Gál Tamás – Szabó Levente – Szerényi László

Rendszerfelügyelet rendszergazdáknak

SZAK KIADÓ

Gál Tamás
Szabó Levente
Szerényi László

Rendszerfelügyelet rendszergazdáknak

SZAK KIADÓ

2007

Rendszerfelügyelet rendszergazdáknak

Gál Tamás – Szabó Levente – Szerényi László

ISBN 978-963-9131-98-9

A szöveg helyességét és az elválasztásokat a MorphoLogic Helyesek nevű programjával ellenőriztük.

SZAK Kiadó Kft. ■ Az 1795-ben alapított Magyar Könyvkiadók és Könyvterjesztők Egyesülésének a tagja ■ 2060 Bicske, Diófa u. 3. ■ Tel.: 36-22-350-209 ■ Fax: 36-22-565-311 ■ www.szak.hu ■ e-mail: info@szak.hu ■ Kiadóvezető: Kis Ádám, e-mail: adam.kis@szak.hu ■ Főszerkesztő: Kis Balázs MCSE, MCT, e-mail: balazs.kis@szak.hu

Tartalomjegyzék

Előszó

Rendhagyó és sok szempontból hiánypótló könyvet tart a kezében az Olvasó. Már a cím is sokat elárul: ez a könyv kifejezetten rendszergazdáknak készült, és minden témát a rendszergazda szemével fejtünk ki benne. Tartalmát tekintve kezdő és haladó rendszergazdáknak is bátran ajánlható – megtalálható benne a Windows-alapú rendszerek ismeretéhez és felügyeletéhez elengedhetetlenül szükséges alapozás, de közben folyamatosan megragadjuk az alkalmat arra, hogy benézzünk a motorháztető alá.

Mindebből az is következik, hogy átlagos felhasználókat érdeklő funkciókról gyakorlatilag nem esik szó ebben a könyvben – arról ezernyit lehet már fellelni a könyvesboltok polcain. Mi most kifejezetten arra fókuszálunk, hogy a világszerte milliók által használt Windows operációs rendszerek működését és felépítését mélységében ismertessük, és megmutassuk, hogyan lehet segítségükkel akár kis-, akár nagyobb vállalatnál egy informatikai rendszert megtervezni, megépíteni és felügyelni.

A könyv felépítése követi a vállalatok informatikai evolúcióját is – az első részben kifejezetten az ügyféloldallal foglalkozunk csak: megmutatjuk, hogy a kizárólag ügyfél operációs rendszerekből álló, néhány gépes hálózat működtetéséhez milyen képességek megismerésére lesz szükségünk, hogyan lehet ezt a környezetet hatékonyan üzemeltetni és felügyelni. Külön kiemelt figyelmet szentelünk a biztonságnak, aminek kapcsán jelentős változások történtek a Windows Vista megjelenésével.

A második részben egy kiszolgálóval bővítjük elképzelt vállalatunk informatikai rendszerét, és megnézzük, milyen előnyök járnak ezzel mind a vállalat, mind a rendszergazda számára – és egyáltalán mikor érdemes kiszolgálót alkalmazni. Ha már van kiszolgálónk, a következő fejlődési lehetőség a címtár beüzemelése, majd a csoportházirend alkalmazása – ezzel is egy külön fejezetünk foglalkozik. Mindezek után – mivel előbb-utóbb úgyis minden elromlik és tönkremegy – utolsó fejezetünkben részletesen foglalkozunk a hibakereséssel és elhárítással is.

A kapcsolódó tananyag

Könyvünk mindössze egyetlen (de jelentős) alkotóeleme egy lényegesen nagyobb tananyagnak, amelynek kidolgozásával az elsődleges célunk az, hogy a lehető legkönnyebbé tegyük minden rendszergazda számára a szakma alapos elsajátítását, és egyben részletesen megismerhessék a legújabb eszközöket is – a Windows Vistát és a Windows Server 2003 R2-t.

A tananyag köré Informatika Tisztán névvel egy előadássorozatot is szerveztünk, ennek 2007 őszén lezajlott 12 előadásával közel 5000 informatikusnak mutattuk meg a rendszerfelügyelet legfontosabb és legérdekesebb újdonságait. Az eseménysorozat sikerére való tekintettel 2008-ban várható annak folytatása is – új tananyagokkal, előadásokkal, helyszínekkel bővítve. A jelenleg elérhető és a jövőben jelentkező tananyagok, eseményinformációk a www.microsoft.hu/it oldalon találhatóak.

Ellentétben az informatikai szakkönyvek többségével, ebből a könyvből gyakorlatilag teljesen hiányoznak a kattintgatós, mindent lépésenként bemutató leírások, helyettük sokkal látványosabb és használhatóbb formában, rövid videókat (mi csak screencastoknak hívjuk őket) készítettünk el – ezek mind megtalálhatóak könyvünk DVD-mellékletén. Ezeken a videókon keresztül részletesen, élőben mutatjuk be a rendszerek képességeinek gyakorlati használatát. Hatalmas mennyiségű anyagról van itt szó: messze több képességet mutatunk meg bennük, mint amennyit az egy napos előadásokon lehetőségünk volt.

A könyv szövege és a videók egymásra épülnek, és jól kiegészítik egymást. Ezzel a megoldással a könyvben sokkal többet tudunk foglalkozni a rendszerek mélységeivel, hátterével, hogy tényleg alapos tudás birtokába lehessen kerülni általa. Más részről a videók segítségével hihetetlenül gyorsan és kényelmesen lehet haladni a rendszer megismerésében, akár a könyv használata nélkül is – majd a számunkra érdekesebb funkcióknak bármikor részletesebben utánaolvashatunk.

Ahhoz azonban, hogy gyakorlati tapasztalatra is szert tegyünk, ez még mindig kevés. Éppen ezért a DVD-mellékletre felkerült a Windows Vista és a Windows Server 2003 R2 virtuális környezetben használható változata, így bármikor lehetőség van a könyvben és a videókban található képességek kipróbálására – méghozzá a virtualizációnak köszönhetően mindezt a nélkül is megtehetjük, hogy emiatt egy külön számítógépet kellene tesztcélokra kineveznünk. A virtuális gépek használatáról könyvünk végén, egy külön leírás formájában található további információ.

A tananyag kidolgozottsága révén arra is tökéletesen alkalmas, hogy az tanfolyamok, főiskolai és egyetemi kurzusok alapját képezze. Azon oktatási intézmények és oktatók részére, akik szeretnék ezt a tananyagot tanítani, a Microsoft Magyarország további segítséget is tud nyújtani – érdemes tehát megkeresni bennünket ezzel kapcsolatban.

Ha már ötször kiolvastuk a könyvet...

Akik még mélyebben szeretnének megismerkedni a Microsoft szoftverek képességeivel, azoknak a hivatalos Microsoft Oktatóközpontok tanfolyamait ajánljuk, amelyek tantermi környezetben, laborgyakorlattal egybekötve segítik az egyes technológiák alapos megismerését. Aki pedig úgy gondolja, hogy már tényleg gyakorlott egy adott szoftver használatában, próbára teheti magát hivatalos Microsoft vizsgákon is. Ezek sikeres teljesítésével világszerte elismert oklevelet és minősítést (Microsoft Certified Proessional, MCP) szerezhet, – ami jelentősen megkönnyíti az elhelyezkedést a szakmában. A legnagyobb vállalatok és Microsoft-partnercégek sokkal szívesebben bíznak feladatot olyan szakemberre, aki már rendelkezik hivatalos Microsoft-vizsgákkal, ezzel is bizonyítva az adott terület mélyreható ismeretét.

Ha a könyv olvasása vagy munkája során bármilyen szakmai kérdése merülne fel, forduljon bátran hozzánk, szívesen segítünk – a TechNet Fórumon *(www.microsoft.hu/technetforum)* a Microsoft szakemberei, a Microsoft által kitüntetett szakemberek *(Most Valuable Professional, MVP),* és a Fórum felhasználói segítenek egymásnak szakmai kérdések megválaszolásában.

Gyakorlás nélkül nem megy!

Bízunk abban, hogy ezzel a könyvvel és a teljes tananyaggal jelentős segítséget tudunk nyújtani a rendszergazda szakma iránt érdeklődők és a szakmával már régebb óta foglalkozó szakembereknek is, hogy hatékonyan bővíthessék ismereteiket. Tíz-tizenöt évvel ezelőtt a szakma megismerése csak hosszú, önálló munkával, és rengeteg hiba elkövetésével volt lehetséges – ma viszont már minden információ és eszköz rendelkezésre áll ahhoz, hogy ezt a tanulási folyamatot lényegesen lerövidítsük – erre szolgál ez a könyv is. De ne felejtsük el, hogy gyakorlásra így is szükség van – időt és energiát kell szánnunk arra, hogy élesben is tudjuk használni ismereteinket.

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani mindazoknak, akik lehetővé tették, hogy ez a könyv és a kapcsolódó tananyag jó minőségben elkészüljön, és minél több mindenkihez eljuthasson. Az alábbi lista jól tükrözi, hogy a jó munkához a sok időn és az alaposságon kívül hatékony csapatmunkára is szükség van. Természetesen, mint ahogy minden szoftver garantáltan hibás, ez a lista is bizonyosan hiányos.

Köszönjük a segítséget:

- *Gál Tamásnak* (Microsoft, MVP) a tananyag koncepciójáért, elkészítéséért, a számtalan előadásért, a screencastokért, a könyv lektorálásáért és a Windows Vista fejezetek véglegesítéséért. Sem a könyvben, sem a tananyagban nincs olyan pont, amin ne lenne felfedezhető a hatásod és szakmai maximalizmusod.
- *Szabó Leventének* (MVP) és *Szerényi Lászlónak* a könyv megírásáért és a rengeteg szakmai segítségért.
- *Pazár Andrásnak* (MVP) a Windows Vista screencastok elkészítésében nyújtott segítségéért.
- Az Informatika Tisztán események előadóinak: *Baki Gábornak*, *Farkas Bálintnak* (Microsoft), *Fóti Marcellnek* (MVP), *Horváth Zoltánnak*, *Németh Zsoltnak*, *Oláh Istvánnak*, *Ország Tamásnak*, *Réczi Gábornak* (MVP), *Szallabek Zoltánnak*, *Szentgyörgyi Tibornak*, *Somogyi Csabának* (Microsoft) és *Soós Tibornak*. A remek előadások mellett rengeteg hasznos visszajelzést kaptunk tőletek a tananyag elkészítéséhez és tökéletesítéséhez.
- Az *IQSOFT-John Bryce*, a *NetAcademia* és a *SZÁMALK* hivatalos Microsoft oktatóközpontoknak, amiért részt vettek a tananyag és a kapcsolódó tanfolyamok megvalósításában.
- A *SZAK Kiadónak*, azon belül is elsősorban *Kis Ádámnak*, amiért ez a könyv kitűnő minőségben megjelenhetett, és ott lehet minden könyvesboltban.
- Valamint minden közreműködő kollégának a Microsoft Magyarországnál, külön kiemelve:
    - *Keszei Balázsnak* az Informatika Tisztán programsorozat koncepciójának kidolgozásával és megvalósításával kapcsolatos hatalmas közös munkáért.

- *Deme Csabának, Takács Péternek* és *Vityi Péternek* a támogatásért.
- *Schlégl Tímeának* és *Biber Attilának* amiért láttatok fantáziát az ötleteinkben, és segítettetek megvalósítani őket.
- *Szőcei Olivérnek és a webes teamnek* az Informatika Tisztán web-oldalának elkészítéséért.
- *Safranka Mátyásnak* a Windows Vistával kapcsolatos szakmai segítségért.

Budai Péter (i-pbudai@microsoft.com)
Programmenedzser – IT szakmai programok
Microsoft Magyarország

Budapest, 2007. december 2.

I. RÉSZ

Az ügyfél

Könyvünk első – az ügyféloldallal foglalkozó – része három jól elkülöníthető fejezetből áll.

Alapismeretek 3. oldal

Az első fejezet az új operációs rendszer bevezetési, telepítési tudnivalóiról, és az általános rendszeráttekintésről szól. A fejezet részeként részletesen beszámolunk a Windows Vista örökölt illetve teljesen új hálózati képességeiről.

Diagnosztika és felügyelet 55. oldal

A második fejezet központi témája a rendszergazdák egyik legfontosabb „működési területe”, a rendszerfelügyelet. Ennek megfelelően ebben a részben számos, az üzemeltetéshez nélkülözhetetlen, integrált felügyeleti eszköz képességeit ismertetjük, a fejezet zárásaként pedig a Helyi házirendről nyújtunk egy alapos áttekintést.

Az ügyfelek biztonsága 97. oldal

Az első rész legvaskosabb fejezete az informatikai biztonsággal foglalkozik. Részletesen és mélyrehatóan ismertetjük a Windows ügyfél operációs rendszerekben alkalmazott biztonsági technológiákat és megoldásokat – az alapoktól kezdve. Természetesen a fejezet döntő hányadában a Vista jelentős mennyiségű új biztonsági szolgáltatásairól, illetve komponenseiről lesz szó.

ELSŐ FEJEZET

Alapismeretek

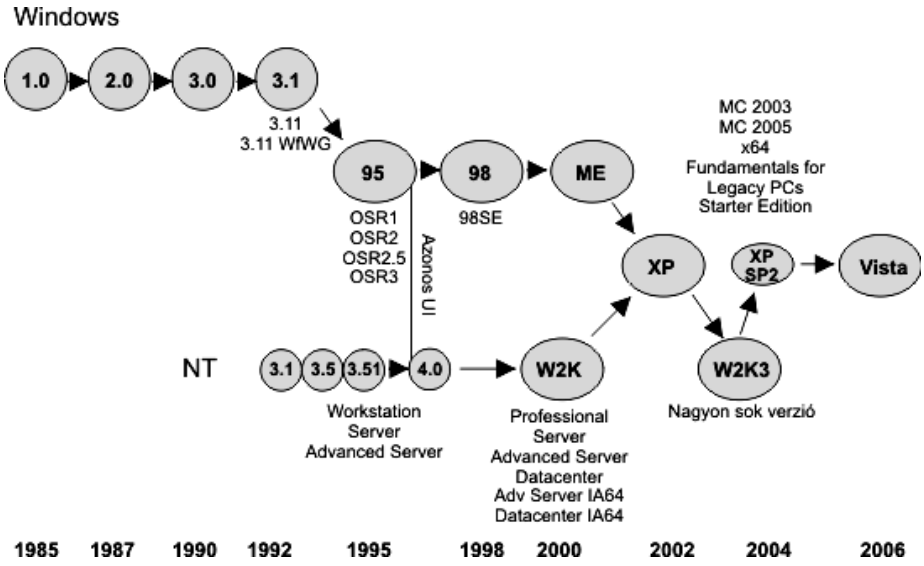
A fejezet tartalma:

Ügyféloldal — bevezetés

A Windows Vista a Microsoft ügyféloldali operációsrendszer családjának hatodik tagja. Technikailag tekinthetjük tehát csak egy következő „rendes" családtagnak a sorozatban. Némi háttérinformáció és gyakorlati tapasztalat birtokában azonban kiderül, hogy valójában jelentős a különbség az e sorozatba tartozó korábbi operációs rendszerek és a Vista között. Köztudomású például az a tény, hogy a Windows Vista nemcsak a legfrissebb, hanem a leghosszabb ideig fejlesztett operációs rendszer is a Microsoft jelenlegi palettáján. A Windows XP 2001. októberi debütálása és a Vista 2006. novemberi, (illetve 2007. január 31., a bárki által megvásárolható példányokat tekintve) megjelenése között több mint öt év telt el, ami az ügyfél operációs rendszereknél hagyományosan nagyjából két ciklust jelent – vagy egy nagyon alaposat.

Az 1.1. ábrán a felső sor a klasszikus Windows-ügyfelek, míg az alsó az NT-alapokra épített operációs rendszerek listája. A két sorozat 2001-ben, a Windows XP-ben egyesült, így a Vistában sincs már jelen ez a fajta megkülönböztetés.

A másik fő érv egy kissé behatároltabb, de kimagaslóan fontos területre mutat, mégpedig az informatikai biztonság és a megbízhatóság területére. A Microsoft által 2002-ban meghirdetett és az összes azóta készült termék tervezésénél és kivitelezésénél használt Trustworthy Computing *(megbízható számítástechnika)* elv mentén érkező változások a Windows XP második szervizcsomagjában érvényesültek először, de teljes mértékű, az alapoktól kezdődő és valóban mélyreható alkalmazásra a Windows Vistában került sor.



1.1. ábra: *A Windows család tagjai*

E két kiragadott érv mellett a gyakorlati használat közben tapasztalhatjuk azt is, hogy a Vista számtalan helyen hoz újítást a korábbi verziókhoz képest a hálózat, illetve a hardver kezelésében, a rendszer üzemeltetésében, karbantartásában és felügyeletében, és sok kisebb és nagyobb, új vagy teljesen megújult eszközzel igyekszik megkönnyíteni az üzemeltető informatikusok munkáját is. Éppen ezért, ebben a kifejezetten rendszergazdáknak szánt könyvben, az ügyféloldali operációs rendszert érintő fejezetekben elsősorban a Windows Vista komponensein és szolgáltatásain keresztül mutatjuk be az operációs rendszer és részegységeinek működését, a segítségével kivitelezhető műveleteket és megoldható feladatokat.

Mindezt eleinte kisebb „hatású" forgatókönyvek alapján tesszük meg, a klasszikus kiszolgálókkal, tartománnyal és központi felügyelettel felvértezett környezet helyett, önálló működést vagy kisebb hálózatos rendszert feltételezve.

Mikor és miért nincs szükség kiszolgálóra?

Ha kevés vagy esetleg egyetlen számítógéppel dolgozunk, akkor nem feltétlenül van szükség kiszolgáló számítógépre, az ügyfélgépek bőven elegendő szolgáltatást nyújtanak a kisebb, társ–társ *(peer-to-peer)* hálózatok működtetéséhez és felügyeletéhez. Az ilyen méretű hálózatok esetén viszonylag ritkán van igény az erőforrások megosztására vagy az erőforrásokat a beüzemelésük után csak minimálisan használják megosztva, mivel a gépek többnyire helyi szolgáltatásokat vesznek igénybe.

Természetesen ilyen környezetben is lehetőségünk van arra, hogy fájlokat vagy nyomtatókat elérhetővé tegyünk a többi gép számára, illetve ekkor is megoldható a munkaállomások felügyelete és a megfelelő jogosultságok kiosztása a felhasználók számára és azok karbantartása. A modern asztali Windows operációs rendszerek a biztonság, a felügyelet és rendelkezésre állás szempontjából felkészültek, így az egyszerűbb adminisztratív feladatokat a helyi, beépített eszközökkel is kifogástalanul elvégezhetjük.

Az alábbi esetekben tehát nincs szükség kiszolgálóra:

- kevés számú géppel dolgozunk;
- nincs hálózati kapcsolat a gépek között;
- nagyon kevés erőforrás-megosztást használunk (vagy egyáltalán nem használunk);
- nincs szükség a gépek és felhasználók központi felügyeletére.

A következő fejezetekben a Windows Vista ügyfél operációs rendszer önálló üzemeltetését, konfigurálását és felügyeletét tárgyaljuk – némiképp összehasonlítva az előző változattal, a Windows XP-vel – valamint áttekintjük azokat a beépített szolgáltatásokat, melyek bizonyos esetekben lényegében szükségtelenné tehetik a kiszolgáló beszerzését. Kezdjük tehát az ügyfél operációs rendszer bevezetésének és telepítésének részleteivel!

A Windows Vista telepítése

A Windows XP, mely a Vista közvetlen elődjének tekinthető az ügyféloldali operációs rendszerek között, összesen két fő változatban jelent meg: az otthoni felhasználóknak szánt **Home**, illetve az összetettebb vállalati hálózatos környezetekben is alkalmazható **Professional** változatban. Ezen kívül természetesen több speciális változat is elérhető volt, mint például a táblaszámítógépek speciális hardverelemeit (pl. az érintőkijelzőjét) kihasználó **Tablet PC Edition**, az otthoni multimédiára kihegyezett **Media Center Edition**, vagy csak a fejlődő országokban kapható, gyengébb teljesítményű számítógépek számára „lebutított” **Starter** változat. A 64-bites processzorok megjelenését követően 2005-től a Windows XP 64-bites változata is elérhetővé vált, mely a 64-bites hardverek csekély támogatottsága miatt azonban nem igazán terjedt el széles körben.

A Vista változatai

A Microsoft, annak érdekében, hogy a lehető legnagyobb felhasználói kör számára elérhetővé tegye a Vistát, összesen hat változatban készítette el az új operációs rendszert, melyek sora az alapfunkcionalitású, otthoni felhasználásra alkalmas kiadástól egészen a professzionális, nagyvállalati környezetekhez megfelelő rendszerekig terjed. A Windows Vista változatai a következőképp alakulnak:

- **Starter** – Gyengébb hardverkörnyezetekhez optimalizált, kis teljesítményigényű változat, a fejlődő (ázsiai, dél-amerikai, illetve afrikai) országok számára – máshol nem is vásárolható meg.
- **Home Basic** – Otthoni használatra, csak az alapvető szolgáltatásokat tartalmazza, minimális hálózati, illetve vállalati támogatással. Az új grafikus felület szolgáltatásai közül csak az alapképességeket tartalmazza, ellenben egyaránt elérhető ebben a változatban is az Internet Explorer 7, a Windows Media Player 11, a Windows Movie Maker, és a megújult Windows Mail.
- **Home Premium** – A Vista otthoni, de emelt szintű környezetben javasolt változata, a teljes Aero grafikus felhasználói felület mellett a táblaszámítógépek komponenseit, illetve több multimédiás szolgáltatást is tartalmaz, melyeknek köszönhetően például teljes értékű házi Media Center PC varázsolható a számítógépből.
- **Business** – Kis- és középvállalatok számára optimalizált kiadás, képes tartományi környezetben működni, felügyelhető pl. RDP-vel, tartalmazza az EFS titkosítást, használja az árnyékmásolatok technológiát, és képes az új, lemezkép-alapú mentésre, azonban nem találhatók meg benne például az extra multimédiás szolgáltatások.
- **Enterprise** – A nagyvállalatok összes igényét kielégítő Enterprise csak mennyiségi licenc keretein belül hozzáférhető, a Business kiadáson túl támogatja a többnyelvű felhasználói felület kezelését, illetve a BitLocker technológiát, mellyel a teljes merevlemezt titkosíthatjuk – például üzleti adatokat tároló notebookok esetén. Ezzel a változattal az említett mennyiségi licensz birtokában 4 további virtuális gépet (pl. a VPC 2007-tel) futtathatunk, szintén Windows Vistával telepítve.
- **Ultimate** – Az Ultimate az összes változat minden képességét és extráját tartalmazza, azoknak ajánlják, akik nem kívánnak kompromisszumot kötni az egyes funkciók elérhetőségét illetően. Ezen felül e változat tulajdonosai folyamatosan számíthatnak (a Microsoft Update szolgáltatás használatával) teljes értékű, új alkalmazások és összetevők letöltésére is.

A Windows XP esetében főként a hálózati képességek – illetve azok hiánya – különböztette meg a Home és a Professional változatokat. A Home nem támogatta a Távoli asztal *(Remote Desktop)* kapcsolat lehetőséget, nem lehetett titkosítani a fájlrendszert, nem tartalmazta az Internet Information Services (IIS) web- és ftp-kiszolgálót, valamint – és ez volt gyakorlatilag a legnagyobb hátránya az üzemeltetés szempontjából – nem lehetett tartományba sem léptetni.

A Vista Home kiadásai az XP-hez hasonló módon különböznek az üzleti és az Ultimate változatoktól, a Tablet PC, illetve Media Center vonal azonban összeolvadt a hagyományos kiadásokkal, így ezek a funkciók a Home Premium, illetve Ultimate változatokban az alapcsomag részeként megtalálhatók.

A fenti hat variáción kívül az Európai Bizottság trösztellenes rendelkezéseinek értelmében a Microsoft köteles volt kiadni úgynevezett „**N**" változatokat is, melyek az alapcsomagban nem tartalmazzák pl. a Windows Media Player multimédiás lejátszóalkalmazást.

A Windows Vista telepítőcsomagja – a képfájl-alapú telepítőnek köszönhetően – mindegyik változatot tartalmazza, a telepítés során a megadott termékkulcs határozza meg, hogy melyik kiadás települ, illetve kulcs megadása nélkül bármelyik változatot futtathatjuk egy 30 napos próbaidőszak alatt. A Starter kivételével minden változat elérhető 32-, illetve 64-bites kiadásban is.

További részletes, magyar nyelvű információk az összetevőkről és változatok közötti különbségekről: *http://www.microsoft.com/hun/windows/products/windowsvista/editions/n/choose.mspx* vagy *http://tinyurl.com/2gtalb*.

Hardverigény

Míg a Windows XP már egy 300 MHz-es Pentium kategóriájú processzorral, illetve 64-128 MB memóriával is beéri (a rendszer használható sebességgel történő futtatásához persze ennél azért erősebb hardver szükséges), a Vista már alapesetben is több erőforrást követel. A Windows Vista hardverigénye:

	Minimum	Ajánlott	Premium Ready
CPU	800 MHz	1 GHz	1 GHz
RAM	512 MB	512 MB	1 GB
GPU	SVGA	DirectX	Aero képes
Video RAM			128 MB
HDD szabad hely	15 GB	15 GB	15 GB

A Windows Vista telepítéséhez tehát legalább 800 MHz órajelű processzorral, 512 MB memóriával (ez valós korlátozás, a telepítő leáll, ha kevesebb van) és – ha az új vizuális effekteket is látni akarjuk – DirectX 9-et hardveresen támogató, Pixel Shader 2.0-képes grafikus kártyával kell rendelkeznünk. Ezek természetesen csak a kötelező minimális feltételek, a rendszer használható sebességgel történő futtatásához, illetve a szolgáltatások maradéktalan kihasználásához ennél erősebb hardverre van szükség.

A Microsoft a számítógépek Vista alatt nyújtott teljesítményének könnyebb meghatározásának érdekében különböző jelzésekkel látta el a PC-konfigurációkat. Jelenleg kétfajta jelölés létezik, azaz a Vista Capable, illetve a Premium Ready:

- A *Vista Capable* matricával ellátott számítógépek képesek a rendszert alapvető funkcionalitással futtatni, de az egyes extrák kihasználásához már előfordulhat, hogy nem elegendő az erőforrásuk.
- A *Premium Ready* jelzésű konfigurációk az összes Vista-funkciót támogatják, vagyis ilyen gép vásárlásakor biztosak lehetünk benne, hogy egyetlen extráról sem kell lemondanunk, a PC maradéktalanul képes kiszolgálni a Vista igényeit.

Telepítési módszerek és előkészületek

A Vista általános telepítése többféle adathordozó, illetve módszer segítségével történhet:

- DVD lemezről – tipikusan ilyen hordozóval vásárolhatjuk meg.
- CD lemezekről – extra esetben (pl. MSDN vagy a TechNet előfizetés részeként), az .iso fájlokat letöltve és CD lemezre kiírva.
- USB-eszközökről – ehhez preparálni kell az adott eszközt, és a számítógép BIOS-ával szemben is vannak különböző elvárások.
- Frissítés korábbi Windows operációs rendszerről.
- Migráció régebbi Windows operációs rendszerekről, akár más célgépre is.

A speciális, elsősorban vállalati környezetben használt automatizált, illetve tömeges telepítéses módszerekről az alábbi címen olvashatunk többet: *http://technet.microsoft.com/en-us/desktopdeployment/default.aspx* vagy http://tinyurl.com/3255p6

Ha a Windows Vistát korábbi rendszerről frissítjük, ajánlatos igénybe venni a Windows Vista Upgrade Advisor segédprogramot, mely a hardver- és szoftverkörnyezet elemzésével ajánlásokat ad a frissítés menetét és az esetlegesen szükséges hardverbővítéseket vagy szoftverfrissítéseket illetően, valamint egy apró ismertetés is helyet kapott benne a Vista különböző változatainak különbségeiről.

