekre aktuálisan ható csoportházirend objektumokat, és összegezve megtekinthetjük az azokban szereplő beállításokat.
- Jelentéseket készíthetünk HTML-formátumban