A Windows Vista Upgrade Advisor a következő webcímről tölthető le: *http://www.microsoft.com/hun/windows/products/windowsvista/buyorupgrade/upgradeadvisor.mspx* vagy *http://tinyurl.com/yqxd4d.*

A Windows Vista Upgrade Advisor
Ebben a screencastban bemutatjuk a Windows Vista Upgrade Advisor működését és lehetőségeit.
Fájlnév: I-1-1a-Windows-Vista-Upgrade-Advisor.avi

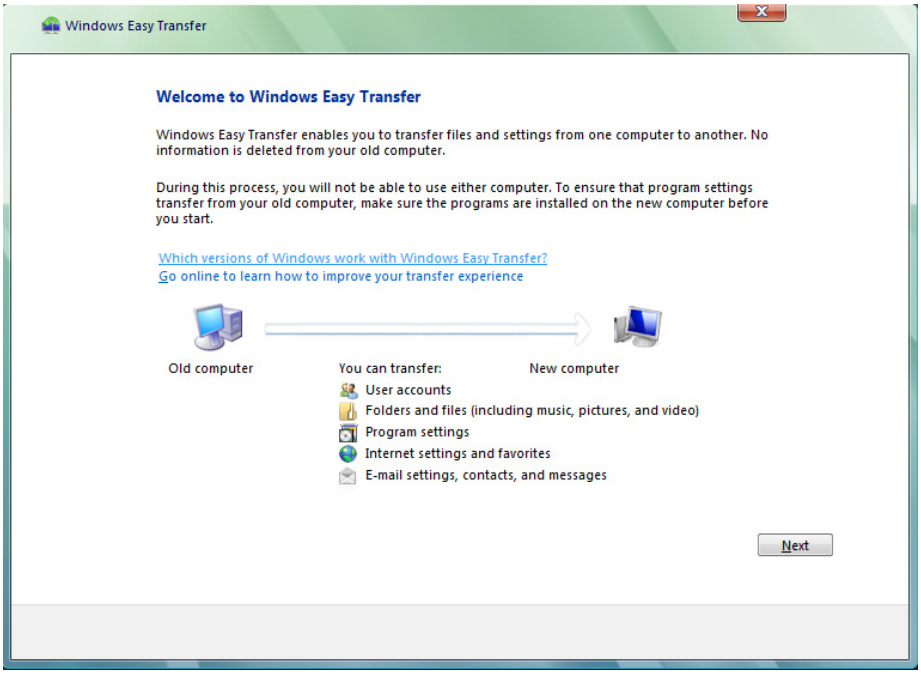
A Windows Vista korábbi verziókról történő frissítésének lehetőségeit az alábbi táblázaton láthatjuk (az X a lehetőséget jelenti).

	Home Basic	Home Premium	Business	Ultimate
XP Professional			X	X
XP Home	X	X	X	X
XP Media Center		X		X
XP Tablet PC			X	X
XP Professional x64				
Windows 2000 Professional				

Fiókok, fájlok és beállítások átvitele

Akár frissítésről, akár migrációról van szó, több lehetőségünk is van az előző operációs rendszer alatt működő felhasználói fiókjaink, rendszer-, illetve programbeállításaink, munkakörnyezetünk és adataink átvitelére a Windows Vista „alá". Ezek a megoldások természetesen használhatóak abban az esetben is, ha már Vistáról költözünk egy másik, Vistára és szükség van a korábbi környezet változatlan használatára. Az első eszköz, amelyet bemutatunk,

az a Vistában alapértelmezés szerint telepített, azaz bárki számára elérhető Windows Easy Transfer *(Windows Áttelepítő)*. Tipikusan a PC és PC közötti átvitelt támogatja, ajánlottan a munkacsoportban lévő otthoni számítógépek között. További fontos jellemzője, hogy extrém esetben szimpla felhasználóként (azaz a rendszergazda nélkül) is használható, az átvitelt a felhasználó által kezdeményezve.



1.2. ábra: *A Windows Easy Transfer sok esetben megfelelő eszköz lehet az adatok átvitelére*

Elsődleges célterülete a Windows XP, azonban képes a Windows 2000 Professional-ról is adatokat „áthúzni", viszont ebben az esetben a különböző program és rendszer beállítások átviteléről le kell mondanunk. A pontos használatához fontos tudni azt is, hogy az alkalmazások beállítása csak akkor történhet meg az új gépen, ha már feltelepítettük ezeket, tehát az eszköz az adott komponens telepítését nem, de a beállítását képes elvégezni.

A használata nem túlságosan bonyolult, ennek ellenére jól variálható lehetőségekkel rendelkezik. A régi gépen (pl. egy XP-n) is telepítenünk kell, de ha elérik egymást hálózatban a gépek, akkor még a Vistán a varázsló egyik lépésében magát a telepítőt is bemásolhatjuk egy megosztásba, tehát nem szükséges a DVD a használatához (persze CD-re, pendrive-ra is kiírja, ha kell). Az új gépen a varázsló utolsó lépésében még egy kulcsot is kapunk, amely a jelszó feladatát tölti be. Ha a Vistán végeztünk, akkor az XP-n elin-

dítva a telepítőt, szintén választhatunk, hogy az átvitel a hálózaton direktben vagy másolással, vagy hálózat nélkül, a CD/DVD/Pendrive trióból választva, vagy éppen egy speciális USB-kábellel végezzük el a műveletet.

Egy másik – kifejezetten haladóknak ajánlott – eszköz vagy inkább eszközcsomag az USMT (azaz a User State Migration Tool), amely a parancssorból működik, szkriptelhető, és távolról is elindítható, tehát megfelel a nagyobb, céges környezet elvárásainak. Két fő, és ezeken kívül még jó pár, a beállítását, finomhangolását igazán rugalmasan lehetővé tevő részekre osztható.

Az USMT használatának egyik legnagyobb előnye az automatizmus, amely egyaránt észrevehető a helyi és tartományi fiókok és profiljaik, a teljes környezet (beleértve az alkalmazások beállításait is) begyűjtésekor, illetve a „kiszórásakor is", mivel mindkét szakaszt elvégezhetjük a csoportházirend segítségével egyszerre akár tetszőleges számú gépen is, anélkül, hogy oda kellene fáradnunk a gépekhez.

Az USMT 3.0.1-es, jelenleg aktuális változata erről a címről tölthető le: *http://www.microsoft.com/downloads/details.aspx?FamilyID=799AB28C-691B-4B36-B7AD-6C604BE4C595&displaylang=en* vagy *http://tinyurl.com/23tuh8*.
További részletes információt pedig ezen a címen találhatunk (magyarul): *http://www.microsoft.com/hun/dl.aspx?id=7424c2fa-0970-45a9-9275-363269023edc* vagy *http://tinyurl.com/youlgt*.

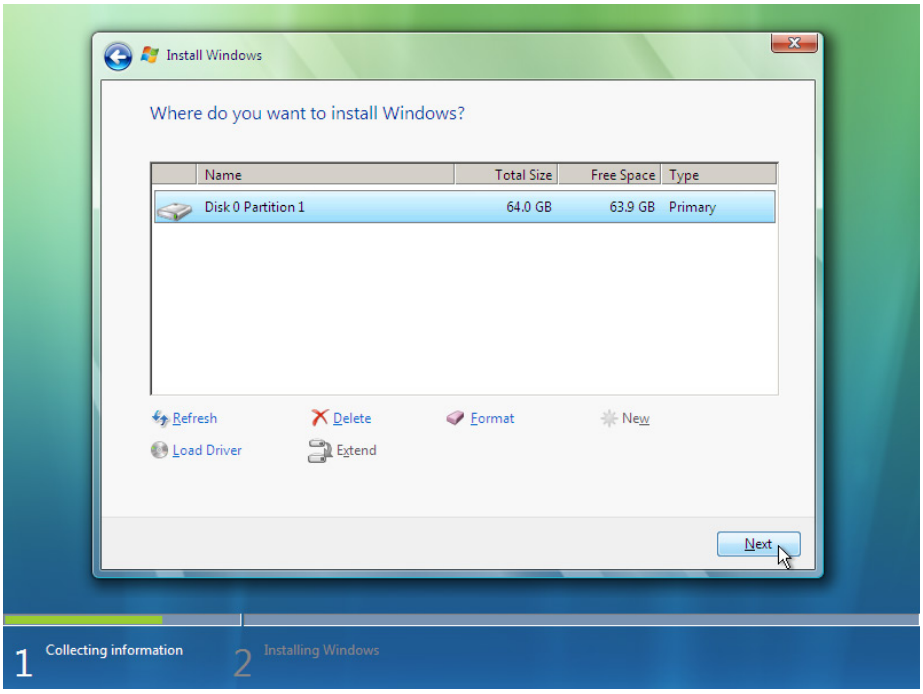
A telepítés folyamata

A Windows Vista teljesen megújult telepítési mechanizmussal érkezik, mely számos előnnyel rendelkezik a korábbiakhoz képest:

- Használható a dinamikus telepítés, azaz pl. a DVD-ről indított frissítő telepítés esetén a telepítő képes az internetről szervizcsomagokat, meghajtófrissítéseket és alkalmazásfrissítéseket is letölteni, így praktikusan biztonságosabbá és stabilabbá tenni az új operációs rendszer működését – már a telepítés közben is.
- A telepítőcsomag teljesen nyelvfüggetlen, ami azt jelenti, hogy a frissítések és bővítmények telepítéséhez többé nem kell, hogy egy adott nyelvi változattal rendelkezzünk, valamint szabadon hozzáadhatók, elvehetők a különböző nyelvi csomagok (akár a telepítés után is pl. a Windows Update segítségével).
- Számos új tömeges telepítési eszköz (WinPe, WSIM, BDD 2007, WDS) áll rendelkezésre, melyekkel a kisebb-nagyobb hálózatokban egyaránt egyszerűen és gyorsan telepíthetünk az egyes képállományokból a há-

lózaton keresztül. A telepítőkészlet komponensekre van bontva, így a rendszergazdák rendkívül részletesen szabhatják testre a telepíteni kívánt összetevőket. Az eszközmeghajtók és a termékfrissítések különböző Microsoft-eszközökkel integrálhatók a telepítőkészletbe.

Ezekről a bővített lehetőségekről a *http://technet.microsoft.com/en-us/desktopdeployment/default.aspx* vagy *http://tinyurl.com/3255p6* címen találunk további információt.



1.3. ábra: *Nőtt a telepítés közben használható a lemezeket, partíciókat érintő opciók száma*

A Vista telepítése alapjaiban elér az XP-étől. Maga a telepítőprogram egy speciális grafikus felülettel rendelkező előtelepítési környezetben fut, ahol a telepítés lehetősége mellett számos helyreállítási és diagnosztikai eszköz – például integrált memóriateszt – is rendelkezésünkre áll.

A telepítési források köre is nőtt, mostantól akár USB-eszközről is telepíthetjük a rendszert. A telepítés elkezdéséhez szükséges alapvető eszközmeghajtók (pl. SATA/RAID-vezérlők) betöltése is lehetségessé vált optikai lemezről vagy szintén más USB-eszközökről (kényelmesen, a telepítés egy adott pontján a háttértároló tallózásával), azaz az F6 billentyű + a kötelező floppylemez páros immár a múlté a Vista esetén.

A telepítés minimális emberi beavatkozást igényel, mindössze a regionális beállításokat, a célpartíciót és a termékkulcsot kell megadnunk, a telepítő az első körben minden másról gondoskodik. Az újraindítás után még szükség lesz némi interaktivitásra, azaz a szokásos adatok (felhasználónév, jelszó, gép neve, időzóna és pontos idő) megadására és beállítására, de gyakorlatilag ezzel minden teendő végére értünk, egy rövid (és automatikus) teljesítményvizsgálat után készen is vagyunk, nincs szükség tehát a hálózati beállításokra, a munkacsoport/tartomány kérdés eldöntésére, illetve pl. az azonnali regisztrálásra és aktiválásra.

A telepítőkészlet szinte teljesen számítógép típus független (természetesen a 32- és 64-bites platformokhoz külön telepítő jár), így a különböző hardverabsztrakciós réteggel (HAL – *Hardware Abstraction Layer)* rendelkező konfigurációkra is telepíthetünk ugyanabból a képfájlból. A Windows Vista viszont már csak a fejlett ACPI-szabványú energiagazdálkodást támogató PC-kre telepíthető.

Frissítés Windows Vistára, 1-2. rész
Ezekben a screencastokban egy Windows XP > Vindows Vista frissítés lépeseit követjük le, az XP-ről indulva, majd az újraindítás után egészen a telepítés végéig.
Fájlnév: I-1-1b-Frissites-Windows-Vistara-I.avi; I-1-1b-Frissites-Windows-Vistara-II.avi

Haladó beállítások a Windows Vista tiszta telepítésekor
Ebben a rövid bemutatóban a telepítés azon haladó részeire térünk ki, amelyek csak egy új telepítés esetén érhetőek el.
Fájlnév: I-1-1c-Windows-Vista-halado-telepites.avi

A Vista aktiválása

Akár tiszta telepítést, akár régebbi rendszerről történő frissítést végzünk, a telepítőprogram bekéri az adott Vista példányhoz tartozó product key-t *(termékazonosító kulcsot)*, telepítés után pedig aktiválnunk kell az operációs rendszert.

A korábbi verziókkal ellentétben a telepítéskor nem kötelező termékkulcsot megadni (ha nem adunk meg kulcsot, akkor bármelyik Vista kiadás telepítését kérhetjük), az érvényes kulcs bevitelére (és a termék aktiválására) harminc nap haladékot kaphatunk.

Az aktiválási folyamat során a termékazonosító kulcs és egy kódolt szám alapján létrejön az úgynevezett telepítési azonosító, amely egyedi módon azonosítja a számítógépet alkotó hardverelemeket. A számítógép aktiválásakor interneten vagy telefonon meg kell adnunk a Microsoftnak a telepítési azono-

sítót, ahol ezt ellenőrizve megerősítik, hogy a telepítés jogszerű volt. Ha valaki az aktiválás befejezése után megpróbálja az operációs rendszert ugyanazzal a termékkulccsal egy másik számítógépre telepíteni, a Microsoft adatbázisában tárolt azonosító jelzi, hogy ez a termékazonosító kulcs már hozzá van rendelve egy adott hardvercsoporthoz (számítógéphez), és az aktiválás sikertelen lesz. A telepítési azonosító csak a termék aktiválása céljából szükséges.

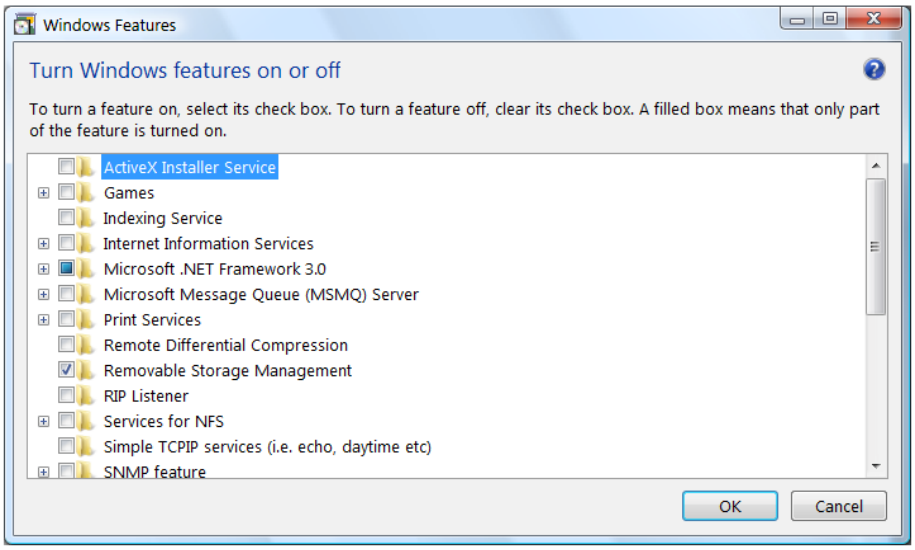
Ha a számítógépnek van internetkapcsolata, az aktiválást mindenképpen ennek felhasználásával célszerű elvégezni. A varázsló lehetővé teszi a telefonos aktiválást is, de ebben az esetben az 50 számjegyből álló telepítési azonosítót a telefon gombjainak segítségével kell megadnunk, és a válaszul kapott 42 jegyű aktiváló kód begépelése is fárasztó lehet.

Más a helyzet azonban, ha olyan számítógépről van szó, amelyet a Vista előtelepített változatával együtt OEM (Original Equipment Manufacturer) gyártótól vásároltunk. Tovább bonyolítja a helyzetet, hogy a legnagyobb OEM gyártókra a többiektől különböző szabályok vonatkoznak:

- A legnagyobb multinacionális számítógépgyártókat a Microsoft felhatalmazta arra, hogy a System Locked Preinstallation- (SLP – a m. *gyári előtelepítés)* technológia segítségével telepítsék, és aktivált állapotban szállítsák az operációs rendszert. A merevlemezre előtelepített (vagy a helyreállító DVD-k segítségével felmásolt) Vista a BIOS-t tartalmazó memóriamodulban tárolt egyedi információ alapján ellenőrzi a számítógép típusát, így nincs szükség külön aktiválásra. Ha ilyen számítógépet vásárolunk, a gép dobozára rá van ugyan ragasztva az eredetiséget igazoló matrica a Vista termékkulcsával, de az operációs rendszer **nem** ezzel a kulccsal van telepítve és aktiválva, mivel a gyártó egyetlen kulcs segítségével telepítheti és aktiválhatja a gépekhez szállított összes Vista példányt. Ha a géphez tartozó helyreállító DVD segítségével telepítjük újra a gépet, akkor nincs szükség aktiválásra (sőt még termékkulcsot sem kell megadnunk!), egészen addig, amíg a gépben az eredeti alaplap (illetve BIOS) van.
- A kisebb számítógépgyártók szintén adhatnak előtelepített operációs rendszert gépeikhez, de ez egy másik OEM változat, így ebben az esetben szükség van az aktiválásra. A gyártókra vonatkozó szabályok szerint a felhasználóknak a gép első bekapcsolásakor meg kell adniuk a gépre ragasztott matrican szereplő termékkulcsot és el kell fogadniuk a licencszerződést, majd a szokásos harminc napon belül aktiválniuk kell a Vista példányt. Újratelepítéskor természetesen újra be kell gépelni a termékkulcsot és el kell végezni az aktiválást is.

Komponensek hozzáadása, illetve elvétele

Ha egyszer már „él” a rendszerünk, ismerkedjünk meg a választható összetevőkkel akár azért, hogy bővítsük a rendszer képességeit, akár azért, hogy némiképp lecsupaszítsuk a számunkra szükségtelen komponensektől. A Windows Vistában az eddigi Add/Remove Programs *(Programok hozzáadása/eltávolítása)* lehetőség is megváltozott, a nevében is és az összetevők mennyiségét tekintve is. Mostantól Turn Windows Features on or off *(Windows-szolgáltatások be- és kikapcsolása)* néven találjuk meg a vezérlőpulton, a Programs and Features *(Programok és szolgáltatások)* csoportban.

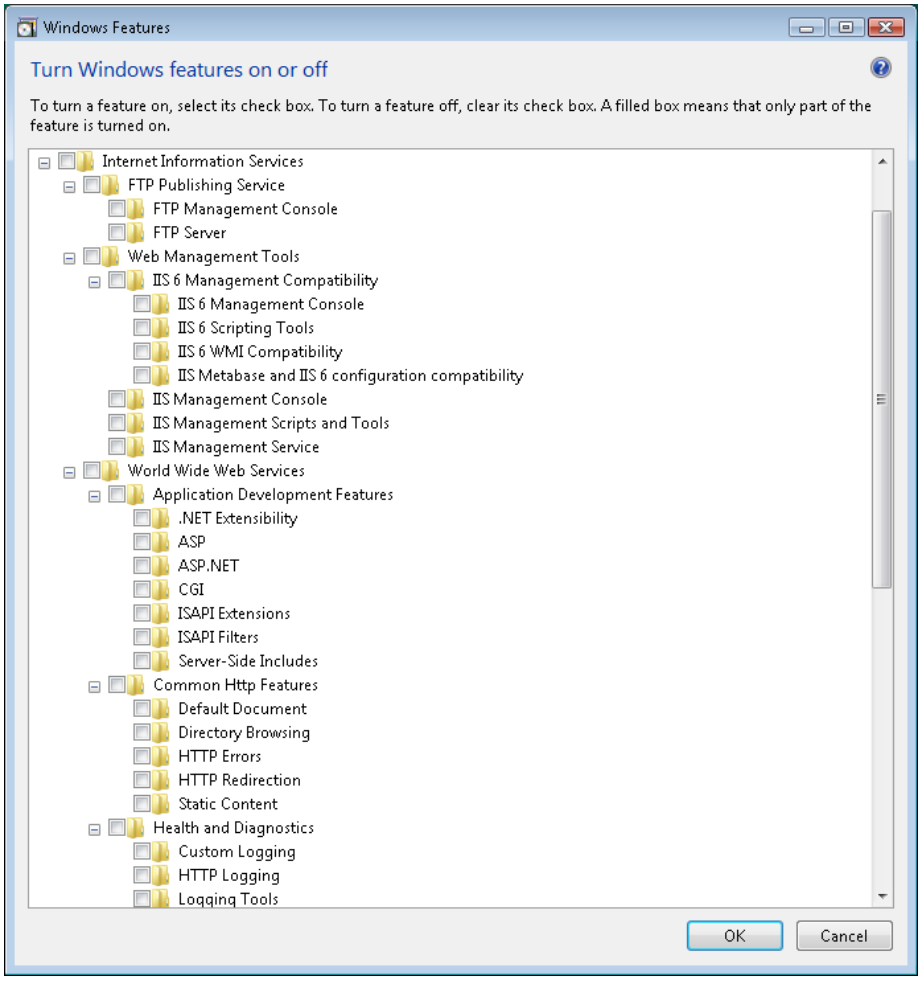


1.4. ábra: *A komponensek hozzáadása/elvétele itt történik*

Az XP komponenseit ismerők számára lesz jó néhány meglepetés, nézzük most át tehát a feltelepíthető / eltávolítható összetevőket.

- **ActiveX Installer Service** *(ActiveX-telepítő szolgáltatás)* – Ezzel a komponenssel lehetőséget adunk a standard felhasználóknak arra, hogy ActiveX vezérlőket telepítsenek. A legtöbb esetben erre a nyilvánvaló biztonsági kockázat miatt nincs szükség, vállalati környezetben viszont előfordulhat, azonban ekkor a Csoportházirend segítségével behatárolhatjuk a hozzáadandó ActiveX vezérlők forrását.
- **Games** *(Játékok)* – Kilenc különböző játékot találunk ebben a kategóriában, és alapesetben mindegyik telepítve van.

- **Indexing Service** *(Indexelő szolgáltatás)* – A visszafelé kompatibilitás miatt van lehetőségünk a régi fájlindexelő szolgáltatás telepítésére is, de ennek hiányosságai miatt valóban csak indokolt esetben tegyük meg.



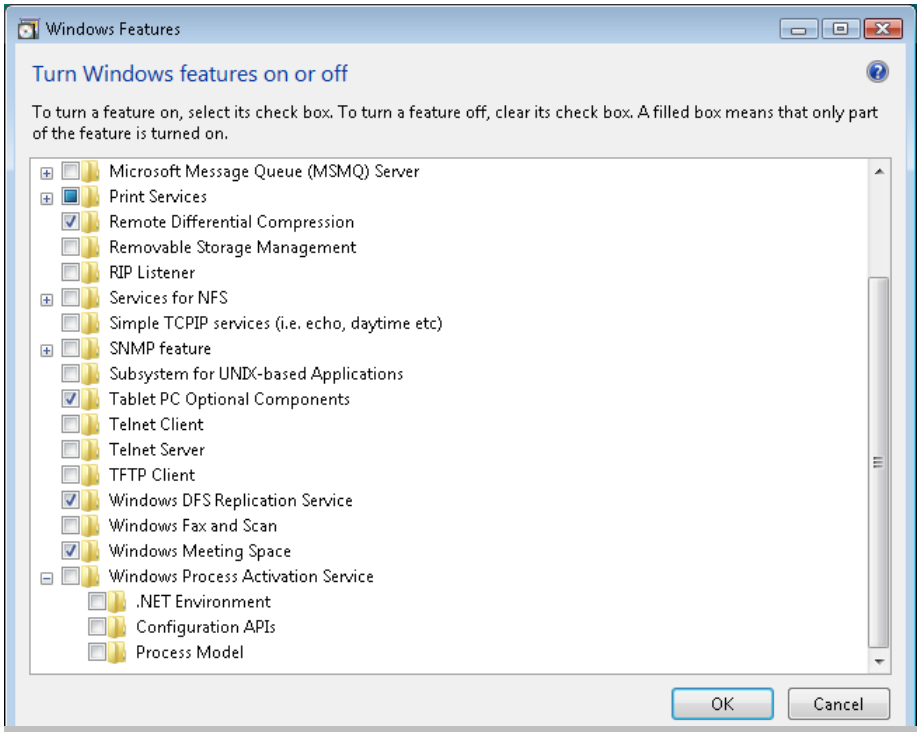
1.5. ábra: *Az IIS modularitása a szolgáltatások telepítésekor is jól látható*

- **Internet Information Services** – Az ügyfélbe épített web- és alkalmazáskiszolgáló új, 7.0-ás változatát is használhatjuk. Alapesetben sem a különböző (ugyanis a 6.0-ás IIS-hez tartozóak is rendelkezésre állnak) felügyeleti eszközök, sem a web-, vagy az FTP-szerver nincs telepítve. Fontos tudni, hogy az ügyfélgépen futó IIS elsősorban a tesztelők, programozók számára fontos és praktikus, más esetekben az IIS szolgáltatásai célszerűen a kiszolgálókon használjuk. Ha viszont meg-

vizsgáljuk az ebben a csoportban hozzáadható elemeket, látni fogjuk az IIS7 egyik legfontosabb tulajdonságát, az egészen elképesztő szintű modularitást, amely a következő képen is jól látható.

- **Microsoft .NET Framework 3.0** – A Microsoft .NET Framework 3.0 használatával fejlesztett alkalmazások apropóján lehet szükségünk rá. A Vistának része a 2.0-ás verzió is, amennyiben viszont ennél korábbi változatra van szükség, akkor ezeket külön telepítenünk kell. Az egyik alkomponens egyébként már része alapértelmezés szerint is a rendszernek, ez az XPS Viewer, azaz az új, a képernyőn és a nyomtatásban is ugyanazt a külcsínt nyújtó dokumentum formátum olvasóprogramja.
- **Microsoft Message Queue (MSMQ) Server** *[Microsoft üzenetvárólista- (MSMQ-) kiszolgáló]* – A gépünkből MSMQ-kiszolgálót faraghatunk e komponens telepítésével, amely az alkalmazások közötti garantált üzenetküldést valósítja meg, azaz a fogadó alkalmazás inaktív állapota esetén eltárolja a küldeményt, és kézbesíti annak elindulásakor. Csak speciális esetekben szükséges.
- **Print Services** (*Nyomtatószolgáltatások)* – Speciális (http-, Vax és Unix) nyomtatókhoz, nyomtatási sorokhoz történő csatlakozáskor szükséges. A hagyományos nyomtatókezeléshez és megosztáshoz nem szükséges.
- **Remote Differential Compression** *(Távoli különbözeti tömörítés)* – Gépek közötti fájlátvitelkor a sávszélesség optimalizálása és ezzel az átvitel sebességének növelése miatt érdemes használni ezt az új, a Windows Server 2003 R2-ben bemutatott speciális tömörítési algoritmust. Működésének lényege az, hogy egy a túloldalon már létező fájl módosítása és újbóli átvitele esetén csak az adott fájlban történt változások replikálódnak, ami akár drasztikus méretű átviteli sebesség növekedéssel is járhat.
- **Removable Storage Management** *(Cserélhető tároló kezelése)* – Az eltávolítható, mentéshez kapcsolódó cserélhető médiák (pl. szalagos egység) és a hozzájuk tartozó katalógusok kezelője. Ha nincs ilyen eszközünk, akkor nem szükséges.
- **RIP Listener** *(RIP-figyelő)* – Ez a komponens a RIPv1 (Routing Information Protocol 1) útvonalválasztási protokollt használó routerektől érkező útvonal frissítéseket figyeli.
- **Services for NFS** *(NFS szolgáltatások)* – A Network File System, azaz a UNIX/Linux operációs rendszerekben használt fájlrendszer hálózati elérése, illetve a saját megosztásaink publikálása ezen operációs rendszert használó gépek felől, illetve felé.

- **Simple TCPIP services (i.e. echo, daytime etc.)** *(Egyszerű TCP/IP-szolgáltatások)* – A korábbi operációs rendszerekből ismerős komponens, néhány alap TCP/IP- szolgáltatást (echo, daytime, quote, chargen, discard) használhatunk, ha telepítjük.
- **SNMP feature** *(SNMP-funkció)* – Telepítése után a gépünk tartalmaz majd egy SNMP-ügynököt, amely a különböző hálózati szolgáltatások ügyfele lehet, azaz láthatóvá válik a hálózatfelderítésre ezt a protokollt használó kiszolgáló szoftverek, illetve hardver eszközök számára. Ennek megfelelően csak indokolt esetben telepítsük.
- **Subsystem for UNIX-based Applications** *(Alrendszer a UNIX-alapú szolgáltatások számára)* – UNIX alapú alkalmazások és szkriptek futtatásához lehet szükséges ez az összetevő. Korábban csak külön letöltéssel volt elérhető.
- **Tablet PC Optional Components** *(Táblaszámítógép választható összetevői)* – Mivel praktikus okokból nincs külön operációs rendszer változat a táblaszámítógépekre (a Windows XP-nél még volt), ezért a kifejezetten az ilyen típusú hardveren használható funkciók e választható komponensen keresztül érhetőek el. Alapesetben ezek a szolgáltatások telepítve vannak, de szükség esetén egyszerűen eltávolíthatóak.
- **Telnet Client** *(Telnetügyfél)* – Szintén biztonsági okokból az eddig integrált, parancssori telnetügyfél immár nem érhető el az alapértelmezett telepítés részeként, a használatához külön kérnünk kell a telepítését.
- **Telnet Server** *(Telnetkiszolgáló)* – Ha valamilyen különleges okból a gépünkből telnetkiszolgálót szeretnénk faragni, akkor ezt a szolgáltatást szintén külön kell telepíteni. A telnetkiszolgáló működéséhez a telepítés után a Windows tűzfalban a megfelelő portot (TCP 21) ki kell nyitnunk. Létjogosultságát ma már nehéz elképzelni, és ennek megfelelően nem is ajánlott ennek a szolgáltatásnak a használata, de ha mégis szükséges, itt tudjuk engedélyezni.
- **TFTP Client** *(TFTP-ügyfél)* – A TFTP az FTP-hez hasonló protokoll, de lényegesen egyszerűbb módon működik, pl. a TCP helyett a kevésbé igényes, és kevésbé ellenőrzött UDP protokollal. A Vista TFTP-ügyfél parancssorból használható, és általában a hálózati eszközeink konfigurációjának, illetve a firmware-eknek a mentésére használjuk.



1.6. ábra: *A telnetügyfelet telepítenünk kell, ha szükségünk van rá*

- **Windows DFS Replication Service** *(Windows DFS-replikációs szolgáltatás)* – Olyan fájlreplikációs szolgáltatásról van szó, amely támogatja a számítógépek közötti gyors és praktikus fájlszinkronizációt. Több új, innovatív megoldás mellett a korábban említett Remote Differential Compression komponenst is tartalmazza.
- **Windows Fax and Scan** *(Windows faxoló és képolvasó)* – Egy előzetesen telepített modemen keresztül vagy egy hálózati faxszerverhez csatlakozva engedélyezi a faxolást közvetlenül az operációs rendszerből. Emellett a lapolvasók használatát is egyszerűbbé teszi, azaz a telepítése után létrehoz egy központi helyet, ahol lehetővé válik a beolvasott anyagok tárolása, és értelemszerűen együttműködik pl. a Photo Gallery alkalmazással is például a képolvasást tekintve.

- **Windows Meeting Space** *(Windows Tárgyaló)* – Ha telepítjük ezt a komponenst, megbeszélések összehívására és lebonyolítására, ezen belül dokumentumok és pl. az Asztalunk megosztására és közös használatára lesz lehetőségünk. A helyes működéséhez szükséges a fájlreplikációs komponens, a People Near Me *(Asztaltársaság*, huhh :D) alkalmazás, illetve a vonatkozó tűzfalszabályok legyártása is.
- **Windows Process Activation Service** *(Windows folyamataktiválási szolgáltatás)* – Ez az elsősorban a programozók számára érdekes komponens felel azoknak a munkafolyamatoknak a teljes életciklusáért, amelyek a .NET 3.0 részeként elérhető WCF-et (Windows Communication Foundation) használó alkalmazásokat futtatnak.

Végül, de nem utolsósorban meg kell említenünk a Windows Ultimate Extras *(Windows Ultimate extrák)* összetevőt, amely egy teljesen új szolgáltatás formájában lehetővé teszi (de csak kizárólag az Ultimate változat tulajdonosainak), hogy a Microsoft Update segítségével teljes értékű alkalmazásokat töltsenek le, többféle kategóriában, a rendszerszoftverektől kezdve egészen a szórakoztató alkalmazásokig.

Komponensek áttekintése, hozzáadása, elvétele
Ebben a screencastban a Vistához adható/elvehető komponenseket tekintjük át.
Fájlnév: I-1-1d-Komponensek.avi

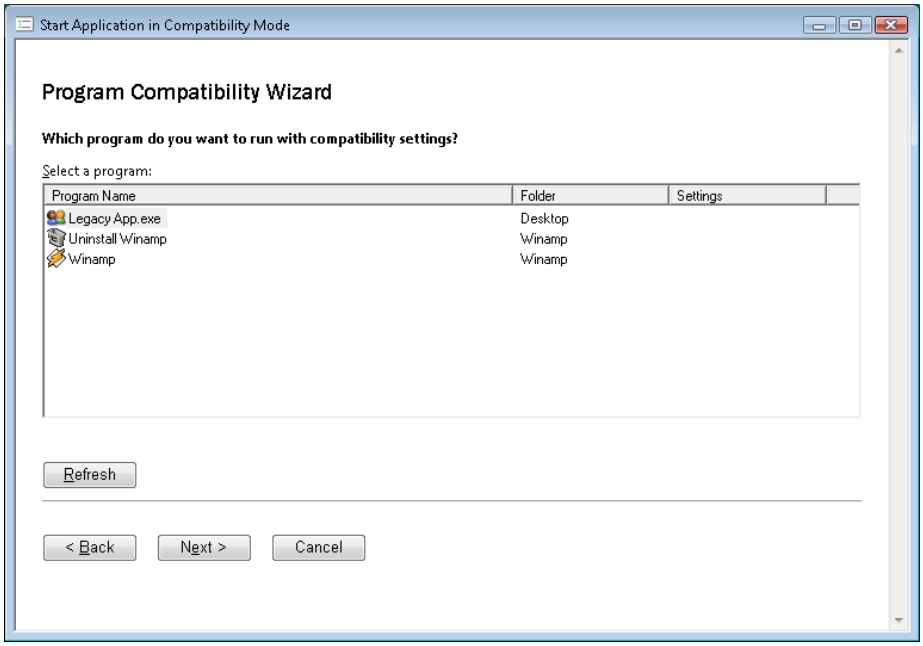
Az alkalmazás kompatibilitás eszközei

Az alkalmazásaink tökéletes, minden igényt kielégítő futtatása az összes létező operációs rendszeren nehéz, ha nem inkább kivitelezhetetlen feladat. Egy új operációs rendszer sokszor feláldozza az új szolgáltatások, technológiák alkalmazásának oltárán a visszafelé kompatibilitást, amely egy régi, akár tizenéves alkalmazás apropóján teljesen érthető következmény. Egészen nagy bizonyossággal állítható, hogy a Windows Vista alatt a Windows XP-vel működő alkalmazások is működnek, illetve az is, hogy a Vista az összes eddigi operációs rendszernél jobban kompatibilis a régi alkalmazásokkal, viszont néhánnyal esetleg mégis gond lehet. Ezen a problémán a Vista kétféle eszközzel próbál segíteni.

A kompatibilitásban sokat segít a Vista fájl- és registryvirtualizációs megoldása, amelyről a 3. fejezetben olvashatunk további részleteket.

Az egyik az ún. Programkompatibilitási segéd *(Program Compatibility Assistant, PCA)*, azaz a Vista automatikus szolgáltatása, amely akkor fut, ha egy régebbi, kompatibilitási problémákkal rendelkező programot észlel. Miután viszont egy régebbi programot már futtatott a Vista alatt, a segédeszköz értesítést küld, ha probléma merül fel, és felajánlja, hogy a program következő futtatásakor kijavítja azt. Ha a kompatibilitási probléma súlyos, a Programkompatibilitási segéd figyelmeztetést küldhet, vagy akár le is állíthatja a programot. A Programkompatibilitás segéd egyébként (pl. vállalati környezetben) a csoportházirend segítségével ki/be kapcsolható.

A másik megoldás, a Programkompatibilitás varázsló *(Program Compatibility Wizard)*, amely manuálisan indítható és beállításaiban már ismerős lehet a Windows XP-t használók számára, viszont némiképp kiegészült új opciókkal is. Ez az eszköz szintén használható az esetleges problémás alkalmazások megkeresésére, majd program kompatibilitási beállítások módosítására.



1.7. ábra: *A kompatibilitási varázsló keres és talál*

A rendszerismere alapjai

A rendszergazdák és a haladó ismeretekkel rendelkező felhasználók számára egy új operációs rendszerben sosem a külcsín az igazán a fontos, hanem sokkal inkább a belbecs. A kulcskérdések elsősorban a kezelésre, a felügyeletre, az esetleges problémák forrásának megtekintésére és megoldására vonatkoznak. A Windows Vistában számtalan szolgáltatás és technológia adott az üzemeltetők feladatainak könnyebbé tétele, illetve praktikus kiszolgálása területén, amelyek közül persze néhány már ismerős lesz a Windows XP-ből. De bizton állíthatjuk, hogy rengeteg új vagy teljesen újraírt eszköz és szolgáltatás használatát is el kell sajátítanunk, ha a feladataink közé fog tartozni a Vista operációs rendszerrel működő számítógépek felügyelete. Első lépésben kezdjük a sort a többnyire már ismerős alapvető felügyeleti eszközökkel és ismeretekkel, amelyeket a második fejezetben ki fogunk egészíteni a haladó megoldásokkal is.

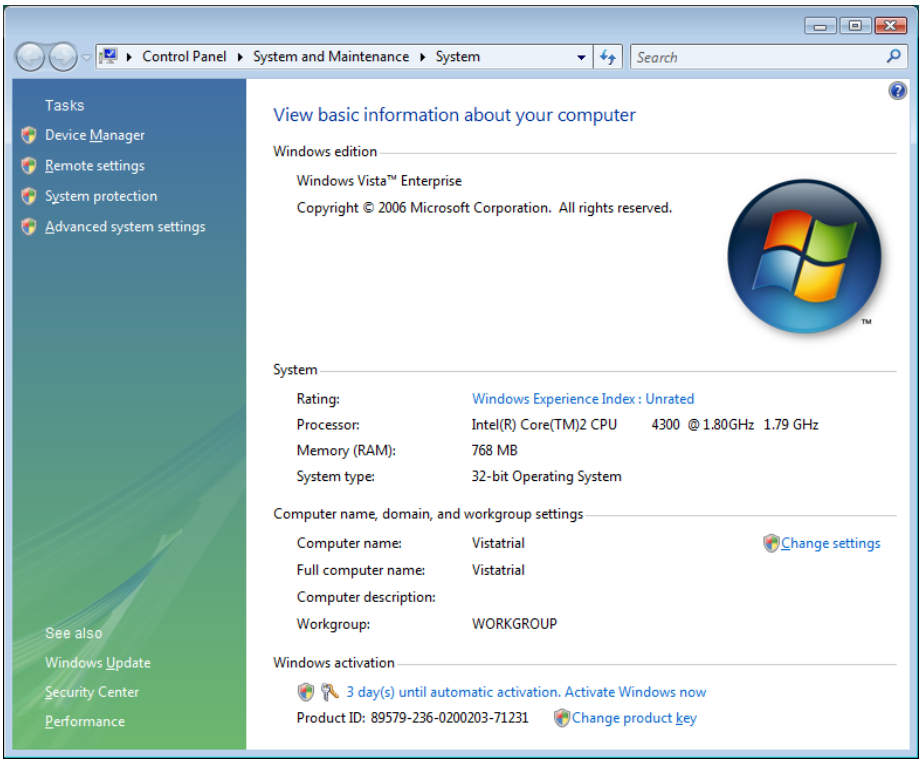
A Rendszer panel részletei

Számítógépünk legfontosabb alapadatait a korábbi Windows verziókhoz hasonlóan a Control Panel *(Vezérlőpult)* System *(Rendszer)* ablakának megnyitásával jeleníthetjük meg. A rendszerre vonatkozó alapvető információk (például a processzor típusa, memória mennyisége stb.) mellett itt találhatjuk meg például a Windows Experience Index *(Windows élményindex)* értékét is. Az index annak jelzésére szolgál, hogy az adott számítógépen a Vista mely szolgáltatásai lesznek használhatók. Az index számítását, vagyis az egyes hardverkomponensekkel (processzor, memória, grafikus kártya, merevlemez) kapcsolatos teljesítménymérést a telepítő program automatikusan elvégzi a telepítés végén, de kézzel mi magunk is bármikor új értékelést kérhetünk. Minden egyes hardverelemhez külön teljesítményérték tartozik (ezeket meg is jeleníthetjük a hivatkozásra való kattintással), az összesített index azonban nem ezek átlaga, hanem az egyes értékek közül a legkisebb. Ha a számítógépben kicseréljük valamelyik hardverelemet, akkor újra kell futtatnunk az index számítását, hogy a frissített értéket jeleníthessük meg.

A következő szakaszban a számítógép nevét, és a munkacsoporttal, illetve tartománnyal kapcsolatos adatokat találhatjuk meg, és ezeket a megfelelő jogosultság birtokában meg is változtathatjuk (lásd később).

Az ablak alsó részén láthatóak a Vista aktiválási állapotára vonatkozó adatok. Ha a telepítés közben engedélyeztük ezt a lehetőséget, és megadtuk a szükséges termékkulcsot, akkor az internetes aktiválás teljesen automatikusan is végbemehet, de az itt található hivatkozás segítségével magunk is bármikor kezdeményezhetjük azt.

A korábbi Windows verziókkal ellentétben a Vista lehetőséget nyújt a product key *(termékkulcs)* megváltoztatására is, de ebben az esetben a módosítás után természetesen újra kell aktiválnunk a Vista példányt.



1.8. ábra: *A Vista rendszer alapadatai*

Az ablak bal oldalán néhány fontos rendszerbeállítás módosítására szolgáló hivatkozást is megtalálhatunk. Itt érhetőek el azok a beállítólapok is, amelyek a Windows korábbi verzióiban a Control Panel *(Vezérlőpult)*/ System *(Rendszer)* ablakában jelentek meg.

- **Device Manager** *(Eszközkezelő)* – segítségével módosíthatjuk a különféle hardvereszközök beállításait és frissíthetjük a hozzájuk tartozó illesztőprogramokat. (A Device Managert elérhetjük a *devmgmt.msc* parancs begépelésével is.)
- **Remote settings** *(Távoli beállítások)* – itt módosíthatjuk a Távoli asztal *(Remote Desktop)* beállításait, vagyis engedélyezhetjük, illetve tilthatjuk a terminálszolgáltatásokhoz való kapcsolódást, és itt adhatjuk meg a távoli segítségnyújtásra vonatkozó beállításokat is.

- **System protection** *(Rendszervédelem)* – Innen érhetjük el a visszaállítási pontok *(Restore points)* automatikus létrehozására vonatkozó beállításokat (a visszaállítási pontok kezelésével kapcsolatos tudnivalók a „Mentés és visszaállítás" szakaszban részletesen foglalkozunk).
- **Advanced system settings** *(Speciális rendszerbeállítások)* – Itt érhetjük el a Vista rendszerteljesítménnyel kapcsolatos speciális beállításait, amelyek segítségével engedélyezhetjük, illetve tilthatjuk bizonyos képi elemek és speciális effektusok (áttűnések, áttetszőség stb.) használatát. Ugyanitt találjuk meg a felhasználók profiljaival és a rendszerindítással kapcsolatos beállításokat, és a virtuális memória beállítási lehetőségeit is.

Alap rendszerfelügyeleti eszközök (System and Maintenance, System Properties)
Ebben az előadásban a legfőbb rendszertulajdonságok részletes áttekintése történik meg.
Fájlnév: I-1-2a-System.avi

Fiók specifikus mappák és megosztások

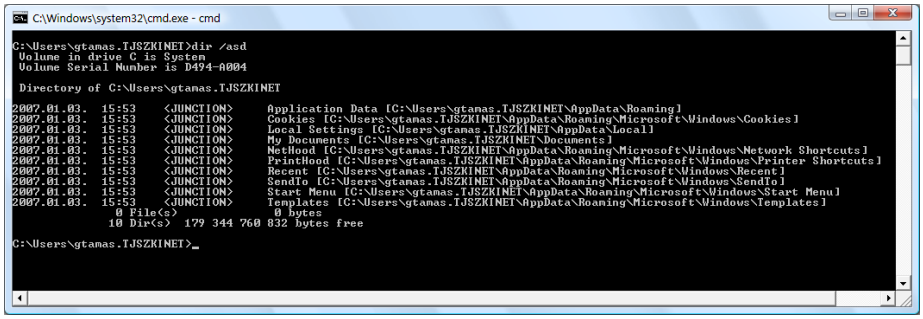
A felhasználók munkakörnyezetét meghatározó fájlok és beállítások a felhasználói profilban tárolódnak. Alapértelmezés szerint itt találhatjuk meg a felhasználók dokumentumait és egyéb adatfájljait, a felhasználóhoz tartozó, fájlként tárolt registrybeállításokat, és az alkalmazások különféle konfigurációs fájljait is.

Alapértelmezés szerint minden, a számítógépre bejelentkező felhasználónak helyben tárolt profilja van, amely az első bejelentkezéskor jön létre. A helyi felhasználói profilok tárolóhelye a *%Systemdrive%\Users* mappa.

A százalékkal jelölt környezeti változókat a *(Sajátgép \ Tulajdonságok \ Speciális \ Környezeti változók)* panelen találjuk meg, de a **set** paranccsal is lekérdezhetjük az értékeiket.

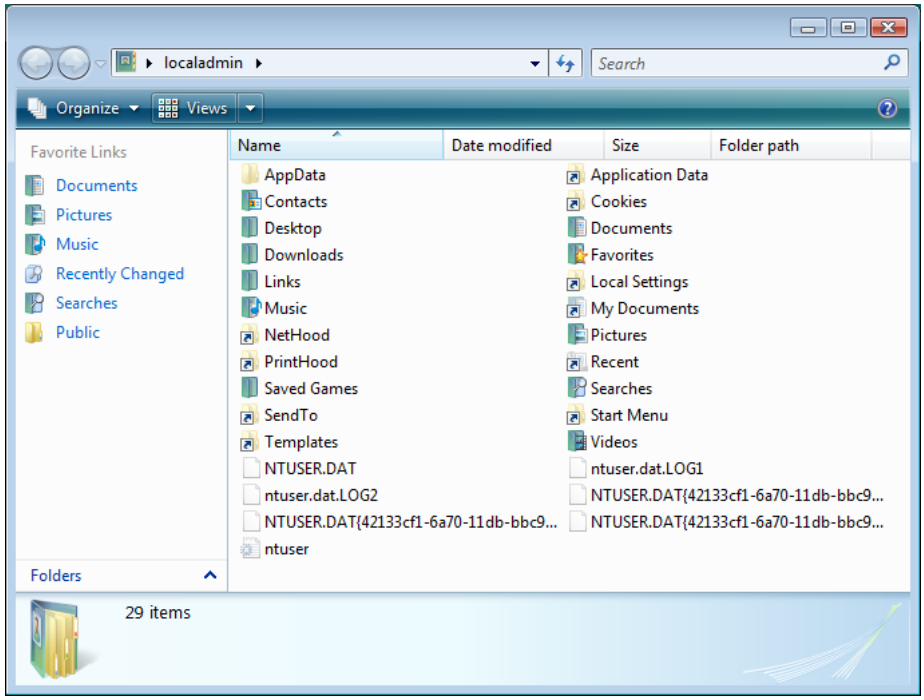
Ezen belül az egyes felhasználók adatai a felhasználónév alapján elnevezett mappákban találhatók meg (például *C:\Users\GipszJ).* A felhasználói profilon belül számos mappát találhatunk, amit az az 1.9. ábrán is látható. Ugyanitt találhatjuk meg az *Ntuser.dat* nevű (rejtett) fájlt is, amely a registrynek a felhasználóra vonatkozó részét, vagyis a *CurrentUser* ágat tárolja. A profilmappában találhatunk még számos rejtett hivatkozást (például a *NetHood, PrintHood, SendTo* stb.), amelyek a régebbi, a Windows XP-profilmappa szerkezetéhez készített alkalmazások működését biztosítják. A rendszerpartíción egyébként megtalálhatjuk a korábban a profilok tárolására használt

Documents and Settings mappát is, de jó ha tudjuk, hogy ez csak egy szimbolikus hivatkozás (ún. junction point, azaz az NTFS speciális megoldása a hivatkozásra) a *Users* mappára, azaz tartalma nincs is.



1.9. ábra: *A dir /asd paranccsal szépen látszanak az NTFS hivatkozások*

Sokkal barátságosabban fest a profilmappa, ha kikapcsoljuk (illetve nem kapcsoljuk be) a rejtett elemek megjelenítését. Ebben az esetben a mappában tizenegy almappa jelenik meg, amelyek mindegyike a különféle típushoz tartozó felhasználói adatok tárolására szolgál.



1.10. ábra: *A felhasználói profil mappái*

A mappák némelyikével már a Windows XP-ben is találkozhattunk [Documents *(Dokumentumok)*, Favorites *(Kedvencek)*, Music *(Zene)*, Pictures *(Képek)*, Videos *(Videók)*], csak a nevük változott kissé, és az elrendezésük vált logikusabbá (a képek, zenék stb. már nem a Documents mappán belül vannak). A többi mappa teljesen új, a felhasználók ezekben tárolhatják például az internetről letöltött fájljaikat, névjegyeiket vagy kereséseiket.

Az ablak bal oldalán a Links *(Kedvenc hivatkozások)* mappa tartalma jelenik meg, ide érdemes felvenni a gyakran használt helyek hivatkozásait, így azok mindig kéznél vannak, vagyis nagyon gyorsan és könnyen elérhetők.

A szokásos mappák mellett a felhasználói profil számos rejtett elemet is tartalmaz: találhatunk itt néhány registryfájlt az AppData mappát, és a Windows XP-vel való kompatibilitás miatt több rejtett hivatkozást is.

Közös profilok

A felhasználók önálló profilmappái mellett két közös profilt is találhatunk a Users mappában:

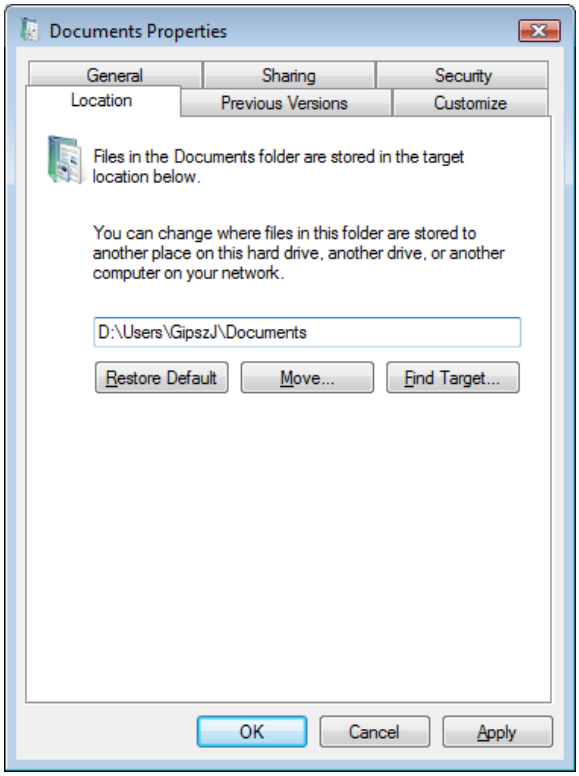
- **Public** *(nyilvános)* **profil** – az itt található Desktop *(Asztal)* és Start Menu mappák tartalma valamennyi felhasználó profiljában megjelenik, így alakul ki az egyes felhasználók Asztala és Start menüje. A Public többi mappájának [Documents *(Dokumentumok),* Pictures *(Képek),* Music *(Zene)* stb.] tartalmát valamennyi felhasználó elérheti, vagyis ezek a megosztott dokumentumok és egyéb fájlok tárolására használhatók.
- **Default** *(alapértelmezett)* **profil** – amikor egy adott felhasználó első alkalommal jelentkezik be egy számítógépre, létrejön a felhasználóhoz tartozó profilmappa, amelybe a Windows átmásolja a Default profil tartalmát (ha nem használunk központilag tárolt *(roaming)* profilt). A Default profil tehát a felhasználói profilok sablonjául szolgál, az itt elvégzett változtatások valamennyi később létrejövő felhasználói profilban érvényesülni fognak. Jól használható például az a módszer, hogy egy megfelelően testreszabott felhasználói profilt egyszerűen bemásolunk a Default mappába (a felhasználói profilok másolására a rendszer tulajdonságpaneljének Advanced system settings *(Speciális rendszerbeállítások)* lapján van lehetőség), ezután valamennyi új profil ennek megfelelően fog elkészülni.

A személyes mappák áthelyezése

Bár a személyes mappák struktúrája sokkal áttekinthetőbbé és logikusabbá vált a Windows XP-vel összehasonlítva, mégis sok esetben szükség lehet egyes mappák, vagy akár a teljes struktúra áthelyezésére. Ha például a rendszerköteten nincs elegendő hely a felhasználó filmgyűjteménye számára, akkor célszerű lehet másik kötetre áthelyezni a Videos *(Videók)* mappát.

A tárhellyel kapcsolatos problémákon kívül számos más érv is szól a rendszer- és a felhasználói adatok külön kötetre helyezése mellett:

- Az operációs rendszer és a személyes adatfájlok szétválasztása sokkal egyszerűbbé teszi a rendszer helyreállítását különféle problémák (fájlsérülés, vírustámadás stb.) estén.



1.11. ábra: *A mappák tulajdonságlapján megnézhetjük és módosíthatjuk a felhasználói mappák valódi helyét*

- A személyes adatok külön kötetre helyezése jelentősen megkönnyíti és hatékonyabbá teszi a különféle disk image- *(lemezkép-)* alapú mentési szoftverek (például a Vista beépített Complete PC Backup programja,

lásd később) használatát. Ebben az esetben a rendszerről készített image lényegesen kisebb lehet, a visszaállítás pedig egyáltalán nem érinti a felhasználók fájljait.

- Jóval egyszerűbben elvégezhető ebben az esetben az operációs rendszer újratelepítése, új verzióra történő frissítése, vagy akár teljes cseréje is (másik operációs rendszerre).

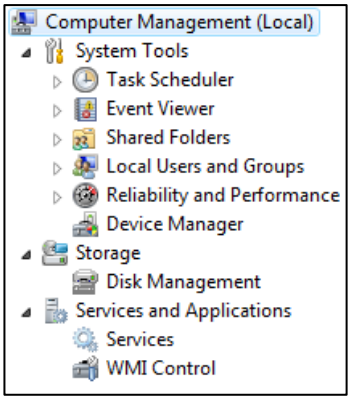
A személyes mappák áthelyezése nagyon egyszerű: az áthelyezendő mappa tulajdonságpaneljének Location *(Hely)* lapján kell módosítanunk az útvonalat. A Dokumentumok mappát például úgy helyezhetjük át, hogy a *C:\Users\GipszJ\Documents* útvonalban a „C" helyére egyszerűen beírjuk a megfelelő meghajtó betűjelét. Ezután a Vista rákérdez az új mappa létrehozására, (ha még nem létezett), majd arra is, hogy a fájlokat is át szeretnénk-e helyezni a régi helyről az újra. Nehéz olyasmit elképzelni, ami a két párhuzamos mappa indokául szolgálhatna, így természetesen mindig helyezzük át a tartalmat is.

Ha egyszerre több (esetleg valamennyi) adatmappát át szeretnénk helyezni, akkor célszerűbb más módszert választani. Hozzuk létre a felhasználói mappákat tároló új mappát (például *D:\Users\GipszJ),* majd jelöljük ki az áthelyezendő mappákat és az egér jobb gombjával húzzuk (ne másoljunk, hanem inkább mozgassunk) át őket az új helyre. A művelet közben a Vista módosítani fogja a megfelelő hivatkozásokat is.

A mappák áthelyezése után célszerű még egy műveletet elvégezni: nem árt, ha módosítjuk a Vista keresőmotorjának indexelésre vonatkozó beállításait, vagyis az új helyet is hozzáadjuk az indexelendő mappák listájához. A lista alapértelmezés szerint tartalmazza az eredeti profilmappát, de az áthelyezéskor ez nem változik meg automatikusan. (Az indexelésre vonatkozó beállításokat többek között a Control Panel *(Vezérlőpult)* Performance Information and Tools *(Teljesítményadatok és -eszközök)* programjának felületéről érhetjük el.)

Közel sem ennyire egyszerű és problémamentes a teljes Users mappa másik kötetre helyezése (ebben az esetben tehát már az új profilok is itt keletkeznének). Erre a feladatra nem kapunk beépített eszközt, és mivel a Users mappa hivatkozásai számtalan helyen szerepelnek a registryben, a „kézi" áthelyezés is meglehetősen reménytelen feladatnak tűnik. A „hivatalos" eljárás csak a telepítés közben működik: a felügyelet nélküli „unattended" telepítés válaszfájljában tetszés szerint beállítható a Users mappa helye. Sajnos azonban még ebben az esetben is számolhatunk néhány mellékhatással (például nem minden frissítés hajlandó települni ilyen rendszerre), ebben az esetben létre kell hoznunk a rendszerköteten egy *C:\Users* nevű szimbolikus hivatkozást (az mklink nevű parancssori eszköz segítségével), ami a Users mappa új helyére mutat.

A felügyeleti konzol: az MMC-program



Az MMC, vagyis a Microsoft Management Console egy összetett felügyeleti eszköz, mellyel a Windows operációs rendszer szinte összes fontos komponensét és szolgáltatását konfigurálhatjuk. Az MMC-konzol egy egységes felületet nyújt az felügyeleti eszközök számára, melyeket modulok képében tölthetünk be ebbe a konzolba, majd a tetszés szerint összeállított MMC-konzolt el is menthetjük .msc formátumba (ekkor bekerül az Administrative Tools *(Felügyeleti eszközök)* programcsoportba). Az MMC-konzol mindegyik Windows-változatban elérhető (írjuk be a *Start/Run* mezőbe: *mmc),* segítségével a helyi számítógépen kívül bármely a hálózatra kötött Windows operációs rendszer felügyelete lehetővé válik – természetesen a korrekt hálózati kapcsolat, illetve a megfelelő jogosultságok függvényében.

A Windows Vista az MMC 3.0-s verzióját tartalmazza, amely újdonságai közé tartozik például a jobb oldali Action pane *(Műveletek munkaablak)*, amelyben helyzetérzékeny módon a fő keret tartalmától függően mindig az aktuális parancsok és műveletek érhetőek el. Az MMC 3.0 a modulok egymásba ágyazhatósága és megjelenítése, valamint a konzol hibakezelése kapcsán is mutat újdonságokat.

A felügyeleti konzol — Microsoft Management Console (MMC)
Ebben az előadásban a (majdnem) minden felügyeleti eszköz alapjának számító MMC-konzol áttekintését láthatjuk.
Fájlnév: I-1-2b-MMC.avi

A Computer Management konzol áttekintése

Az egyik leggyakrabban használt MMC-konzol az Computer Management *(Számítógép-kezelés)* névre hallgató, ez gyakorlatilag a rendszergazdák fő eszköze az operációs rendszer konfigurálásánál és hibaelhárításánál. A Computer Management gyárilag összeválogatott modulokból álló MMC-konzol, a legfontosabb eszközöket tartalmazza:

- **System Tools** *(Rendszereszközök)* – itt találhatók a Feladatütemező, az Event Viewer *(Eseménynapló)*, a hálózat felé megosztott erőforrások, a Local User and Groups *(Helyi felhasználók és csoportok),* a rendszerstabilitási és teljesítménymérő modul, valamint a hardverek felügyeletét ellátó Device Manager *(Eszközkezelő)*.
- A **Storage** *(Tárolás)* részben a lemezkezelő bővítmény kapott helyet, melyen keresztül a rendszerhez csatlakoztatott valamennyi helyi meghajtót konfigurálhatjuk (particionálás, formázás, lemezellenőrzés, meghajtó betűjel változtatás stb).
- **Services and Applications** *(Szolgáltatások és alkalmazások)* – A harmadik szekcióban alapesetben (a szolgáltatások növekedésétől függően bővülhet, tipikusan a szervereken lesz ez így) a Windows-szolgáltatásokat felügyelő modul, illetve a WMI Control (Windows komponensszolgáltatások felügyelete) található meg.

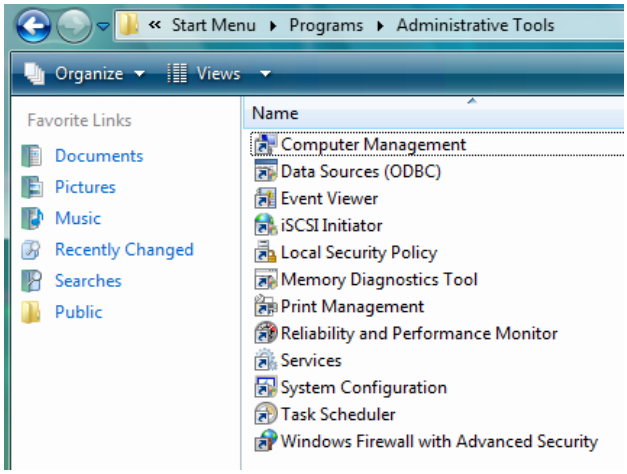
A Computer Management MMC eszközeit a későbbi fejezetekben részletesen és külön-külön is ismertetjük.

A Computer Management konzol áttekintése
Ebben a mini előadásban a talán a legtöbbet használt rendszergazda eszköz a Computer Management MMC bemutatása látható.
Fájlnév: I-1-2c-Computer-Management-MMC.avi

A felügyeleti eszközök *(Administrative Tools)*

A Computer Management *(Számítógép-kezelés)* MMC-t az Administrative Tools *(Felügyeleti eszközök)* programcsoportból érhetjük el, ahol egyébként a fenti konzolon kívül a számítógép karbantartásához szükséges összes egyéb eszközt is megtalálhatjuk. Ezek az eszközök tipikusan a helyi gépre érvényes konfigurációk megváltoztatásához használatosak, de legtöbb modulból lehetőségünk van a hálózat egy másik gépének kezelésére is.

A felügyeleti eszközök *(Administrative Tools)* áttekintése és a System Configuration Utility
Ebben a screencastban a felügyeleti eszközök gyűjtőhelyének, az Administrative Tools programcsoportnak az eszközeit, valamint a kissé megváltozott System Configuration segédprogramot mutatjuk be.
Fájlnév: I-1-2d-Administrative-Tools.avi



1.12. ábra: *Az Adminstrative Tools csoport*

Vegyük sorra az Administrative Tools csoportban található eszközöket:

- **Data Sources (ODBC)** – Ez az alkalmazás a különböző adatbázisok közti kapcsolatok beállítását teszi lehetővé.
- **Event Viewer** *(Eseménynapló)* – Az eseménynaplóban az operációs rendszer működésével kapcsolatos minden eseményt felügyelhetünk, elkülönítve láthatjuk az alkalmazások és a rendszer által küldött információkat, figyelmeztetéseket és hibaüzeneteket. A Windows Vistában az egyes rendszerkomponensek külön eseménynaplóba jegyzik tevékenységüket, így még strukturáltabbá és áttekinthetőbbé válik a napló. Az egyes komponensnaplók igen részletesen beszámolnak a rendszer működéséről, még a Windows teljesítményét rossz irányban befolyásoló tényezőkről is kaphatunk jelentéseket. A következő fejezetben részletesen „kibontjuk" az Eseménynapló jellemzőit és lehetőségeit.
- **iSCSI Initiator** – Ez a modul a hálózaton vagy akár az interneten keresztül elérhető távoli számítógépek háttértárolóinak (vagy önálló háttértárolók) csatlakozását és felügyeletét teszi lehetővé.
- **Local Security Policy** *(Helyi biztonsági házirend)* – A helyi számítógép részletes biztonsági beállításait tekinthetjük meg és szerkeszthetjük ezen a konzolon keresztül. A biztonsági házirendek segítségével a rendszergazda konfigurálhatja az operációs rendszer védelmi szolgáltatásait, valamint jogosultságokat oszthat ki egyes felhasználócsoportoknak. A második fejezet végén részletesen tárgyaljuk a Helyi házirendet.

- **Memory Diagnostics Tools** *(Memóriadiagnosztikai eszköz)* – Mivel a Windows stabil működésének alapfeltétele, hogy a memóriamodulok kifogástalanul működjenek, a Vistában már beépített memóriatesztelő alkalmazással ellenőrizhetjük a RAM modulok működését. Háromféle teszt választható, az egyszerű gyors vizsgálattól kezdve egészen a legbonyolultabb írási és olvasási műveleteket szimuláló próbáig. A memóriateszt elvégzéséhez a számítógép újraindítása szükséges, maga a vizsgálat karakteres felhasználói felületen, még a Windows betöltődése előtt lezajlik. Az ellenőrzés bármikor megszakítható és a rendszer betöltődik. Miután bejelentkeztünk a Windowsba, automatikusan jelentést kapunk a legutóbbi teszt eredményéről.

A Memory Diagnostics Tool
Ebben a mini demóban az új memória tesztelő alkalmazás lehetőségeit mutatjuk be.
Fájlnév: I-1-2e-Memoriavizsgalat.avi

- **Print Management** *(Nyomtatókezelés)* – A Print Management konzolban az összes helyileg telepített nyomtatót, a hozzájuk tartozó eszközillesztő-programokat, a nyomtatóportok állapotát, valamint a rendelkezésre álló nyomtatási sablonokat (pl. papírfajták) kezelhetjük.
- **Reliability and Performance Monitor** *(Megbízhatóság- és teljesítményfigyelő)* – A Windows XP-ben is megtalálható teljesítménydiagnosztikai alkalmazás meglehetősen kibővített változatát találjuk ebben a konzolban. Szinte minden rendszerkomponens teljesítményét különkülön figyelemmel kísérhetjük, naplózhatjuk, sőt akár időzített mérést is végezhetünk. A mérés befejeztével lehetőségünk van egy előre definiált ütemezett feladat elindítására. A konzol másik feladata a rendszer stabilitásának nyomon követése, melyet az eszköz egy grafikonon vizuálisan is ábrázol. A rendszerstabilitási napló elemzésével a rendszergazda visszamenőleg értesülhet olyan eseményekről, melyek egyegy alkalmazás vagy akár a teljes rendszer leállását, hibás működését okozták. A napló segítségével nem csak a hibákat, hanem az olyan eseményeket is figyelemmel kísérhetjük, mint az alkalmazások, eszközmeghajtók telepítése/törlése. A következő fejezetben részletesen szó esik majd erről a komponensről.
- **Services** *(Szolgáltatások)* – Szolgáltatásnak nevezzük azokat a rendszerfolyamatokat, melyek a háttérben futva az operációs rendszer indításától a leállításáig olyan alapvető funkciókat látnak el, mint például a hálózati, a biztonsági, vagy a multimédiás alrendszer működtetése. Ez a konzol a szolgáltatások felügyeletét látja el, azaz itt állíthatjuk be,

hogy az egyes integrált rendszer-, illetve az utólag – akár külső szoftverek által telepített – szimpla szolgáltatások hogyan induljanak, milyen szolgáltatásfiókkal működjenek, mi történjen velük, ha valamilyen hiba következtében leállnak, illetve megnézhetjük az adott szolgáltatás függőségi viszonyait is. A harmadik fejezetben visszatérünk a rendszerszolgáltatásokra, elsősorban a biztonságra fókuszálva.

- **System Configuration** *(Rendszerkonfiguráció)* – E rendszerbeállító alkalmazás segítségével a Windows indulásának körülményeit változtathatjuk meg. Hibakeresés alkalmával lehetőségünk van diagnosztikai indítási módot választani, ahol csak a Windows működéséhez legszükségesebb összetevők töltődnek be, konfigurálhatjuk a rendszerbetöltő speciális beállításait, valamint egyetlen helyről indíthatunk olyan további felügyeleti eszközöket, mint az eseménynapló, a rendszervisszaállítás, a feladatkezelő, vagy a Beállításszerkesztő *(Registry Editor)*.

- **Task Scheduler** *(Feladatütemező)* – A Vista feladatütemezője teljesen megújult, számtalan új feltétel alapján indíthatunk automatikusan különböző folyamatokat a rendszerben. A feladatütemező megnyitásakor egy központi nézetben láthatjuk az utóbbi 24 órában lefutott és a jelenleg is aktív feladatok státuszát. Az egyes feladatok ütemezési lehetőségei számos új lehetőséggel bővültek, valamint a végrehajtható feladatok közé – a programfuttatás mellé – bekerült a képernyőn megjelenítendő üzenet, illetve e-mail küldése is. Az időzített feladatokat hálózati környezethez és a tápellátás aktuális állapotához is köthetjük. Az új feladatütemező szorosan együttműködik az eseménynaplóval, így az általunk beállított egyes rendszereseményekhez szabadon társíthatunk programfuttatást, vagy üzenetküldést is. A következő fejezetben részletesen szó esik majd erről a komponensről is.

- **Windows Firewall with Advanced Security** *(Fokozott biztonságú Windows tűzfal)* – A Windows XP-ből ismerős egyszerű tűzfalbeállítások a Vistában is elérhetők, de az új operációs rendszer az alapműveleteken kívül rendkívül részletes beállítási lehetőségeket is kínál egy külön MMC-konzolon keresztül. A Windows Firewall modul megnyitásakor rögtön láthatóvá válik az új tűzfal egyik legfőbb újdonsága, a profilkezelés. A szolgáltatás hálózati környezettől függően három profilnak megfelelően tud működni: otthoni, céges környezet, illetve nyilvános hálózat. Az egyes profilokhoz külön szabályrendszert hozhatunk létre, valamint a Vistában már a kimenő forgalom szűrését is beállíthatjuk, ám ez a funkció alapértelmezésként nincs bekapcsolva. A tűzfal-konfigurációs konzolban teljesen személyre szabhatjuk az egyes szabályokat, szinte minden paramétert megváltoztathatunk: megad-

hatjuk, hogy a szabály melyik profilban éljen, milyen programra vonatkozzon, az alkalmazás milyen protokollokon és portokon keresztül, mely IP-címről mely IP-cím felé kommunikálhat. Az új tűzfal konzolban kapcsolatbiztonsági szabályokat is felállíthatunk két gép hálózatban történő összeköttetéséhez, melyekhez igénybe vehetjük az integrált IPSec (hálózati forgalom titkosító) szolgáltatásait. A harmadik fejezet végén részletesen szó esik majd erről a komponensről is.

Ügyfélgép beléptetése tartományba

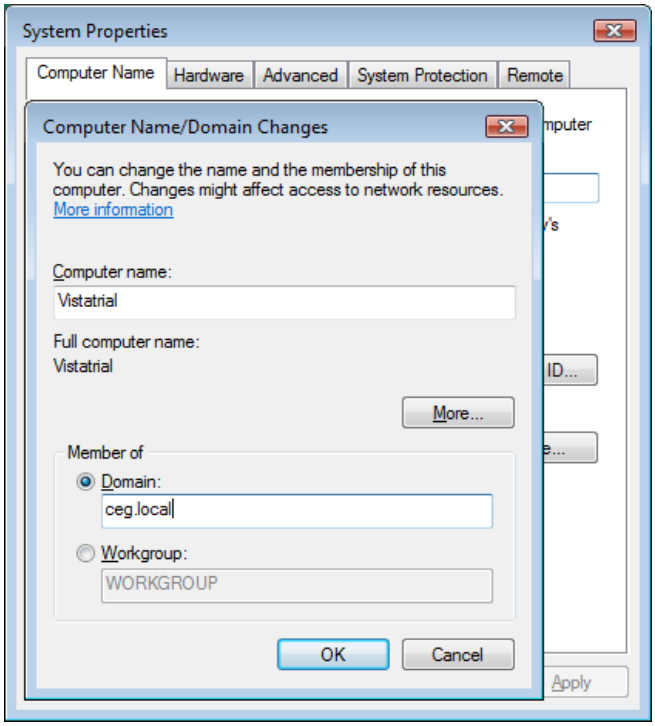
Egy hálózat számítógépei munkacsoport vagy Active Directory tartomány tagjai is lehetnek. Az alapértelmezett munkacsoport tagság (egy gép esetén is) a számítógépek laza csoportját jelenti, egy adott munkacsoporthoz való tartozás tulajdonképpen semmi komoly következménnyel nem jár sem a számítógép, sem a hálózat számára. A munkacsoportok a következő tulajdonságokkal rendelkeznek:

- Az összes számítógép egyenrangú, valamennyi, a hálózati működéssel kapcsolatos szolgáltatást bármelyik erre alkalmas számítógép biztosíthatja.
- Minden számítógép önálló felhasználói adatbázissal, így önálló, a többi géptől független felhasználói fiókokkal rendelkezik.
- A számítógépek és a felhasználói fiókok valamennyi beállítását (a jogosultságok kiosztását is) külön-külön kell megadnunk minden egyes számítógép és felhasználói fiók esetében.
- A munkacsoport valamennyi számítógépnek egyetlen alhálózathoz *(subnet)* kell tartoznia.

Az Active Directory-tartomány a számítógépeknek (és felhasználói fiókoknak) a rendszergazda által definiált csoportja, amelynek segítségével lehetővé válik valamennyi hálózati és helyi erőforrás központi felügyelete. (Az Active Directory-tartományok létrehozásával és felügyeletével az ötödik fejezetben részletesen fogunk foglalkozni.) A tartományok a következő legfontosabb tulajdonságokkal rendelkeznek:

- A tartományhoz tartozó számítógépek nem egyenrangúak, bizonyos szolgáltatásokat csak az erre kijelölt kiszolgálók (a tartományvezérlők) láthatnak el, a többi számítógép (kiszolgálók és ügyfélgépek egyaránt) ezek szolgáltatásait veszik igénybe a felhasználók hitelesítésével, a rendszer különféle beállításainak letöltésével és még számos más feladattal kapcsolatban.

- A tartományhoz tartozó számítógépeken (a tartományvezérlőket kivéve) van ugyan helyi felhasználói adatbázis is, de a gépekre a tartományban központilag létrehozott felhasználói fiókok használatával is be lehet jelentkezni (helyi fiók nélkül), és a helyi felhasználói jogosultságok kiosztásakor is használhatók a tartományi csoportok és felhasználói fiókok (célszerűen a helyi csoportok tagjai közé való felvétellel).
- A tartományhoz tartozó számítógépek és felhasználói fiókok beállításait a rendszergazda központilag szabályozhatja.
- A számítógépek különböző helyi hálózatokhoz is tartozhatnak.



1.13. ábra: *Csatlakozunk a* ceg.local *nevű tartományhoz*

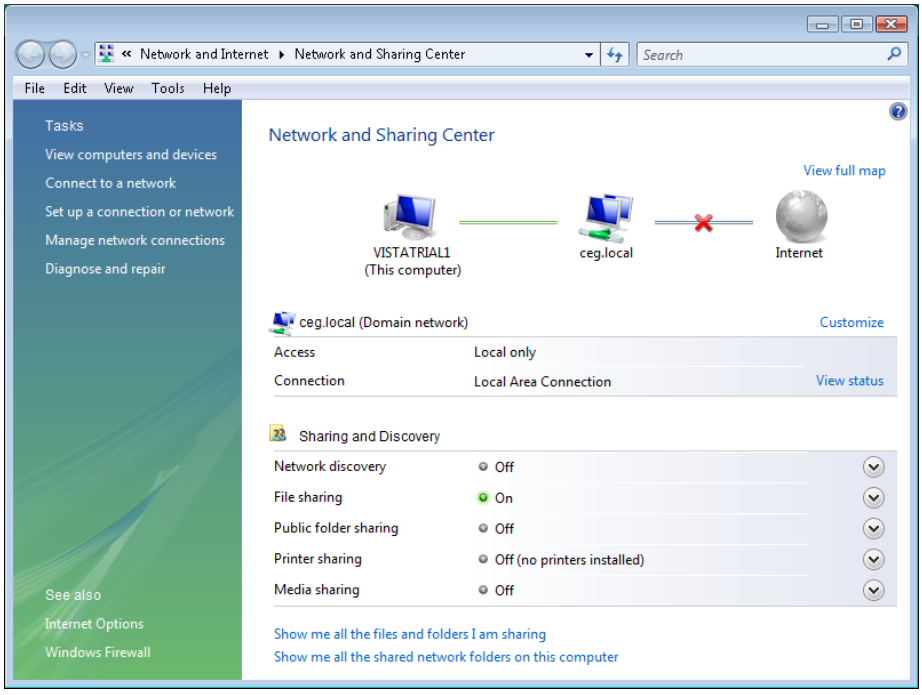
Hogy a számítógépet tartományba léptethessük, be kell állítanunk a TCP/IP-paramétereket (különös tekintettel a DNS-kiszolgálóra), szükségünk van egy helyi rendszergazda fiók jelszavára és a csatlakozás során meg kell adnunk egy olyan tartományi felhasználó (rendszergazda) nevét és jelszavát is, akinek az Active Directory címtárban joga van a megfelelő számítógépfiók létrehozásához.

Hálózat a Windows Vistában

A hálózati és megosztási központ

A Windows Vista teljesen megújult hálózatkezelésének első látható nyomait akkor fedezhetjük fel, ha megnyitjuk a Network and Sharing Center *(Hálózati és megosztási központ)* nevű, speciális ablakot. Ez egy olyan központosított hely, ahol a hálózatok kezelésével kapcsolatos valamennyi információ, illetve beállítási lehetőség megtalálható. Többféle módon is elindíthatjuk:

- A Start menü Keresés mezőjébe írjuk be: network, majd kattintsunk a felső listában megjelenő ikonjára.
- Control Panel > Network and Internet.
- A Windows Explorerből a jobboldalon a Hálózat nevű mappára kattintva megjelenik a menüsorban.
- A Tálca jobb szélén a jobb gombbal a hálózat ikonra kattintva megjelenik a menüben.



1.14. ábra: *Hálózati és megosztási központban szinte mindent megtalálunk, aminek köze van a hálózathoz*

A kezdőlapon rögtön láthatjuk a jelenlegi kapcsolat sematikus ábrázolását, leolvashatjuk a hálózaton szereplő eszközök nevét, illetve a Windows itt grafikus formában is jelzi, ha valamelyik kapcsolatban hiba lépett fel. Az adott hálózat teljes térképét a View Full Map *(Teljes térkép)* hivatkozásra kattintva tekinthetjük meg (lásd később).

A hálózatot jelképező ábra alatt találhatók az aktuális hálózati kapcsolat adatai, a hálózat neve, az elérés típusa (helyi vagy internetes kapcsolat), valamint a kapcsolódáshoz használt hálózati interfész neve. Az egyes kapcsolatok esetében a jobb oldali Customize *(Testreszabás)* hivatkozásra kattintva szabhatjuk testre a kapcsolatok nevét, ikonját, valamint itt rendelhetünk hozzájuk hálózati profilt is. A View status *(Állapot)* hivatkozás alatt találhatjuk a kapcsolat klasszikus konfigurációs lapját és innen olvashatjuk le gépünk aktuális IP-címét, az átjáró és DNS-kiszolgálók címét.

A hálózati kapcsolatok alatt egy tételes felsorolás formájában láthatjuk a helyi számítógép hálózati szolgáltatásaira vonatkozó legfontosabb beállításait (Sharing and Discovery – *Megosztás és felderítés):*

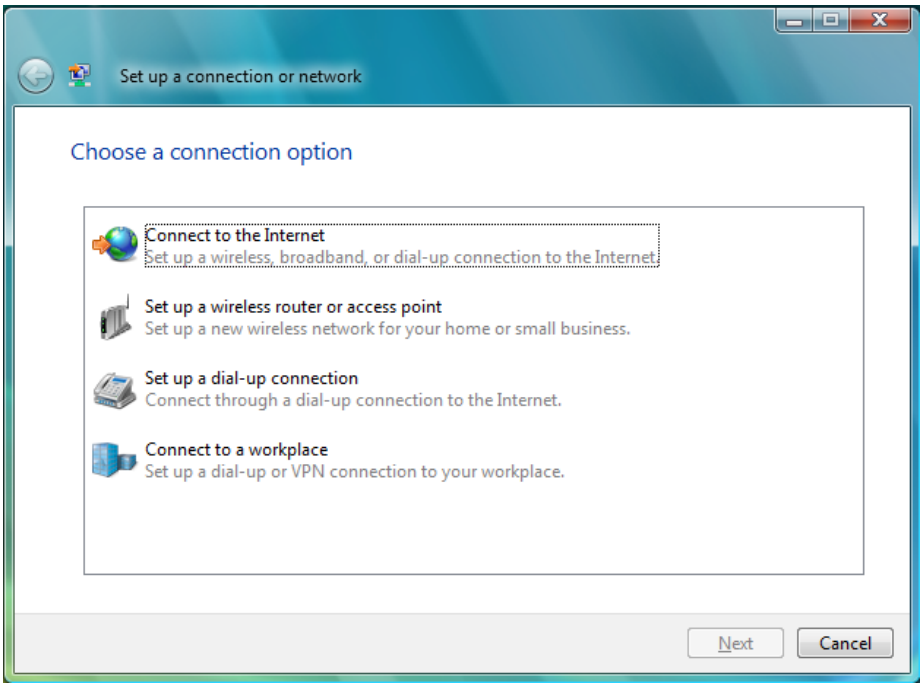
- **Network Discovery** *(Hálózat felderítése)* – Lehetővé teszi, hogy a Vista automatikusan érzékelje a hálózatra kötött számítógépek jelenlétét, és az azokon megosztott erőforrásokat, ezzel felgyorsítva az azokhoz történő kapcsolódást. Egyúttal a mi gépünk „láthatóságát" is engedélyezhetjük vagy tilthatjuk itt.
- **File sharing** *(Fájlmegosztás)* – A fájl- és nyomtatómegosztást kapcsolja be, illetve ki. A Windows Intézőben csak akkor tudunk fájlokat vagy mappákat megosztani, ha ez a szolgáltatás engedélyezve van. A mappákat, illetve a nyomtatókat csak olyan személyek érhetik el a hálózatról, akiknek létezik érvényes felhasználónevük és jelszavuk a helyi gépen.
- **Public folder sharing** *(A Nyilvános mappa megosztása)* – A Public (All Users) mappa megosztása a hálózat felé, többféle jogosultsággal. Ebbe a mappába általában olyan dokumentumokat szokás elhelyezni, melyeket a számítógép összes felhasználója és a hálózaton kapcsolódók számára is elérhetővé kívánunk tenni.
- **Printer sharing** *(Nyomtató megosztása)* – A helyi nyomtatók hálózaton keresztül történő megosztásával a távoli számítógépekről is lehetővé válik a nyomtatás a saját nyomtatónkra. A telepített nyomtatók megosztását és a felhasználók jogosultságait nyomtatónként be kell állítani, ez a kapcsoló csak a nyomtatási szolgáltatás globális megosztását szabályozza.

- **Password protected sharing** *(Megosztás jelszavas védelemmel)* – Ha jelszavas elérhetőséget kívánunk biztosítani a hálózat többi felhasználójának, engedélyezzük ezt a lehetőséget. Ha a Password protected sharing szolgáltatás ki van kapcsolva, a publikus mappák jelszó megadása nélkül is elérhetők. Ez a lehetőség egy tartományi fiókkal rendelkező gép esetén nem látható.
- **Media Sharing** *(Médiafájlok megosztása)* – A médiatartalom megosztása teljesen új funkció a Vistában. A rendszer képes a Windows Media Player lejátszási listáját a hálózat többi számítógépe – illetve olyan speciálisan médialejátszásra (is) alkalmas eszközök felé, mint az Xbox 360 játékkonzol, vagy különböző Media Center extenderek *(bővítmények)* – megosztani, így a zenei és videófájlokat nem kell minden számítógépen tárolni. A lejátszási lista teljes egészében, vagy részlegesen is megosztható. A médiamegosztás részletes konfigurációját a Windows Media Player beállításai között találhatjuk.

A megosztott erőforrásokat és felderítési beállításokat megjelenítő táblázat alatt két további hivatkozást találhatunk, melyek az általunk megosztott mappákat, illetve a számítógépünk összes megosztott mappáját mutatja meg.

A Network and Sharing Centerben a hálózatokhoz történő kapcsolódást és a már meglévő hálózati kapcsolatok, illetve hálózati kártyák konfigurációját is elvégezhetjük. Ha a bal oldali kékeszöld sávban a Set up a connection or network *(Kapcsolat vagy hálózat beállítása)* parancsra kattintunk, a hálózati kapcsolódás varázslóban találjuk magunkat, ahol a kapcsolat típusától függően több irányba is elindulhatunk.

- Létrehozhatunk egyszerű internetes kapcsolatot, melyhez használhatunk telefonos, szélessávú kábeles, illetve vezeték nélküli elérést is.
- Beállíthatunk vezeték nélküli hozzáférési pontot vagy egy útválasztót.
- Kapcsolódhatunk publikus vagy védett vezeték nélküli hálózatokhoz.
- Ideiglenes, úgynevezett ad hoc vezetéknélküli hálózatot hozhatunk létre másik számítógéppel, telefonnal, vagy egyéb pl. WiFi-képes eszközzel.
- Beállíthatunk virtuális magánhálózatot (VPN), mellyel munkahelyünk helyi hálózatához csatlakozhatunk – biztonságos körülmények között az interneten keresztül.



1.15. ábra: *Az összes hálózati kapcsolattípus elkészíthető az új varázslóval*

Az elkészült hálózati kapcsolatokat a Connect to a network *(Csatlakozás a hálózathoz)* hivatkozásra kattintva láthatjuk majd, ahonnan – szintén egy apró, de hasznos újdonság miatt csoportosítva – az összes létező kapcsolat elérhető.

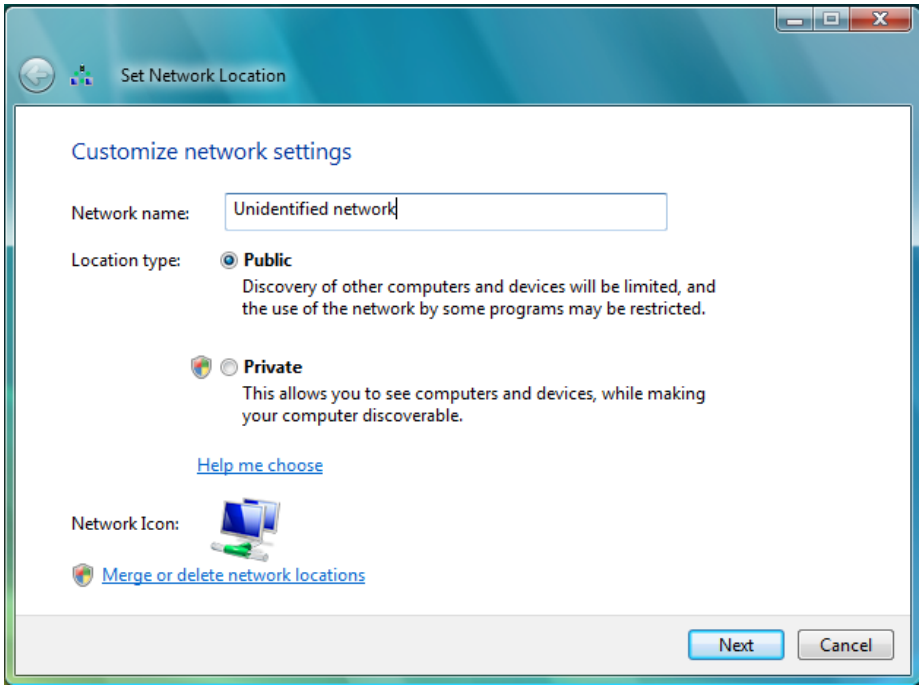
A kapcsolatok – a Windows Vista újratervezett, informatív varázslóinak köszönhetően – könnyen beállíthatók, de ha mégis elakadunk, rögtön megoldási javaslatokat is kapunk a rendszertől. A kapcsolódás esetleges sikertelensége esetén az automatikus hálózat-diagnosztika is elérhető, mely a leggyakoribb konfigurációs hibákat önállóan képes kijavítani. A Manage network connections *(Hálózati kapcsolatok kezelése)*, illetve Manage wireless networks *(Vezeték nélküli kapcsolatok kezelése)* hivatkozások mögött a Windows hálózati interfészeit, illetve a beállított vezeték nélküli hálózatok tulajdonságait konfigurálhatjuk. A Diagnose and repair *(Diagnosztizálás és javítás)* paranccsal pedig a korábban említett automata hálózati diagnosztika eszközt indíthatjuk el.

A hálózati és megosztási központ (Network and Sharing Center)
Ebben a screencastban a Network and Sharing Center összes lehetséges beállítását és szolgáltatását megtekinthetjük.
Fájlnév: I-1-3a-Network-and-Sharing-Center.avi

A hálózati profilok

A Windows Vista a megnövelt biztonság, illetve a könnyebb felügyelet érdekében úgynevezett hálózati profilokat különböztet meg, attól függően, hogy a számítógép milyen környezetben működik. Három gyárilag definiált hálózati profil létezik: tartományi, privát, illetve publikus.

A hálózati profilok tulajdonképpen olyan beállításcsomagok, melyek tartalmazzák a kapcsolathoz használt interfész típusát, az alapértelmezett átjáró MAC-címét, és egyéb kapcsolatspecifikus adatokat, valamint tartományi hálózat esetén a hitelesítő kiszolgáló adatait. A profil a hálózathoz történő első kapcsolódáskor jön létre.

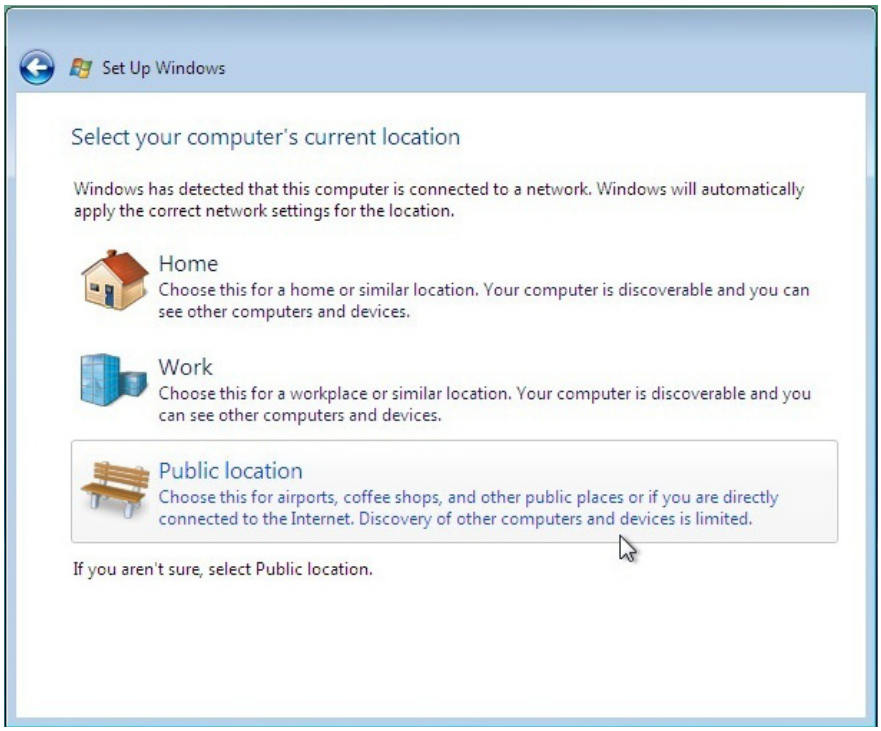


1.16. ábra: *Bizonyos esetekben mi magunk is választhatunk vagy változtathatunk hálózati profilt (tartományi tagság esetén nem)*

Az egyes hálózattípusok jelentései az alábbiak:

- **Domain** *(tartományi profil)* – Ha a számítógép tagja egy Windows-tartománynak, a hálózati kapcsolat profilja automatikusan domain lesz, függetlenül attól, hogy a gép éppen csatlakoztatva van-e, vagy sem.

- **Private** *(Privát)* – A személyes profil olyan – tipikusan otthoni – munkacsoportos hálózatot jelöl, melyben lazább biztonsági szabályok érvényesek.
- **Public** *(Nyilvános)* – Minden olyan hálózat, mely nem tartományi és nem is személyes. Publikus hálózati profilt célszerű használni a repülőtereken, internetkávézókban és egyéb nyilvános helyeken elérhető – többnyire vezeték nélküli – hálózatokhoz kapcsolódáskor, ilyenkor ugyanis a legszigorúbb biztonsági szint lép életbe. Egy új kapcsolat is mindig ezzel a legszigorúbb profillal indul el, és csak az automatikusan észlelt eltérő környezet felismerésekor módosul.



1.17. ábra: *Három hálózati profil áll rendelkezésre*

Az aktuális profil – ahogy a különböző hálózatok között mozgunk – természetesen változhat. Ezeket a változásokat a Vistában a Network Location Awareness (NLA – *hálózati szintű hitelesítés)* szolgáltatás detektálja, majd ennek megfelelően gondoskodik a profilváltásról és az új biztonsági szabályok alkalmazásáról.

A hálózati profil váltása rendkívül rövid idő, elvileg mintegy 0,2 másodperc alatt végbemegy, így a két profil közt „lebegő” gépet érő támadások gyakorlatilag kiküszöbölhetők.

Amikor hálózatiprofil-váltás történik a Windows automatikusan alkalmaz minden olyan beállítást a hálózati interfészre és a rendszer egészére (megosztások, felderítési beállítások, tűzfalkonfiguráció stb.), melyek az adott környezetnek megfelelő helyes működéshez szükségesek. A Network Location Awareness szolgáltatás publikus programozási interfészt (API) is nyújt, így a hálózati profilokkal a külső fejlesztők által írt programok is együtt tudnak működni. Az NLA-t továbbá vezérelhetjük a csoportházirenden keresztül is, így a rendszergazda definiálhatja például a tűzfal működését az egyes hálózati profilokban. Az alábbi táblázat a Windows-tűzfal, a hálózati megosztások és a hálózatfelderítés alapértelmezett beállításait mutatja az egyes hálózati profilok esetén:

	Tartomány	Privát	Nyilvános
Windows tűzfal	Bekapcsolva	Bekapcsolva	Bekapcsolva
Hálózatfelderítés	Csoportházirend alapján	Bekapcsolva	Letiltva
Fájl- és nyomtatómegosztás	Csoportházirend alapján	Letiltva	Letiltva

A TCP/IP-protokoll

A TCP/IP (Transmission Control Protocol/Internet Protocol) protokollkészletre épül szinte minden hálózattal kapcsolatos művelet, nem csak a Windows, de egyéb operációs rendszerek és hálózati eszközök esetén is. Mivel az internet szabványos protokolljáról van szó, napjainkban a TCP/IP a legelterjedtebb hálózati protokoll, ennek megfelelően nem is javallott mást használni, hacsak erre nincs kifejezetten szükség valamilyen speciális alkalmazás vagy szolgáltatás üzemeltetése miatt.

A TCP/IP hálózati alrendszer szerves része a Windows operációs rendszernek, telepítéskor automatikusan felkerül és nem is távolítható el, mindössze a működése tiltható le. A Windows TCP/IP-konfigurációjának megváltoztatásakor nem kell újraindítani a rendszert, mindössze a hálózati kapcsolat szakad meg egy pillanatra, majd az összeköttetés automatikusan újra létrejön, immár az új beállításokkal.

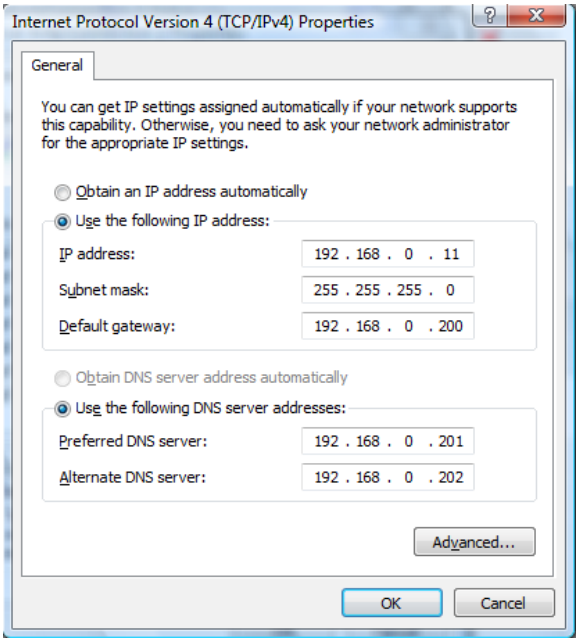
Egy egyszerű esetben, hardveres szempontból gyakorlatilag elég csak két gépet összekapcsolnunk, és máris „hálózatról" beszélhetünk, de a fizikai (vagy vezeték nélküli) összeköttetésen kívül mi szükséges még egy működő Windows-hálózat beüzemeléséhez?

- **IP-cím** – Az IP (Internet Protocol) cím egyedi, 4 bájt hosszúságú, négyszer három számjegyre tagolt azonosító, mellyel minden aktív hálózati interfészt és TCP/IP-protokollt használó számítógép rendelkezik. Az operációs rendszer az IP-címek alapján azonosítja be az egyes számítógépeket, így a távoli erőforrások elérése mindig IP-cím alapján történik a háttérben – még akkor is, ha a „felszínen" gépnév szerint hivatkozunk azokra.

  Az IP-cím privát vagy publikus típusú lehet, a kettő közötti különbség jelentős, mivel a privát IP-címekkel beállított gépek gyakorlatilag zéró lehetőséggel rendelkeznek az internetre kapcsolva, mivel semmilyen útválasztó nem engedi ki a privát IP-tartományból érkező hálózati csomagokat. Ez adja egyben a biztonságosságukat is, ezért egy akármilyen belső hálózatban csak a privát címtartományokból választunk vagy kapunk IP-címet, és a tűzfalunk és/vagy az útválasztónk rendelkezik olyan, második hálózati interfésszel, amely elérheti az internetet és amelynek ennek megfelelően publikus IP-címe van, és amely egyúttal az ún. hálózati címfordítást *(Network Address Translation, NAT)* is elvégzi majd.

  Az IP-címeket a hálózatban megadhatjuk kézzel (statikus IP) vagy az erre a célra szolgáló automatikus címkiosztást *(Dynamic Host Configuration Protocol, DHCP)* végző kiszolgálótól kapjuk. Ha egyik lehetőséggel sem élünk, a Windows automatikusan kioszt magának egy privát IP-címet, amely mindig a 169.254.0.1 – 169.254.255.254 tartományból érkezik. Az ilyen címzési módszert APIPA-nák (Automatic Private IP Adressing) nevezzük.

- **Alhálózati maszk** – Az alhálózati maszk szintén 4 bájt hosszúságú és szintén négyszer három számból áll, feladata pedig a gépre vonatkozó címtartomány kijelölése. Címtartományok használatára több alhálózati szegmens kiépítésekor lehet szükség, illetve amikor a hálózatba kötött gépeket logikailag el kívánjuk szeparálni egymástól. A maszknak alhálózatonként egységesnek kell lennie, és a Windows az IP-címből automatikusan generálja számunkra, így általában nem szükséges kézzel megadni, de lehetséges korrigálni.



1.18. ábra: *Az IP-cím megadása*

Gyakorlatilag e két adat segítségével egyszerű vagy ideiglenes környezetben már működhet is a hálózatunk, de kicsit alaposabban (a TCP/IPv4 panelen továbbhaladva) a következő paraméterek és lehetőségek beállítása is megtörténhet.

- **Alapértelmezett útválasztó** – Az itt megjelölt IP címmel rendelkező eszköz lesz az, amely a gépünk más – a helyi hálózattól eltérő – hálózatba történő kapcsolódásában segít. Ez a „más" hálózat lehet például az Internet (ilyenkor tipikusan a tűzfalunk belső IP címe kerül ide), de lehet egy másik (akár belső) hálózat felé vezető útválasztó címe is.
- **DNS** – Az imént említettük, hogy a távoli erőforrásokra név szerint is hivatkozhatunk, vagyis a számítógép ún. hostneve alapján. Az operációs rendszer hostneve bármikor megváltoztatható, általában csak a könnyebb beazonosítás a célja. A hostnév és az IP-cím összepárosítását a DNS, vagyis a Domain Name System szolgáltatás végzi, mely egy-egy úgynevezett DNS-zónában gyűjti a név-cím párokat. Kiszolgálót is tartalmazó környezetben általában (tartomány esetében pedig kötelezően) van helyi DNS-kiszolgáló is, tehát ebbe a mezőbe e helyi DNS-kiszolgáló(k) IP-címei kerülnek be. Ha kiszolgáló nincs, viszont van internetkapcsolat, akkor két eset lehetséges, vagy a tűzfalunk végzi a DNS szolgáltatást az internet felé, vagy a szolgáltatónk DNS-kiszolgálóinak publikus IP-címeit kell használnunk.

Ez volt a TCP/IP-panel General *(Általános)* része. Az Advanced *(Speciális)* gombra kattintva először az alapbeállítás részleteit láthatjuk újfent, azzal a különbséggel, hogy itt a többszörös beállításokra (több IP-cím, több átjáró) is lehetőségünk lesz.

A következő fül a részletes DNS-beállításokra mutat, ahol a további DNS-kiszolgálók (ha esetleg kettőnél több van), a DNS-utótagok hozzáfűzésének sorrendje, illetve az elsődleges DNS-zóna neve (amely a tartományi beléptetés és használat során lehet hasznos) állítható be, valamint a szintén helyi DNS-kiszolgáló használata esetén lényeges automatikus DNS-regisztráció lehetősége érhető el.

Az utolsó fül a régi típusú névfeloldási módszer beállításaira vonatkozik. A WINS (Windows Internet Name Service – neve ellenére semmi köze az internethez) feladata hasonlatos a DNS-éhez, és nagyjából csak a régebbi operációs rendszerekkel és alkalmazásokkal fenntartandó kompatibilitás miatt használjuk a mai napig. A WINS-kiszolgáló a számítógépek – szintén kihalófélben lévő – úgynevezett NetBIOS (Network Basic Input/Output System) neveinek gördülékeny feloldásáért felel. Ezen a panelen a NetBIOS névfeloldásban szintén komoly szerepet játszható speciális fájl, az *lmhosts* tartalmát importálhatjuk, illetve a NetBIOS TCP/IP feletti működését engedélyezhetjük. Az elsőre a Vistában ritkán (további részletek az LLMNR protokollnál ebben a fejezetben), a másodikra a helyi hálózatokon szinte mindig szükség van.

A NetBIOS név az a gépet jelölő egyedi és rövid név, amelyet pl. a telepítéskor is megadunk gépnév gyanánt, Fontos tudni, hogy a hostnév és a NetBIOS-név nem ugyanaz. A hostnév, vagy másként DNS-név általában a számítógép NetBIOS-nevéből és az elsődleges tartományi utótagból áll, vagyis például: *szamitogepem.tartomany.hu*. A DNS- vagy hostnévre gyakran FQDN (Fully Qualified Domain Name) – teljes domainnévként is hivatkozunk.

A Windows TCP/IP-konfigurálását értelemszerűen elvégezhetjük a grafikus felületről, de a paramétereket lekérdezhetjük és megváltoztathatjuk a parancssorból is. A Windows 2000/XP/2003/Vista rendszereknél ezt az *ipconfig* paranccsal tehetjük. Paraméterek nélkül csak az alapértelmezett hálózati kapcsolat legfontosabb adatait láthatjuk, ha az összes interfész minden beállítására vagyunk kíváncsiak, használjuk *ipconfig /all* formában az utasítást.

A TCP/IP-ről, az IP-címzésről, a publikus és privát címekről és a címkiosztás részleteiről további, mélyebb részletek olvashatóak a 4. fejezetben.

A TCP/IP-beállítások
Ez a screencast a TCP/IP alap és haladó szintű beállításáról szól, pontról pontra megmagyarázva a paraméterek és opciók jelentését.
Fájlnév: I-1-3b-TCPIP.avi

Új protokollok és szolgáltatások a Vistában

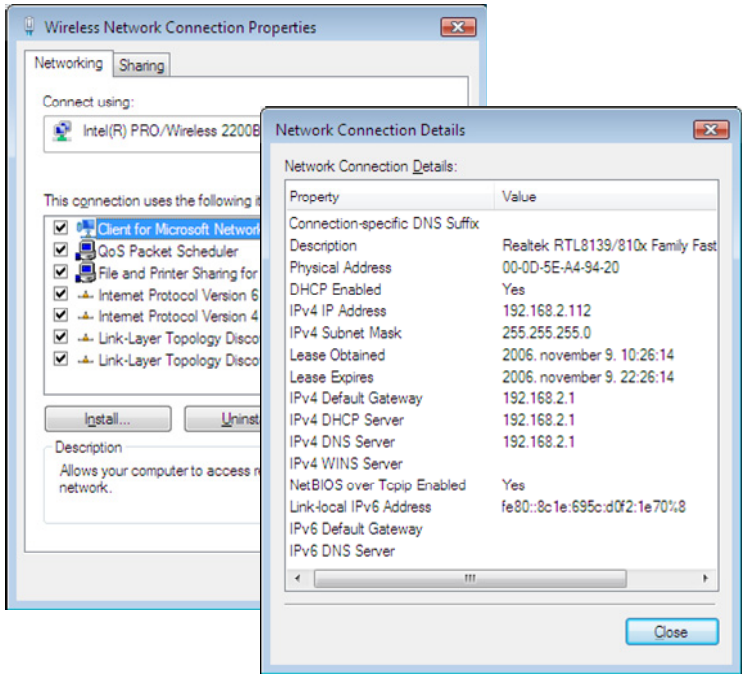
IPv6

A Windows Vista teljesen újraírt hálózati verme a jelenleg elterjedt IPv4-en kívül már natívan támogatja a TCP/IP következő, 6-os verzióját (IPv6) is. A 128-bites (16-bájtos) címekkel operáló IPv6 protokoll bevezetésére főként azért volt szükség, mert a világszerte működő gépek számának ugrásszerű növekedése miatt, napjainkban egész egyszerűen elkezdtünk kifogyni a kiosztható IP-címekből. Emellett az IPv6 lehetőséget adott a TCP/IP-protokollal kapcsolatos néhány technológiai alapelv újragondolására is.

Az IPv6 tehát jóval tágabb címtartományok létrehozását teszi lehetővé, valamint a jelenlegi megoldásoknál könnyebben konfigurálható, gyorsabb és biztonságosabb adatátvitelt tesz lehetővé.

Összehasonlításképpen, egy 128-bites címterület a földfelszín minden négyzetméterén 655 570 793 348 866 943 898 599 (6,5 x 10^{23}) cím létrehozását teszi lehetővé. Az IPv6 címzésről információkat a következő helyen találhatunk (magyarul): *http://www.microsoft.com/technet/prodtechnol/windowsserver2003/hu/library/ServerHelp/22c4b4c0-0276-4190-b5a0-b3f3d83ad048.mspx?mfr=true* vagy *http://tinyurl.com/34f47o*.

A Windows Vistában a korábbi két egymástól teljesen független protokollvermet *(tcpip.sys és tcpip6.sys),* egy úgynevezett Dual IP architektúra váltja, így a rendszer az IPv4 és IPv6-os hálózatokat külön-külön, de mégis egyszerre tudja kezelni. Ennek köszönhetően a Windows egy időben kétfajta IP-címmel is rendelkezhet, egy 4-es, illetve egy 6-os verziójával. A Vista Dual IP architektúrája egy hálózati vermen belül kezel mindent, így továbbra is egy szállítási rétegre (TCP, UDP) és egy adatkapcsolati rétegre van szükség.



1.19. ábra: *Az IPv6 minden szinten rendelkezésre áll*

A Vista IPv6 kezelése teljes IPSec-támogatást is nyújt, így az új formátumú címekkel is használhatjuk a nyílt szabványokból álló kriptográfiai keretrendszert. (Az IPSeckel később a tűzfal kapcsán bővebben is foglalkozunk.)

Az IPv6 mindezeken kívül elérhető PPP (Point-to-Point Protocol) kapcsolatok esetén is (kivéve PPTP VPN használatakor), mely két állomás közti közvetlen kapcsolatoknál – főként telefonvonalon történő betárcsázás vagy közvetlen kábeles összeköttetés esetén használatos. Az IPv6 természetesen támogatja a korábban már említett automatikus címkiosztást is, mind dedikált DHCP-kiszolgálóval, mind anélkül.

A Vista alapértelmezésként mind az IPv4, mind az IPv6 protokollt telepíti, valamint mindkettő beállításai elérhetők a grafikus felületről is. Ha esetleg szkriptekkel automatizált konfigurációra van szükségünk, természetesen a parancssoron keresztül is megváltoztathatjuk a protokollok összes paraméterét – erre kiválóan alkalmas a kibővített funkcionalítással rendelkező „netsh" parancs. (Az IPv6-os konfigurációs lehetőségek bővebb ismertetéséhez adjuk használjuk a „netsh interface ipv6 /?" parancsot.)

A Peer-to-Peer Networking platform

A Windows Vista hálózatkezelésében több újdonságot is felfedezhetünk a kiszolgáló nélküli, társ–társ *(peer-to-peer)* alapon felállított munkacsoportok működtetése során is. A Vista, a korábbi verziókhoz képest sokkal önállóbban és gördülékenyebben képes ezekben a hálózatokban üzemelni, mivel több olyan új szolgáltatás is rendelkezésre áll, melyekkel bizonyos szintig kiválthatók a szerverek. A kiszolgáló nélküli hálózatkezelés támogatásához a Microsoft egy külön platformot hozott létre, mely Windows Peer-to-Peer Networking névre hallgat, és melyhez kapcsolódó protokollok előző verzióival már a Windows XP-ben is találkozhattunk. Ez a szolgáltatásegyüttes megkönnyíti a társ–társ hálózatba kötött számítógépek együttműködését, és az egyes ügyfeleken működő szolgáltatások igénybevételét.

Link-Local Multicast Name Resolution

Az LLMNR-protokoll legfontosabb tulajdonsága az, hogy DNS / WINS-kiszolgáló nélkül képes a helyi hálózaton részt vevő ügyfélszámítógépek host- és NetBIOS neveit feloldani, lássuk hogyan.

Ha tehát a gépünk nem egy nagyobb, kiszolgálókkal ellátott hálózat tagja, akkor is számtalan esetben szükségünk lesz a hálózati nevek és címek kiderítésére. A Windows 2000 óta a DNS-típusú névfeloldás a Windows-ügyfelek alapmódszere, viszont DNS-kiszolgáló híján egy megoldásunk marad, a *hosts* fájl. Ez a fájl a *%windir%\sysrem32\drivers\etc* mappában található, és a hostnevek IP-címhez társítását végzi – ha manuálisan feltöltjük. A gond ezzel a megoldással csak az, hogy a fájl statikus, ezért csak a sohasem változó nevű/IP-című gépeket tartalmazó hálózatoknál alkalmazható, ráadásul kényelmetlen minden gépen külön beállítani a host-táblát. Érdekességképpen megemlíthető, hogy valamikor réges-régen, még az internet hőskorában, jóval a DNS-zónák és szerverek előtt is ezt a megoldást használták a névfeloldásra, azaz kézzel korrigálták a bejegyzéseket, majd ftp-vel töltötték le az érvényes *hosts* fájlokat. Persze nem sokáig élhetett ez a módszer, a dinamikusan működő DNS-kiszolgálók és -zónák tíz- és százezrei sokkal megbízhatóbb és pontosabb módszert jelentenek.

Persze ne feledkezzünk el a régi (Windows 9x, Me, NT) gépekről sem, hiszen ezeknél a gépek neveinek és IP-címeinek kiderítése még a NetBIOS-névfeloldási módszerrel történt. Annál kevésbé szabad erről megfeledkezni, mivel a modern, DNS-sel történő névfeloldás hiányában a Vista is a tartalékszolgáltatáshoz nyúl, azaz szintén a NetBIOS-alapú névfeloldással fog próbálkozni.

A NetBIOS-típusú névfeloldás esetén az IPv4-ügyfelek a NetBIOS TCP/IP felett (NetBT) protokollon keresztül, *NetBIOS Name Query Request* üzenetek küldésével oldhatják fel az azonos alhálózaton található szomszédos számítógépek neveit. A célgép a névkeresésre válaszként *NetBIOS Name Query Res-*

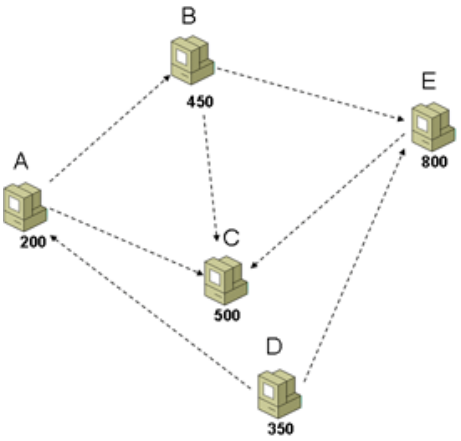
ponse üzenetet küld vissza a kérdező félnek, és a név IP-címmé fordítása végbemegy. A NetBT azonban csak IPv4 esetén működik, a 6-os verziójú TCP/IP-protokoll nem támogatja a NetBIOS nevek használatát, valamint e megoldás komoly hátránya az is, hogy szórt (broadcast) üzenetekkel működik, azaz rengeteg felesleges csomaggal terheli a hálózatot. Ez utóbbit csökkenti az ún WINS-kiszolgáló, illetve kiszolgálók hiányában az ún. *lmhosts* fájl, ami a *hosts* fájlhoz hasonló elven működik, sőt ugyanabban a mappában is található – minden Windows operációs rendszer esetén.

Szépen látható tehát, hogy a korrekt névfeloldás biztosítása, azaz a gépek egymás közötti alapszintű elérése komoly gond lehet erre szakosodott kiszolgálók nélkül, egy kicsi, vagy ideiglenesen összeállított hálózatban. Ezt a problémakört orvosolandó megszületett a Link-Local Multicast Name Resolution protokoll, mely önállóan, NetBT, és akár DNS-kiszolgáló nélkül is képes a helyi hálózat gépeinek névfeloldására. Az LLMNR üzenetek a DNS-éhez hasonló struktúrát alkalmaznak, azzal a különbséggel, hogy a névfeloldást kérő csomagok egységesen az 5355-ös UDP-portra továbbítódnak, és a válaszok is szintén erről a portról indulnak. Az LLMNR névfeloldási gyorsítótár, mely minden Vista-rendszerű számítógépen megtalálható, a DNS-gyorsítótártól elkülönítve kerül rögzítésre, így a különböző hálózatok közti váltásnál ez nem okozhat zavart, valamint az üzemben lévő DNS-kiszolgáló esetleges kiesésekor az LLMNR zökkenőmentesen átveszi a DNS szerepét és a számítógépek a továbbiakban peer-to-peer alapon próbálkoznak a névfeloldással.

Peer Name Resolution Protocol

A Peer Name Resolution Protocol (PNRP) elnevezésű technológia eredetileg a Windows XP-hez készült, később a Microsoft ezt továbbfejlesztve beépítette a Windows Vista-ba, így az új rendszer már alapértelmezésként tartalmazza ezt a szolgáltatást. A PNRP lehetővé teszi a kliensszámítógépek automatikus név szerinti egymáshoz kapcsolását, mindezt névkiszolgáló hiányában is. A PNRP sok különbséget mutat a hagyományos DNS-szerver működéséhez képest. A PNRP használatához nem szükséges DNS-szerver, nagymértékben skálázható (akár több millió nevet is kezel), valamint meglehetősen hibatűrő és megbízható szolgáltatás. A DNS-től eltérően a PNRP nem használ névgyorsítótárat, így a névlista mindig azonnal frissül, tehát nincsenek vakvágányra futott kérések, ami főként a mobilfelhasználókkal történő kapcsolattartásban jelent nagy előnyt. A PNRP nemcsak hostnevet, hanem IP-címet és portszámot is közvetít, így segítségével nemcsak maguk a számítógépek, hanem az azokon futó egyes szolgáltatások is közvetlenül elérhetőek. A PNRP titkosított eljárást alkalmaz a nevek terjesztésére, így az adatok védve vannak a hálózati forgalmat „lehallgatókkal" szemben.

A PNRP-t használó számítógépek közül először mindig az egymáshoz legközelebb eső kliensek veszik fel a kapcsolatot, majd fokozatosan kialakul egy olyan kapcsolatlánc, melyet az alábbi ábra is mutat.



A Peer Name Resolution Protocol egyik tipikus felhasználási területe a Microsoft online tárgyalásokat és előadásokat lehetővé tévő Windows Meeting Space *(Windows Tárgyaló)* szolgáltatása.

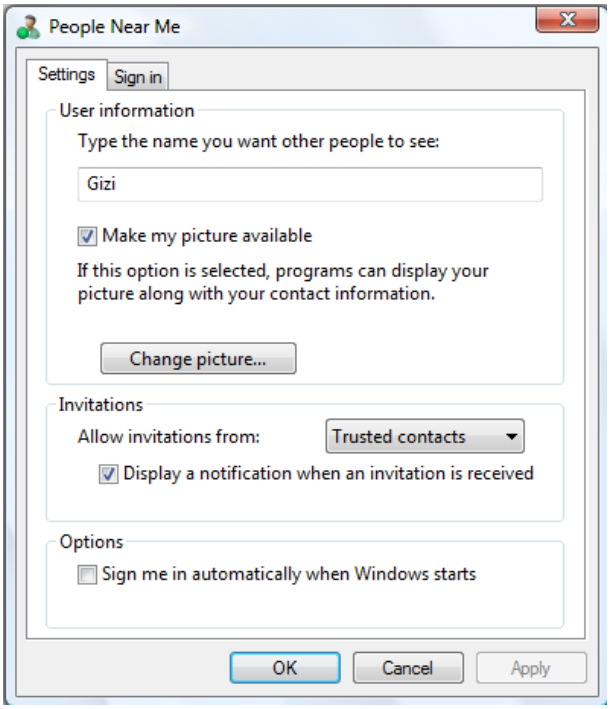
A Windows XP alapcsomagja a PNRP 1.0-s verzióját tartalmazza, de frissítésként a 2.0 is telepíthető rá, így biztosítható a két Windows-platform zökkenőmentes együttműködése.

A PNRP 2.0 frissítés Windows XP-hez a következő címről tölthető le: *http://www.microsoft.com/downloads/details.aspx?FamilyID=55219164-ec71-4a32-a648-4ed2582ebc7cA*.

PNM — People Near Me

A helyi hálózaton végzett együttmunkálkodás további elősegítése érdekében a Microsoft programozói egy új, publikus, tehát a külső fejlesztők számára is szabadon felhasználható API-kra épülő alkalmazáskapcsolati rendszert építettek be a rendszerbe. A People Near Me *(Asztaltársaság)* szolgáltatáshoz egy keretprogram érhető el a Windows Vista operációs rendszerben, melybe a népszerű Windows Live Messenger-hez hasonlóan név és jelszó megadásával kell bejelentkeznünk. Miután aktiváltuk a szolgáltatást, meghívókat küldhetünk, illetve fogadhatunk, melyek elfogadásával különböző – a PNM technológiát hasznosító – erőforrásokat vehetünk igénybe a távoli számítógépeken.

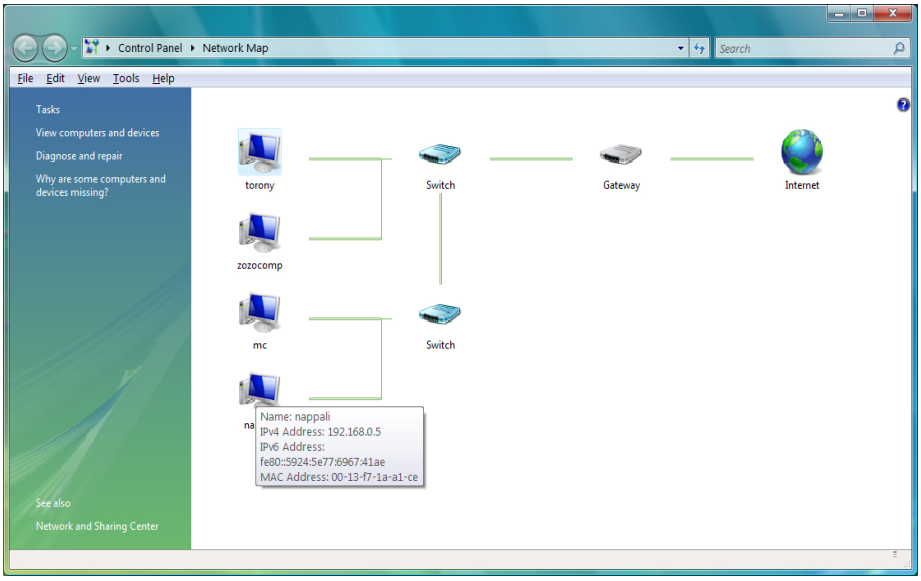
A Microsoft maga is készített egy ilyen alkalmazást, mely Windows Meeting Space *(Windows Társalgó)* névre hallgat és amellyel a Windows Vistán futó bármely alkalmazást, vagy akár a teljes Asztalt megoszthatjuk – akár csak megtekintésre, akár közös használatra is – partnereinkkel. A People Near Me támogatja a biztonságos kapcsolatfelvételt is, a tanúsítvánnyal ellátott meghívók biztosítják, hogy a kapcsolódási kérelmet megbízható forrásból kapjuk. A meghívókat e-mailen vagy akár a Meeting Space által generált speciális konfigurációs fájlban is továbbíthatjuk.



1.20. ábra: *A People Near Me szolgáltatás hasznunkra válhat csoportmunka esetén*

A hálózati térkép

A Windows Vista egyik újdonságaként a hálózati térkép egy sematikus ábrán grafikusan is ábrázolja a számítógép-hálózat elemeit. A térképen látható eszközök ikonjára mutatva további információk jelennek meg az adott objektumról, rákattintva pedig azok alapértelmezett műveleteit érhetjük el (számítógép esetén a megosztott erőforrások tallózása, útválasztóknál pl. a konfigurációs lap megjelenítése). Mindez egy teljesen új speciális protokoll, az LLTD (Link-Layer Topology Discovery) segítségével teljesülhet. Az LLTD egy, az adatkapcsolati rétegen működő hálózatfelderítési technológia, mely a hálózaton szétküldött kérdésekre érkezett válaszok alapján képes feltérképezni a hálózat jellegét, az arra csatlakoztatott eszközöket és számítógépeket. Emellett a QoS (Quality-of-Service) szolgáltatásban is segíthet, mivel képes kezelni a hálózati sávszélességgel, illetve az ügyfélgépek „egészségi” állapotával kapcsolatos kéréseket.

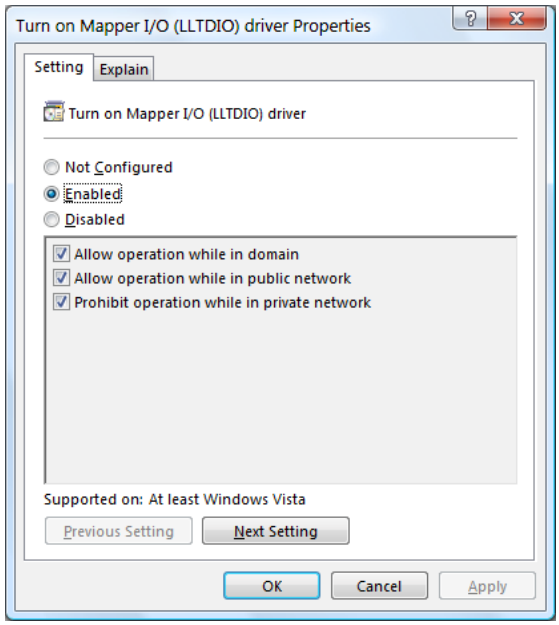


1.21. ábra: *A hálózati térkép több mint egy színes-szagos lehetőség*

Szerencsére az LLTD-frissítés (LLDT Responder) Windows XP-hez is elérhető, így a korábbi operációs rendszert használó számítógépek is látszani fognak a térképen (különben csak az „egyéb eszközök” listában jelennének meg, a térkép alján egy vízszintes sorban). A Universal Plug&Play (UPnP) protokollt alkalmazó eszközök pedig mindenféle szükséges konfigurálás nélkül szintén láthatóak a térképen.

Az LLTD Responder Windows XP-hez a következő címről tölthető le: *http://www.microsoft.com/downloads/details.aspx?FamilyID=4f01a31d-ee46-481e-ba11-37f485fa34ea* vagy *http://tinyurl.com/26u6zr*.

Az LLTD biztonsági okokból alapértelmezésként csak munkacsoportos hálózatban érhető el, tartományi környezetben nem. Ha mégis szükségünk lenne a térképre, a csoportházirenden keresztül engedélyezhetjük annak működését (Computer Configuration/Administrative Templates/Network/ Link-Layer Topology Discovery). Két lehetőségünk is lesz, egyrészt megengedhetjük, hogy a gépek „lássák” a többi eszközt, azaz képesek legyenek hálózati térképet generálni (Turn on Mapper I/O (LLTDIO) driver), másrészt azt is megengedhetjük/tilthatjuk, hogy az adott gépet lássák-e más gépekről, azaz szerepeljünk-e más gépeken készített hálózati térképeken (Turn on Responder (RSPNDR) driver). Ráadásul mindkét esetben finomíthatjuk is a beállítást, mivel hálózati profil alapján is szelektálhatjuk az LLTD hatókörét.



1.22. ábra: *Tartományban is használhatjuk az LLTD-t, de előtte engedélyezzük a csoportházirendben*

MÁSODIK FEJEZET

Diagnosztika és felügyelet

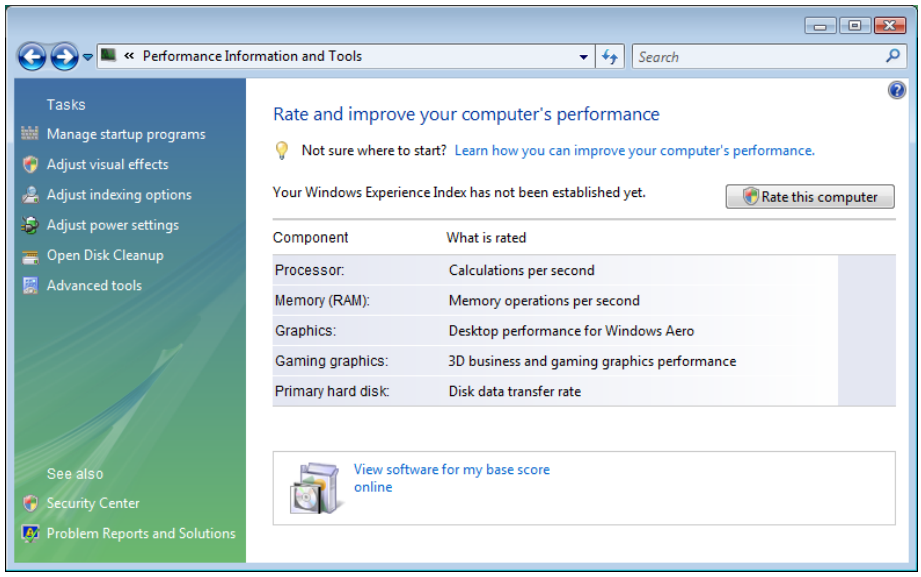
A fejezet tartalma:

Általános felügyeleti áttekintés

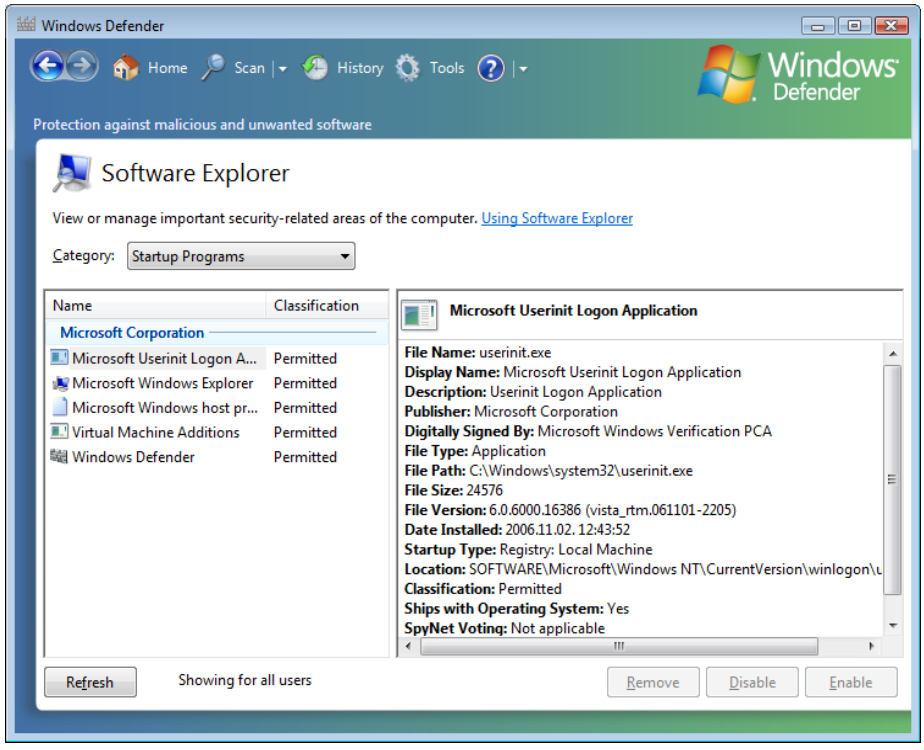
A rendszergazda feladata, hogy a teljes informatikai infrastruktúrát folyamatosan ellenőrzése alatt tartsa, az óhatatlanul előforduló hibákat és problémákat minél hamarabb elhárítsa, hogy a munka zavartalanul folyhasson. Egyes statisztikák szerint a rendszergazdák havonta átlagosan 36 órát töltenek el csak a hibakereséssel, illetve a rendszer állapotának ellenőrzésével. A Windows Vista számos részben, vagy akár teljes mértékben automatizált, haladó tudású diagnosztikai és felügyeleti eszközzel rendelkezik, melyekkel jócskán csökkenthetjük az üzemeltetésre szánt időt, ennek megfelelően többet foglalkozhatunk a produktív munkával.

Performance Information and Tools

A Control Panel *(Vezérlőpult)* ikonjai között találhatjuk meg a Performance Information and Tools *(Teljesítményadatok és -eszközök)* nevű programot, amelynek felületén áttekintést kaphatunk az adott számítógép legfontosabb teljesítményadatairól (ezek alapján határozza meg a telepítőprogram a korábban már említett Windows élményindexet), a bal oldalon található hivatkozások segítségével pedig számos olyan eszközt indíthatunk el, amelyek segítséget nyújtanak a gép teljesítményével kapcsolatos különféle paraméterek beállításában.

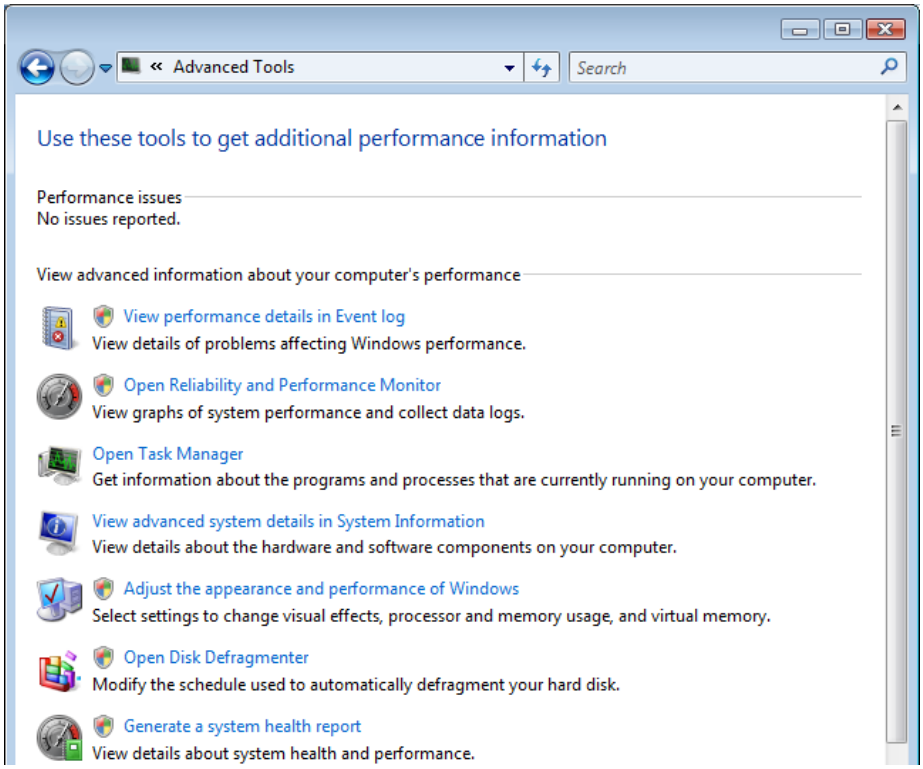


2.1. ábra: *A Performance Information and Tools felülete*



2.2. ábra: *Automatikusan induló programok a Windows Defenderben*

- **Manage startup programs** *(A rendszerindításkor induló programok kezelése)* – a hivatkozás segítségével a Windows Defender Software Explorer *(Szoftvertallózó)* lapját nyithatjuk meg, ahol áttekintést kaphatunk a rendszerben automatikusan elinduló, az éppen futó és a hálózathoz csatlakozó folyamatokról (program neve, szállítója, indítás típusa, digitális aláírás stb.).
- **Adjust visual effects** *(Megjelenítési hatások beállítása)* – a hivatkozás segítségével a rendszer teljesítményét erősen befolyásoló vizuális hatások (áttűnések, átlátszóság, simítás stb.) beállítólapját nyithatjuk meg.
- **Adjust indexing options** *(Indexelési beállítások módosítása)* – itt állíthatjuk be a Vista kereső szolgáltatásához tartozó indexelés különféle paramétereit, például kiválaszthatjuk az indexelésbe bevont mappákat stb. Ezzel kapcsolatban meg kell említenünk, hogy a Vista keresési alrendszere teljesen átalakult, azaz miután a Windows Desktop Search egy fejlett változata beépült az operációs rendszerbe alapos keresési filozófiaváltás történt: nemcsak minden fájl indexelhető és kereshető, de minden lista is, pl. Start menü, az Explorer nézetek és a Vezérlőpult is.

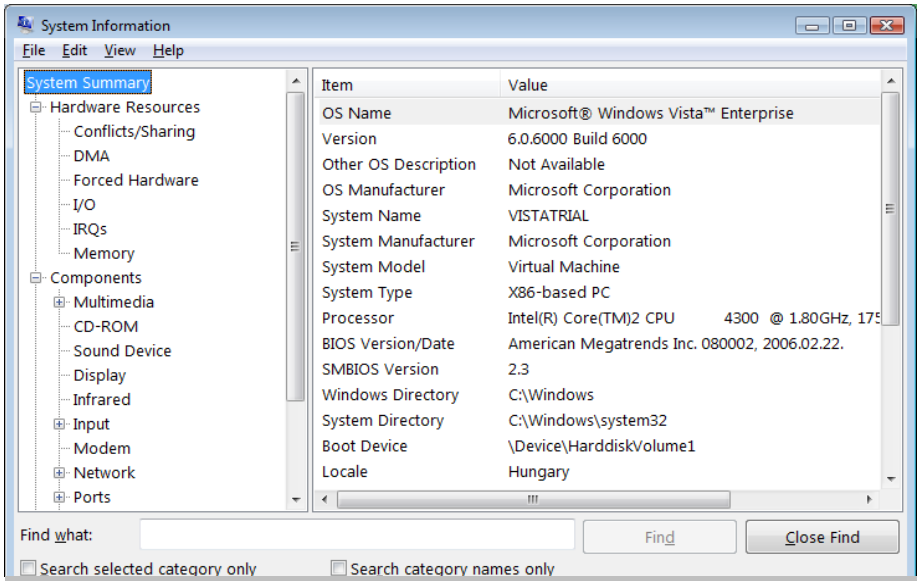


2.3. ábra: *Az Advanced Tools szakaszból számos hasznos eszközt indíthatunk el*

- **Adjust power settings** *(Energiaellátási beállítások módosítása)* – a számítógép energiatakarékossági funkcióival kapcsolatos beállításokat érhetjük el a hivatkozás segítségével.
- **Open Disk Cleanup** *(A lemezkarbantartó megnyitása)* – a fölöslegesen foglalt lemezterület (Lomtár tartalma, ideiglenes fájlok stb.) automatikus keresését és felszabadítását elvégző varázslót indíthatjuk el a hivatkozás segítségével.
- **Advanced tools** *(Speciális eszközök)* – a lap hivatkozásainak segítségével egy helyről indíthatunk el számos hasznos eszközt, amelyek további segítséget adhatnak a számítógép teljesítményével kapcsolatos finomhangoláshoz.

Diagnosztikai segédprogramok

A System Information eszköz *(Rendszerinformáció, msinfo32.exe)* a számítógép hardverkonfigurációjáról, a számítógép egységeiről és szoftvereiről, például az illesztőprogramokról jelenít meg információkat. Az eszköz a megjelenített adatokat a Windows Management Instrumentation- (WMI-) technológia segítségével gyűjti össze. Az eszköz bal oldali táblájában a kategóriák (és azokon belül az egyes eszközök) felsorolása, jobb oldali táblában pedig a kiválasztott eszköz adatainak részletezése jelenik meg.



2.4. ábra: *A System Information felületén csak a konfigurációs adatok megjelenítésére van lehetőség, a beállításokat itt nem módosíthatjuk*

A System Information eszköz által megjelenített adathalmaz bővíthető, vagyis a számítógépre telepített programoktól függően az itt szereplőkön kívül további kategóriákat is találhatunk a listában. Alapértelmezés szerint a következő kategóriák jelennek meg:

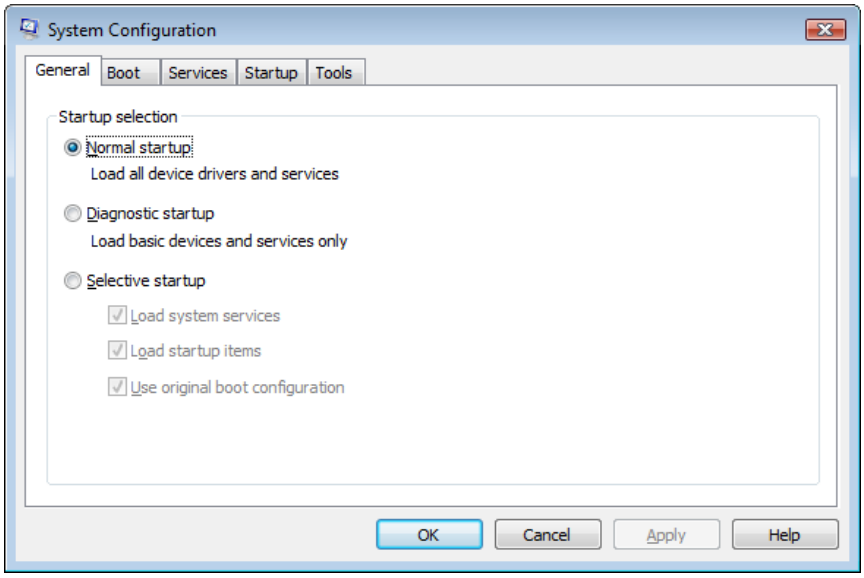
- **System Summary** *(Összefoglaló a rendszerről)* – ebben a szakaszban a számítógépre és az operációs rendszerre vonatkozó általános információkat találhatunk, például a számítógép nevét és gyártóját, a memória mennyiségét, a BIOS típusát stb.
- **Hardware Resources** *(Hardvererőforrások)* – ebben a szakaszban a megosztott rendszererőforrásokra vonatkozó adatokat találhatunk, itt jelennek meg például az egyes eszközökhöz tartozó I/O-portok és megszakítások, DMA-csatornák stb.
- **Components** *(Összetevők)* – ebben a szakaszban a számítógép különféle komponenseire (például lemezmeghajtók, hangeszközök, modemek stb.) vonatkozó adatok jelennek meg.
- **Sofware Environment** *(Szoftverkörnyezet)* – ebben a szakaszban az illesztőprogramokról, hálózati kapcsolatokról és egyéb programokhoz kapcsolódó részletekről kaphatunk információt.
- **Applications** *(Alkalmazások)* – opcionálisan itt jelennek meg az egyes alkalmazásokhoz tartozó további adatok, például az Office-programra vonatkozóan igen részletes adatokat találhatunk ebben a szakaszban.

Amennyiben egy konkrét adatot szeretnénk megkeresni, használhatjuk az ablak alsó részén található Find what *(Keresendő szöveg)* mezőt.

A System Configuration alkalmazás *(Rendszerkonfiguráció, msconfig.exe)* olyan speciális eszköz, amely a Windows-rendszer indítását megakadályozó problémák azonosítását segíti. Az eszköz segítségével beállíthatjuk, hogy a rendszer indítása bizonyos szolgáltatások és automatikusan induló programok nélkül történjen.

A következőkben röviden áttekintjük a System Configuration alkalmazás egyes lapjait és a lehetséges beállításokat.

- **General** *(Általános)* – ezen a lapon a számítógép indítási módját (a következő rendszerindításra vonatkozóan) választhatjuk ki. A szokásos indítás mellett lehetőség van a hibakeresési üzemmódban és a rendszergazda által kiválasztott szolgáltatásokkal és illesztőprogramokkal történő indításra is.



2.5. ábra: *A System Configuration felületén a rendszer indításának különféle paramétereit állíthatjuk be*

- **Boot** *(Rendszerindítás)* – itt az operációs rendszer indítására és különféle speciális hibakeresési beállításokra vonatkozó lehetőségeket találunk. A kiválasztható opciók nagyjából megegyeznek az F8 billentyű lenyomásával (rendszerindítás közben) elérhető Advanced Boot Options *(Speciális rendszerindítási beállítások)* menü lehetőségeivel. (Az egyes menüpontok használatával a hatodik fejezetben részletesen is foglakozni fogunk.)
- **Services** *(Szolgáltatások)* – a listában a rendszerindítás során betöltött valamennyi szolgáltatást megtalálhatjuk, azok jelenlegi állapotával együtt [Running *(Fut)* vagy Stopped *(Leállítva)*]. Lehetőségünk van az egyes szolgáltatások engedélyezésére, illetve tiltására is (a következő rendszerindításra vonatkozóan).
- **Startup** *(Indítás)* – a listában a rendszerindítás részeként automatikusan elinduló alkalmazásokat találhatjuk meg. Ha egy alkalmazást a következő indításkor nem szeretnénk elindítani, egyszerűen törölhetjük a mellette lévő jelölőnégyzetet.
- **Tools** *(Eszközök)* – Áttekintő listát jelenít meg a futtatható diagnosztikai, és egyéb speciális eszközökről (Computer Management *(Számítógép-kezelés)*, TaskManager *(Feladatkezelő)*, EventViewer *(Eseménynapló)*, regedit stb.).

Felügyeleti alapeszközök és segédprogramok
Ebben a screencastban megismerkedhetünk többek között a Task Manager és a a Resource Monitor újdonságaival, valamint áttekintjük a Performance Information and Tools programcsoport elemeit.
Fájlnév: I-2-1-Felugyeleti-alapeszkozok.avi

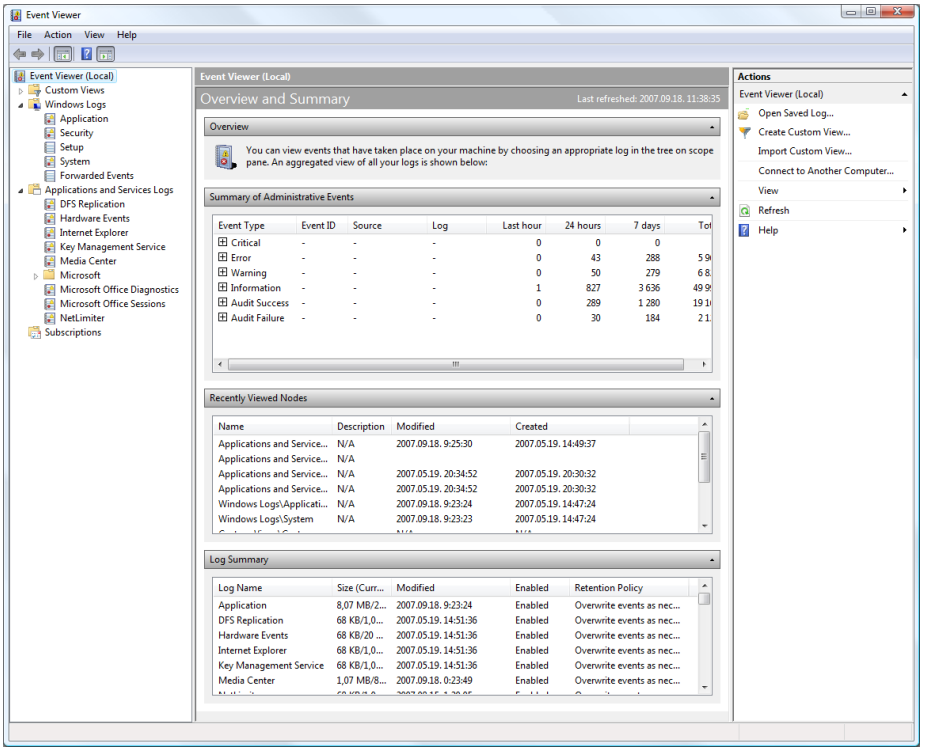
Haladó felügyeleti eszközök

Az Eseménynapló *(Event Viewer)*

Az eseménynapló a Windows-rendszerek és rendszergazdáik legfőbb és egyben legnépszerűbb hibakereső eszköze. A Felügyeleti eszközök *(Administrative Tools)* közül elérhető eseménynapló egyetlen központi helyre gyűjti össze az operációs rendszer komponensei (és sok esetben a külső alkalmazások) működése közben bekövetkezett fontosabb események listáját. A Vista megújult eseménynaplója teljesen új felhasználói felületet kapott, ezért nemcsak a működésben, és a kezelésben, hanem a megjelenésben, és az áttekintési lehetőségekben is több logikus és praktikus újdonságot tapasztalhatunk.

Az eseménynapló – mint lényegében minden felügyeleti eszköz a Windows-ban – egy MMC 3.0-bővítményként töltődik be. A nyitóképernyő három fő területből tevődik össze. A bal oldalon láthatjuk az előre definiált naplónézeteket, majd a különböző naplófájlokat több csoportban, illetve legalul a speciális naplófeliratkozások tárolóját. A középső szekcióban az indítás utáni gyors áttekintés érdekében a közelmúltban bekövetkezett legfontosabb események listája található, valamint a legutoljára megtekintett naplók és egy összesítés a naplók állapotáról. A jobb oldalon – amint az az új MMC-ben általánossá vált – egy feladat-, illetve utasításlistát érünk el, mely a középső keret kiválasztott elemeihez igazodva dinamikusan változik. Vegyük észre azt, hogy ha egy bejegyzésen állunk éppen a kurzorral, akkor a feladatlista láthatóan két külön részből áll: a felső részben az adott naplófájllal, az alsó részben pedig a konkrét bejegyzéssel kapcsolatos műveleteket érhetjük el.

A korábbi eseménynaplókban rettenetes mennyiségű információt halmozott fel az operációs rendszer, alapesetben – ügyféloldalon – mindösszesen csak három kategóriában. Ez ahhoz vezetett, hogy rendkívül nehéz volt megtalálni a szükséges információt, hiszen keresés nélkül csak az ömlesztett formában láthattuk a bejegyzéseket. A Vistában az egyik legfontosabb változás a naplófájlok területén a strukturáltság kialakítása, azaz, hogy minél kevesebb erőfeszítéssel, minél hamarabb megleljük a megfelelő bejegyzést, komponensekként és szolgáltatásonként csoportosítva.

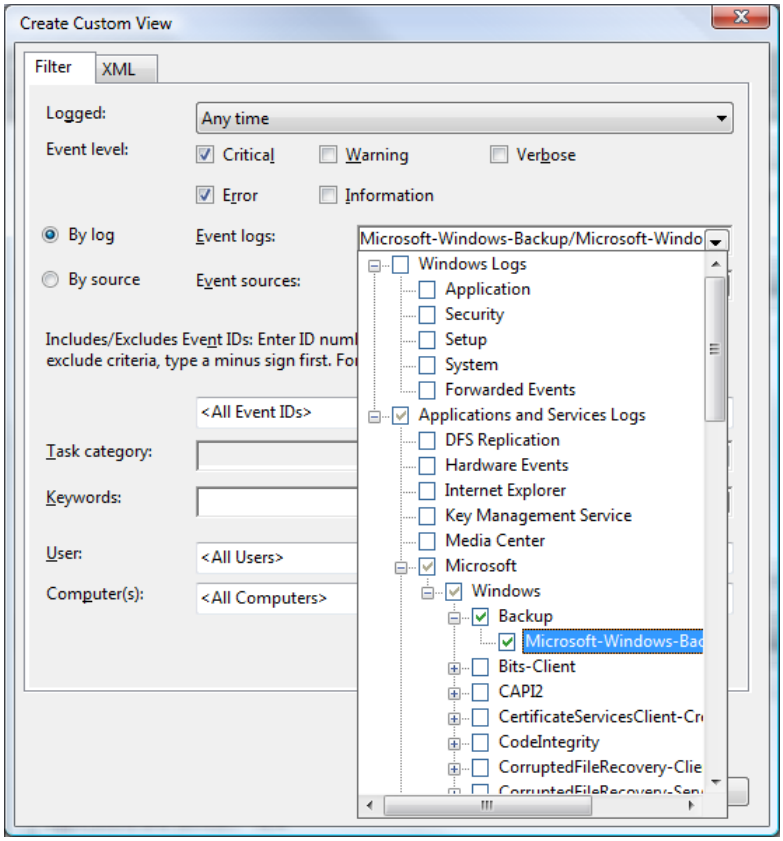


2.6. ábra: *Az Eseménynapló az elindítás után máris informatív*

A naplófájlok két fő csoportban találhatóak, a szokásos Windows-naplók (Windows Logs) az Alkalmazásnaplón *(Application Log)*, a Biztonsági naplón *(Security Log)* és Rendszernaplón *(System Log)* kívül kiegészültek egy telepítési naplóval, illetve a külső gépekről érkező naplók tárolójával *(Forwarded Events)*. A nagy változás viszont nem itt van, hanem kissé lentebb tekintve: bekerült egy új rész is a fa-könyvtárszerkezetbe Applications and Service Logs *(Alkalmazás és szolgáltatásnaplók)* néven. Itt lényegében az összes Windows-szolgáltatást és rendszerösszetevőt megtalálhatjuk (a Microsoft mappában pl. közel ötvenet), de bővíthetősége folytán akár külső alkalmazások is beépíthetik ide saját eseménynapló-tárolójukat.

Eseménynapló — áttekintés és a naplófájlok
Ez a két mini előadás segítséget nyújt az Eseménynapló teljesen új felépítésének elsajátításában.
Fájlnév: I-2-2a-Esemenynaplo-attekintes.avi, I-2-2b-Esemenynaplo-naplofajlok.avi

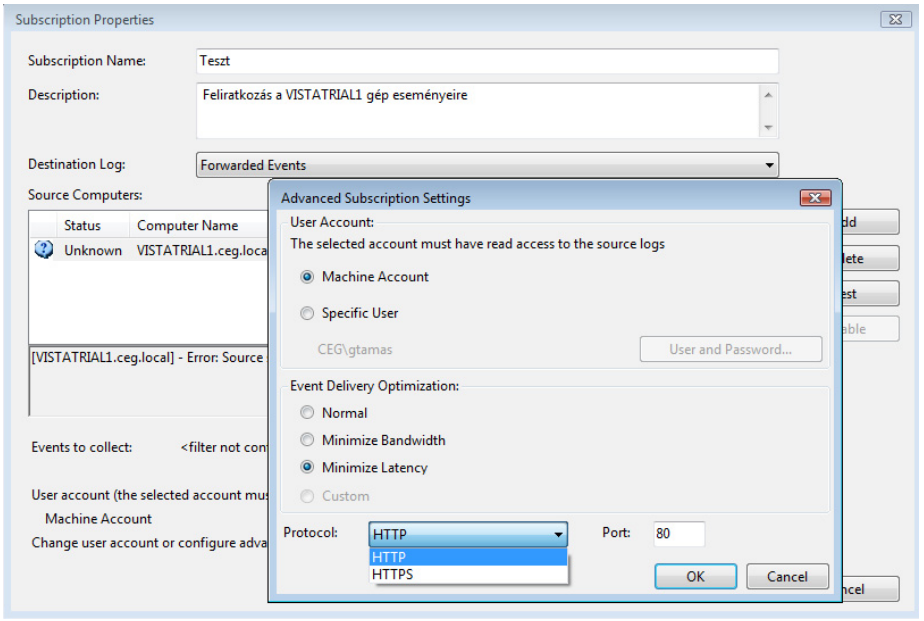
A strukturált elrendezésen kívül, több új elemet és szolgáltatást is láthatunk ebben a faszerkezetben. Vegyük sorra ezeket!



2.7. ábra: *Az egyéni nézeteknél bármely naplókategóriából választhatunk forrást*

- **Custom Views** *(Egyéni nézet)* – Az új eseménynaplóban lehetőségünk van saját, testreszabott naplónézeteket létrehozni és elmenteni, amelyek tartalma természetesen frissül is majd automatikusan, egy-egy új bejegyzés apropóján. Ha csak egy-egy adott sorszámmal rendelkező eseményre, vagy csak egy eseménytípusra vagyunk kíváncsiak, itt egy rendkívül részletes szűrővel (amelyet egyébként még számos további helyen is használhatunk majd) meghatározhatjuk a vizsgált halmazt. Megadhatunk akár többszörös feltételeket is, valamint – szintén újdonságképpen – többféle naplótípusból is válogathatunk egyszerre eseményeket *(Cross-log queries)*. Az általunk lementett egyéni nézetek mentés után bekerülnek ebbe a mappába, és természetesen utólag is szerkeszthetőek, másolhatóak, vagy akár exportálhatóak is egy másik gépre.

Eseménynapló — egyéni nézetek
Ez a screencast az események testreszabott szűrését megvalósító megoldásról szól, érintve az ún. Cross-Log Queries megoldást, azaz a keresztbehivatkozást a szűrőfeltételeknél.
Fájlnév: I-2-2c-Custom-Views.avi



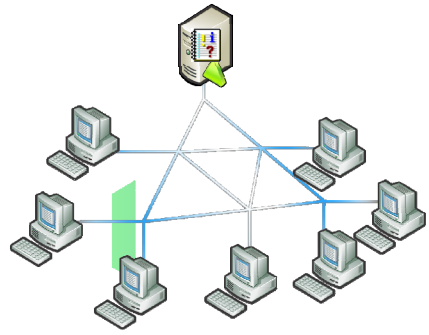
2.8. ábra: *A naplóküldés jogosultsági beállításai és optimalizálása*

- **Forwarded Events** *(Továbbított események)* – A Vista eseménynaplója nemcsak a helyi gépről, de a hálózat segítségével elérhető további számítógépek naplójából is képes információkat lekérdezni. Ehhez a Subscriptions *(Csatlakozás más számítógéphez)* bejegyzés alatt fel kell iratkoznunk a távoli gép eseménynaplójának figyelésére. A célirányos információgyűjtés érdekében természetesen itt is megadhatunk szűrési feltételeket, például naplótípust, eseménytípust, időpontot, az esemény forrásául szolgáló rendszerkomponenst, eseményazonosítót, értékhatárokat és különböző kulcsszavakat. A távoli gépek naplóbejegyzései alapértelmezésként a Forwarded Events gyűjtőmappába kerülnek, gépnév szerint rendszerezve, ám a célmappát a feliratkozáskor szabadon megadhatjuk. A gépek közti kommunikáció folyhat standard HTTP, de akár titkosított HTTPS-protokollon is, de megadhatunk egyéni TCP-portot is. A sávszélességgel történő takarékoskodás érdekében lehetőségünk van optimalizálni az adattovábbítást, vagy akár prioritást is adni a kapcsolatnak.

Eseménynapló — események küldése és összegyűjtése
Ebben az előadásban több különböző gép fogja beküldeni a Vistát futtató gyűjtő számítógépre az előzetesen kiválasztott Eseménynapló részleteket.
Fájlnév: I-2-2d-Event-Forwarding.avi

Az Event Subscription technikai feltétele, hogy minden naplóküldő gépen elérhető és beállítható legyen a WinRM-szolgáltatás (a WS-Management részeként), illetve a fogadó gépen szükség lesz a WS-Eventing protokollra is.

- **WS-management** – A Microsoft és számos más IT-nagyvállalat (pl. IBM, Sun, Intel, AMD, Dell stb.) által közösen kifejlesztett, SOAP-szabványra épülő rendszerfelügyeleti technológia, mely lehetővé teszi a felügyelt eszközök (legyenek azok szoftverek, vagy hardverek) egységes protokollon keresztül egyaránt elérhetők és kezelhetők legyenek. A Microsoft saját rendszereiben a .Net Web Service gondoskodik a WS-Management ellátásáról.
- **WS-Eventing** – Szintén webszolgáltatás-alapú protokoll, mely az események szállításáért felel. A Windows Vista szintén alapértelmezésként tartalmazza, a Communication Foundation – így a Microsoft .NET-keretrendszer – részeként azonban Windows XP-hez is elérhető.



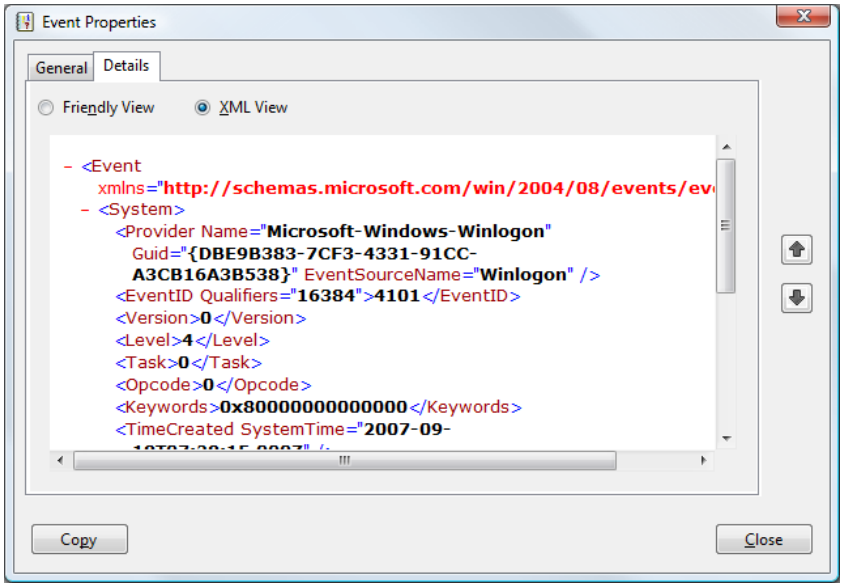
Mivel az adatgyűjtés az imént említett webprotokollokon keresztül zajlik, az egész művelet teljesen „tűzfalbarátnak” nevezhető, azaz egyszerű webszolgáltatásként kezelhetjük, valamint zökkenőmentesen együttműködik a már meglévő webes szolgáltatásokkal, például az IIS-sel. Bár a WinRM nem függ az IIS-től, ha mindkét szolgáltatás aktív, közös portokon (80, 443) kommunikálnak a hálózaton. A WinRM lefoglalja a */wsman* URL-előtagot, így az IIS-t üzemeltető rendszergazdáknak figyelniük kell rá, hogy a számítógépről publikált egyéb webes erőforrások (weblapok) ne használják ezt az előtagot.

A WinRM konfigurálásához használjuk *winrm quickconfig* parancsot, amely elindítja és automatikus indításúra teszi a WinRM-szolgáltatást, létrehozza a tűzfal kivételszabályát, valamint egy listenert, amelyen figyeli a beérkező kéréseket. A Vistán mindezt a rendszergazdai parancssorból (jobb gomb a parancssor ikonon és *Run as administrator*) indíthatjuk el. A WinRM-ről további részleteket találunk e fejezet utolsó előtti szakaszában.

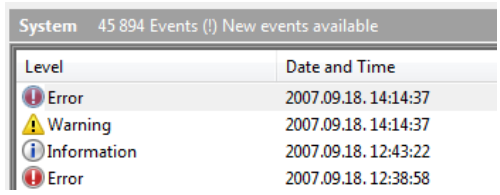
- **Analytic and Debug Logs** *(Elemzési és hibakeresési napló)* – A haladó hibakeresést szolgáló, részletes nyomkövetésre használható naplók alapértelmezésként nem látszanak az Eseménynaplóban, azaz igény szerint nekünk kell engedélyeznünk. Ezt megtehetjük a View *(Nézet)* menü Show Analytic and Debug logs *(elemzési és hibakeresési naplók megjelenítése*) parancsával. Ha bekapcsoljuk ezt a nézetet, számos új naplótípus tűnik fel a Microsoft főkönyvtáron belül, melyek például programfejlesztéskor és Windows-szolgáltatások hibakeresésénél nyújthatnak segítséget. Tudnunk kell azt is, hogy ezzel a paranccsal még nem indul el ezen speciális naplók feltöltése, ehhez egyesével kell az eddig rejtett naplófájlokon engedélyezni a működésüket. Látható tehát, hogy a használatuk csak több lépcsőben érhető el, és ez nem véletlen: ez a fajta intenzívebb naplózás jelentős mennyiségű erőforrást is elvonhat a rendszer többi részétől.

Az eseménynapló legnagyobb szerkezeti újítása, hogy immár a nyílt szabványokra támaszkodó XML-formátumra támaszkodik a bejegyzések megjelenítésénél és exportálásánál is. A strukturált XML-fájlok akár saját fejlesztésű alkalmazásból is lekérdezhetőek, így szorosabb együttműködés és kompatibilitás érhető el.

Bizonyos esetekben szükséges lehet a naplófájlok archiválása is, erre az eseménynapló több lehetőséget is kínál. Egyrészt lehetséges a naplók automatikus mentése, így a korábbi bejegyzések nem íródnak felül, valamint akár exportálhatjuk is az aktuális naplót különböző formátumokba. Az exportált állomány minden adatot tartalmaz az eseménnyel kapcsolatban, a főbb paramétereken túl a bejegyzés szöveges leírásával egyetemben minden bekerül a fájlba. A naplók mentéséhez az az új, XML-alapú *.evtx* formátumú fájlokon kívül továbbra is használhatjuk a szöveges *.txt* és pontosvesszővel tagolt *.csv* állományokat is. Az eseménynaplók archiválási és mentési beállításait az egyes naplók jobbkattintással elérhető helyi menüjében találhatjuk. Jó tudni, hogy egy régi, előző operációs rendszerekből származó, mentett eseménynapló fájlt *(.evt)* is megnyithatunk a Vistában, majd akár el is menthetjük, illetve konvertálhatjuk.

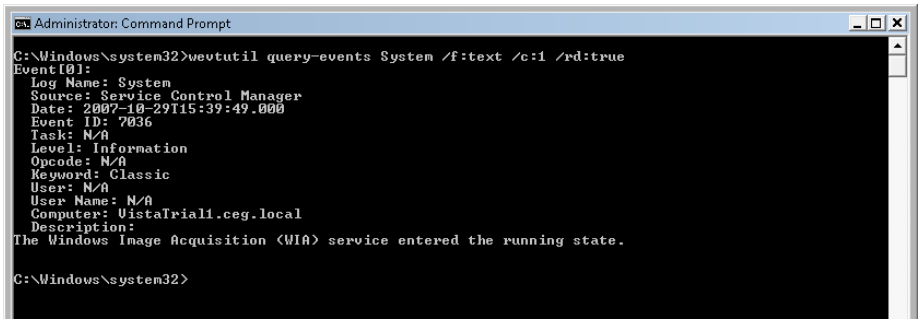


2.9. ábra: *Egy naplóbejegyzés XML-nézetben*



További újdonság, hogy ha éppen megnyitottunk egy naplót, új bejegyzés létrejöttekor a grafikus felületen, a fejlécben értesítést kapunk a lista bővüléséről. Ha ekkor frissítjük a nézetet, máris láthatóvá válnak az új események. Ha pedig nem találunk egy bejegyzést a hosszú listában, a Vista eseménynaplója végre a keresést is támogatja, melyet a jobboldali feladatsávból indíthatunk.

Az eseménynaplót nemcsak a grafikus felületről, hanem parancssori eszközzel is kezelhetjük. A *wevtutil.exe* parancs számtalan paraméterrel rendelkezik, melyekkel több feltétel szerint kérdezhetjük le az eseménynaplók bejegyzéseit, akár egyszerű szöveges, akár XML-formátumban. A *wevtutil.exe*-t akár külső alkalmazásból is meghívhatjuk, így lehetőség adódik automatizált adatgyűjtésre, vagy ütemezett feladatként, felügyelet nélkül is futtathatjuk azt. A felügyelet nélküli eseménykövetéshez egyébként nagy segítséget nyújt az eseménynapló és a feladatütemező szoros integrációja is, melyet a következő szakaszban ismertetünk.



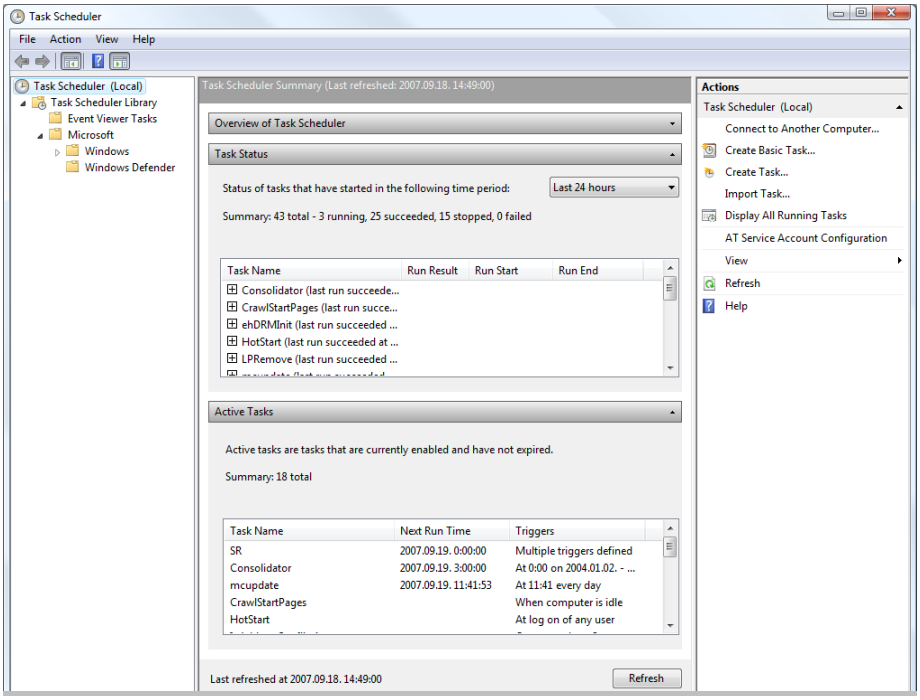
2.10. ábra: *Ha szükséges, parancssorból is elérhetjük az eseményeket*

A Feladatütemező

Az eseménynaplóhoz hasonlóan a Felügyeleti eszközök *(Administrative Tools)* között találhatjuk a rendszergazdák második legfontosabb szerszámát, a Feladatütemezőt *(Task Scheduler)*. Bár már a korábbi Windowsok is lehetővé tették időzített feladatok futtatását, a Vista feladatütemezője mellett akár el is bújhatnának, az új operációs rendszerben ugyanis egy rendkívül kifinomult eszközt kapunk kézhez. Több új időzítési opció, komplex feltételrendszerek állnak rendelkezésünkre, valamint szkriptekkel teljes egészében automatizálható a modul.

A feladatütemező megjelenése nagyban hasonlít az eseménynaplóéra, jobb oldalt a feladatkategóriákat láthatjuk fastruktúrában – melyek szintén külön-külön tartalmazzák a Windows beépített rendszerfeladatait – középen az úgynevezett Task dashboardon *(Leírássáv)* a soron következő és a legutóbb lefutott folyamatok sorakoznak, míg jobbra a már szokásos feladatsáv húzódik.

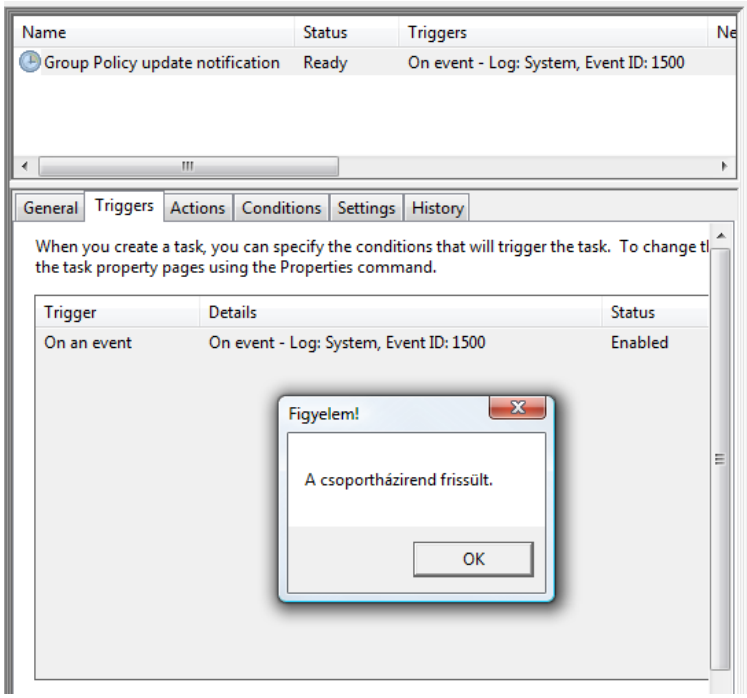
A bal oldali könyvtárszerkezetben az ún. Task Library (*Feladatütemező könyvtár)* ponton belül a *Microsoft\Windows* mappákban gyárilag előre definiált folyamatokat találhatunk, melyek az operációs rendszer különböző önkarbantartó és automatikus diagnosztikai eszközeit működtetik (például ütemezett töredezettségmentesítés vagy rendszer-visszaállítási pontok készítése). Ezek a bejegyzések alapértelmezésként nem látszanak, a View *(Nézet)* menü Show Hidden Tasks *(Rejtett feladatok megjelenítése)* parancsával jeleníthetjük meg őket. Lehetőség szerint ne állítsuk el, vagy tiltsuk le ezeket a feladatokat, de vizsgáljuk meg bátran a szerkezetüket, hiszen egyfajta példatárként is szolgálhatnak.



2.11. ábra: *A Feladatütemező nyitóképernyője*

A testreszabott, általunk készített időzített feladatok létrehozása során számtalan új lehetőség és paraméter áll rendelkezésünkre. A megújult varázslónak két változata is van, egy egyszerűbb Create Basic Task *(Alapfeladat létrehozása)* nevű, mely néhány alapvető paraméter megadásával felgyorsítja és megkönnyíti az ütemezés elkészítését, valamint az egyszerűen csak Create New Task *(Feladat létrehozása)* névre keresztelt, ahol egészen elképesztő részletességgel adhatunk meg minden szükséges opciót, illetve feltételt.

Az új feladatütemezőben az eseménynapló bejegyzéseihez is társíthatunk gyorsan és egyszerűen feladatot, amely gyakorlatilag egy Basic-típusú feladat lesz. Ha például értesülni szeretnénk egy bizonyos esemény bekövetkeztéről, nem szükséges folyamatosan a naplókat bújnunk, egyszerűen beállíthatunk egy üzenet-megjelenítést (vagy e-mail küldést) az eseménynapló működéséhez kötve. Ezt – az egyszerűség jegyében – akár az eseménynaplóban is megtehetjük, ehhez csupán a kijelölt naplóbejegyzésre kell kattintanunk a jobb gombbal, majd kiválasztanunk az Attach Task To This Event *(Feladat csatolása az eseményhez)* parancsot. Ilyenkor eleve rögzül az adott esemény azonosítója, kategóriája és forrása, így aztán más dolgunk nem is lesz a varázslóban csak eldönteni, hogy valamely program indítását kérjük, vagy egy üzenetablak megjelenítését a képernyőn, vagy – a megfelelő SMTP-konfiguráció birtokában – az említett e-mail küldés is könnyedén kivitelezhető.

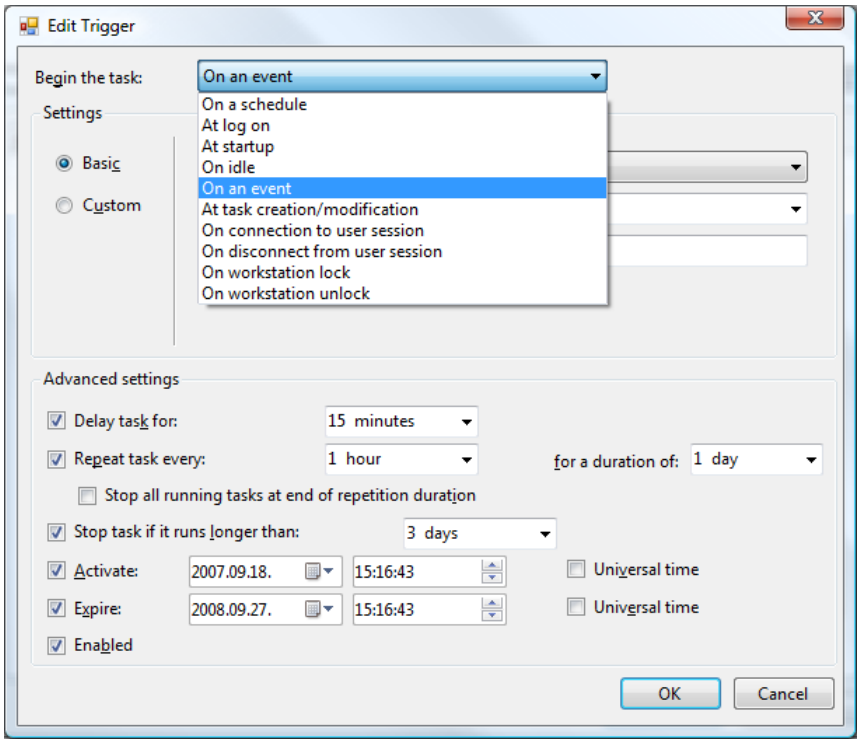


2.12. ábra: *Egy, az Eseménynapló bejegyzésén alapuló „Basic Task" üzent nekünk*

Az eseménynaplóból definiált időzítések a feladatütemező Event Viewer Tasks *(Feladatütemező könyvtár)* mappájába kerülnek.

Ha a szimpla nevű (de mégis sokkal összetettebb) Create New Task *(Feladat létrehozása)* varázslót indítjuk el, akkor rögtön, már a General *(Általános)* fülön szembetűnhet néhány fontos újdonság, pl. a User Account Control *(Felhasználói fiókok felügyelete)* kikerülését ebben az esetben indokoltan lehetővé tevő jogosultsági szint meghatározás [Run with highest privileges *(Futtatás legmagasabb szintű jogokkal)*] vagy pl. az adott feladat teljes elrejtése, amelyet immár bonyolult, közvetlen API-programozás helyett egy jelölőnégyzettel tehetünk meg. Látható az is, hogy az egyes feladatok, mivel Vista-specifikus tulajdonságokat is hordozhatnak, csak saját környezetben szerkeszthetők, de ha kompatibilitási módban tároljuk le azokat, menedzselhetővé válnak Windows 2000/XP, illetve Windows Server 2003 rendszerekről is.

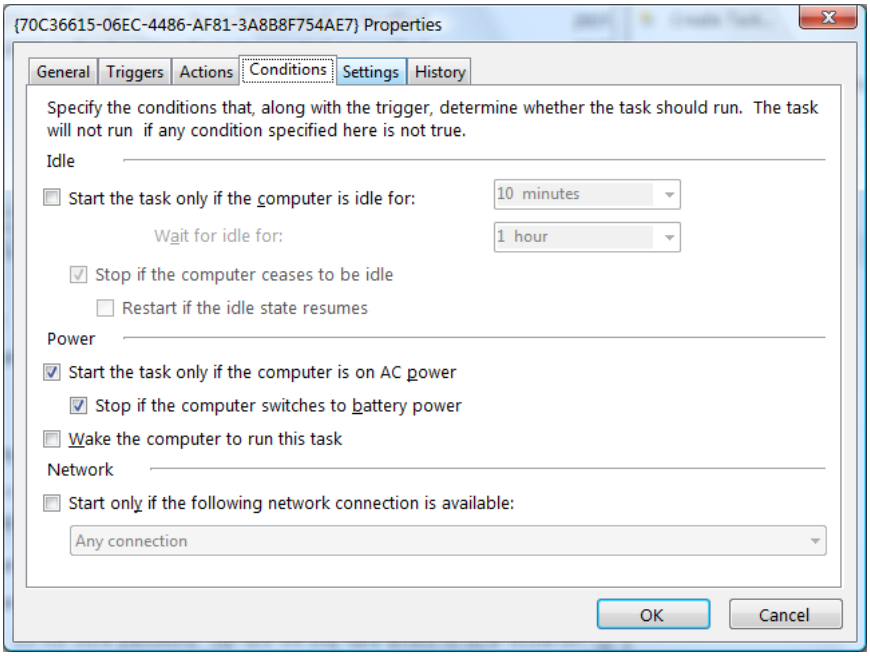
Az eseményeken kívül további indítási feltételekkel gazdagodott a feladatütemező, amelyeket a Triggers *(Indítás)* fülön vehetünk használatba. Ilyen újdonság például a munkaállomás zárolása/feloldása, vagy a felhasználói munkamenethez történő csatlakozás – legyen az helyi bejelentkezés vagy Távoli asztal *(Remote Desktop)* használatával létrejövő kapcsolat.



2.13. ábra: *Több új triggert is használhatunk*

A feltételeknél *(Conditions)* beállíthatjuk a feladatok indítására vonatkozó a gép üresjárattal kapcsolatos paramétereit. Ezen kívül a már meglévő energiagazdálkodási szempontok közé bekerült a hálózati konfiguráció vizsgálata is, így meghatározhatjuk, hogy egy adott feladat csak bizonyos hálózatra történő csatlakozás esetén fusson le.

A feltételeknél *(Conditions)* a már meglévő energiagazdálkodási szempontok közé bekerült a hálózati konfiguráció vizsgálata is, így meghatározhatjuk, hogy egy adott feladat csak bizonyos hálózatra történő csatlakozás esetén fusson le. További változás, hogy az „üresjárati idő” fogalmát a Vista kicsit másképp értelmezi, mint a korábbi rendszerek. Míg a régebbi Windowsokban az üresjárat azt jelentette, hogy a felhasználó egy megadott ideig nem kommunikált a rendszerrel — nem használta a billentyűzetet, sem az egeret — addig a Vistában egész más a helyzet. A feladatütemező akkor nyilvánítja üresjáratnak a rendszer működését, ha a képernyőkímélő fut, vagy az elmúlt 15 perc 80%-ában nem volt lemez-, illetve processzorhasználat. Ezt az állapotot a Windows minden 15. percben ellenőrzi, tehát, ha egy 30 perces üresjáratot feltételező ütemezés 10 percnyi üresjárat után aktiválódik, a feladat 5 percen belül elindul, hacsak az elmúlt 25 percben nem volt aktív a rendszer.



2.14. ábra: *A hálózati opciók teljesen újak*

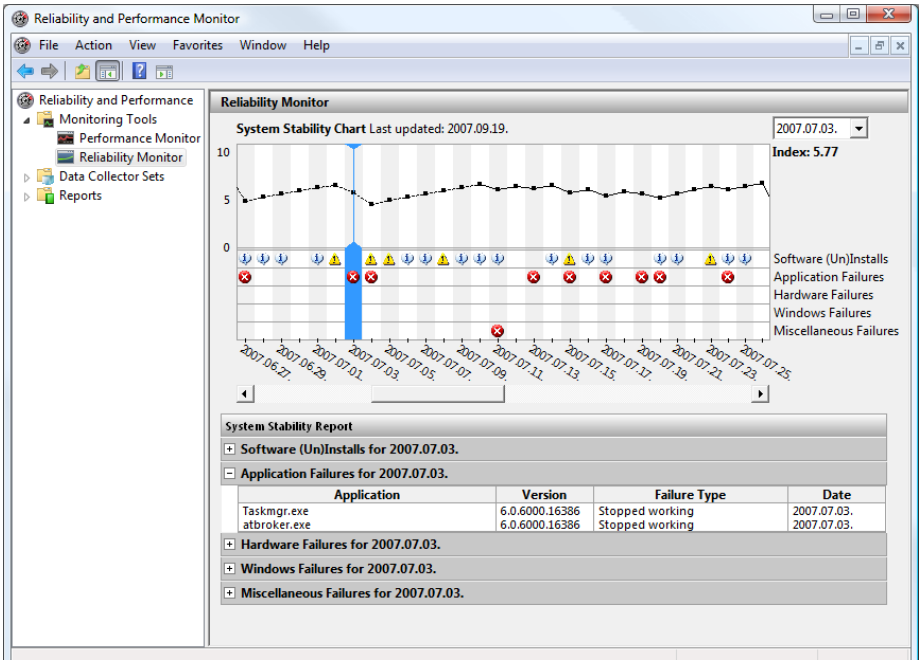
A feladatoknak megadhatunk határidőket is, melyek után elévülnek és így már nem futhatnak le, valamint különböző ismétlési és kivételes leállítási lehetőség is rendelkezésünkre áll a Setting (Beállítások) fülön.

A Feladatütemező
Ebben a screencastban megnézzük a teljesen megújult Feladatütemező egyszerű és összetett időzített feladatvégrehajtási képességeit, valamint teszteljük a Feladatütemező és az Eseménynapló közös lehetőségeit.
Fájlnév: I-2-2e-Feladatutemezo.avi

A megbízhatóság és a teljesítmény figyelése: Reliability and Performance Monitor

A Reliability Monitor *(Megbízhatóság- és teljesítményfigyelő)* a rendszergazdák egyik legnépszerűbb eszköze lehet, hiszen használatával nem szükséges az eseménynaplót végigböngészniük, vagy különböző naplófájlokban kutatniuk – egyetlen lapon láthatják a rendszer „EKG”-ját. A szolgáltatás követ minden a rendszerrel kapcsolatos eseményt, a programtelepítésektől kezdve az alkalmazáshibákon át, a rendszerleállásig, majd egy összesített grafikonon ábrá-

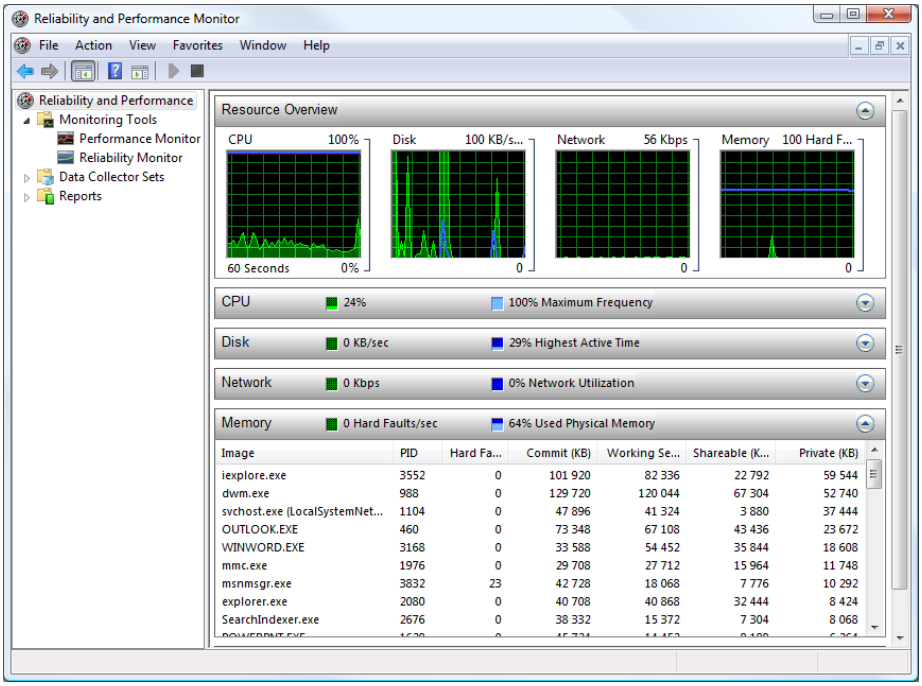
zolja a múlt történéseit – öt különböző sorban, a hiba vagy jelenség besorolásától függően. A grafikon 24 óránként frissül és egy-egy ellenőrzőpontnál rövid összefoglalást olvashatunk az aznapi bejegyzésekről. A rendszerstabilitást egy 10-es skála szerint osztályozza a szolgáltatás, melynek minden napi aktuális értéke megtekinthető visszamenőleg is.



2.15. ábra: *Akár hónapokra visszamenőleg is kiderülhetnek a turpisságok*

Az összetett eszköz másik modulja, a korábból már valószínűleg ismerős, de most új elemekkel és külcsínnel megjelenő, a teljesítménymérést szolgáló Performance Monitor *(Teljesítményfigyelő)*. Az eszköz nyitólapján egy áttekintő ábrát láthatunk, a négy legfontosabb erőforrás – a processzor, a merevlemez, a hálózat és a memória – pillanatnyi kihasználtságáról. Ha a részletekre vagyunk kíváncsiak, egyszerűen kattintsunk a megfelelő grafikonra és alább egy táblázatban láthatjuk az alkalmazások és szolgáltatások erőforrás-használatát, mindezt valós időben.

A Performance Monitor *(Teljesítményfigyelő)* akár felügyelet nélküli adatgyűjtésre is alkalmazható, ha azokat a későbbiekben szeretnénk analizálni. A bal oldali sávban elhelyezkedő Data Collector Sets *(Adatgyűjtő-csoportosítók)* mappában néhány gyárilag beállított adatgyűjtő beállítást találhatunk, de akár saját magunk is szabadon összeállíthatunk egyéni adatgyűjtést a számtalan processzorra, a memóriára, a diszkekre vonatkozó paraméter alapján.



2.16. ábra: *Alaposabb és pontosabb áttekintést kapunk a Vista Resource Monitorból*

A Performance Monitorban létrehozott kollektorok a feladatütemező szolgáltatással együttműködve futnak majd és így kollektorokhoz riasztásokat is társíthatunk, például, ha egy megfigyelt teljesítményszámláló egy megadott határérték fölé (vagy alá) kerül, előre meghatározott műveletet hajthatunk végre. A kollektorok egymásba is ágyazhatók, így az imént említett művelet akár egy másik mérés indítása is lehet. A mérési eredményeket – valós időben – különböző paraméterek szerint elhelyezett és elnevezett fájlba menthetjük, megadhatjuk a mintavételezések gyakoriságát, valamint az összegyűjtött adatok maximális számát is. Az elkészült fájlokon kívül természetesen a Performance Monitorban közvetlenül is követhetjük a mérési eredményeket, a generált jelentések pedig a Reports *(Jelentések)* nevű mappába kerülnek.

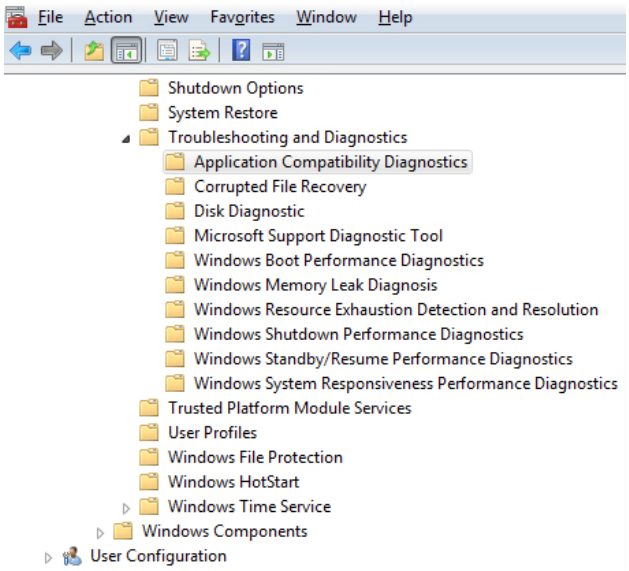
Reliability és Performance Monitor
Ez a két screencast a Reliability és Performance Monitor áttekintéséről, valamint ennek az összetett MMC-nek az első, teljesen új komponenséről szól.
Fájlnév: I-2-2f-RPM01.avi, I-2-2f-RPM02.avi

Rendszerszintű diagnosztikai eszközök

Az eseménynapló ugyan remek eszköz, mégsem képes minden szinten a rendszerrel kapcsolatos hiba felderítésére, különösen nem pl. a hardvereszközöket illetően. A Windows Vista több olyan diagnosztikai szolgáltatást is nyújt, melyek használata már régóta a rendszergazdák vágyai közé tartoztak, és amelyeket eddig többnyire csak külső eszközökkel tudtak helyettesíteni.

Diagnostic Policy Service

A Windows Vistában egy külön keretrendszer, az úgynevezett Windows Diagnostic Infrastructure (WDI) gondoskodik a különféle rendszerkarbantartó és hibaelhárító komponensek együttműködéséről. Ezek az eszközök közé tartozik a memória- és lemezellenőrző, a hálózati diagnosztika és az alkalmazások stabilitását és kompatibilitását felügyelő szolgáltatás, valamint a rendszerindítás sebességét automatikusan finomhangoló szolgáltatás is. A WDI-keretrendszer részeként működik a Diagnostic Policy Service *(a m. diagnosztikai házirendszolgáltatás)* (DPS), mely az egyes diagnosztikai modulok működését koordinálja a hibafelderítési és elhárítási folyamatok során. A DPS szokásos Windows-szolgáltatásként megtalálható a Services *(Szolgáltatások)* felügyeleti konzolban. A DPS lehetőségeinek további testreszabása a Helyi vagy a csoportházirenden keresztül történhet *(Computer Configuration/ Administrative Templates/System /Troubleshooting and Diagnostics)*, kismillió paraméterrel.



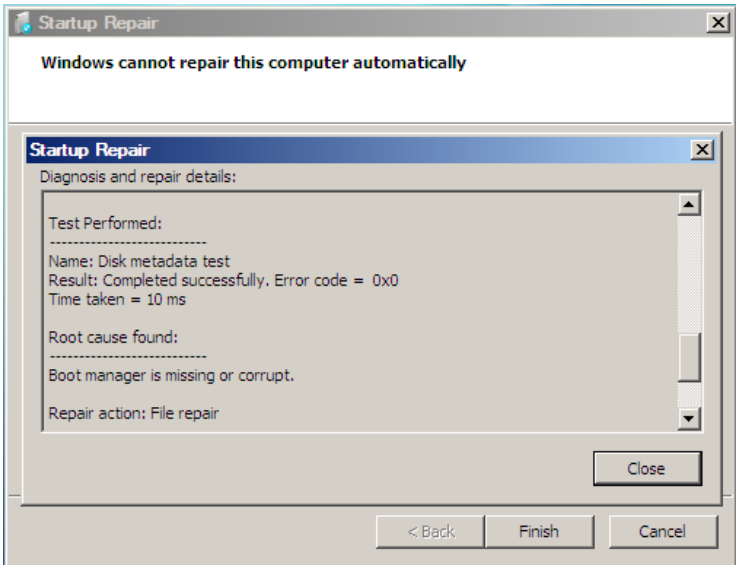
2.17. ábra: *A DPS házirend opciói*

Memória- és lemezellenőrzés

A fájlrendszer ellenőrzéséhez használatos CheckDisk *(chkdsk.exe)* már régóta része a rendszernek, a Vista ebből a segédeszközből is egy új verziót kapott, mely valamelyest részletesebb információkkal látja el az adminisztrátorokat. A *chkdsk* futtatható offline és online módban is, míg előbbi esetben egy másik számítógép rendszerlemezét vizsgáljuk, utóbbiban a rendszer „saját maga alatt" próbál rendet tenni az esetlegesen megsérült fájlrendszerben. Ha a *chkdsk*-t csak vizsgálati módban, paraméter nélkül futtatjuk, nem szükséges újraindítani a rendszert, ekkor azonban nem képes javításokat végezni a lemezen. Ha a segédprogramot a */F* (fix) kapcsolóval indítjuk a Windows következő újraindítása közben zajlik le a vizsgálat és a feltárt hibák, (index-adatbázis- és tartalomjegyzék-sérülések) javítása.

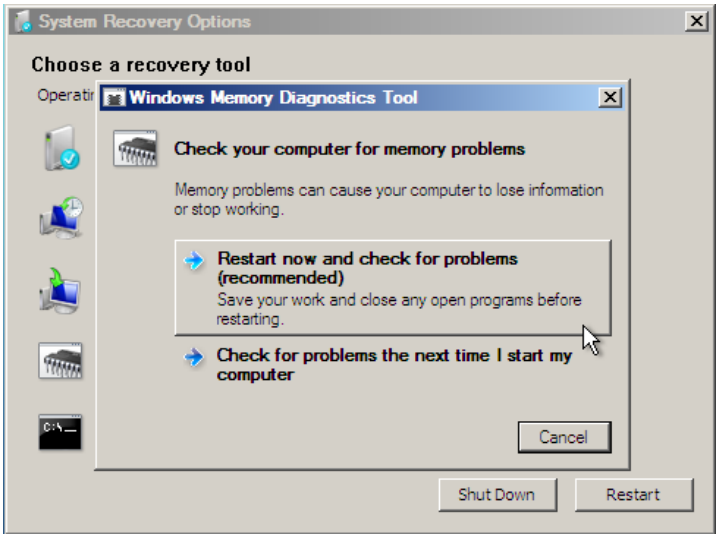
Rendszerindítási hibák

Arra az esetre, ha a Windows valamilyen oknál fogva nem indulna, a telepítő lemez tartalmaz egy Startup Repair Tool *(Indítási javítási eszközök)* nevű bővítményt, mely képes a leggyakoribb konfigurációs hibák, illetve sérült rendszerbetöltő fájlok javítására. Az eszközt a Windows telepítő menüjéből érhetjük el.



2.18. ábra: *A Startup Repair eszköz*

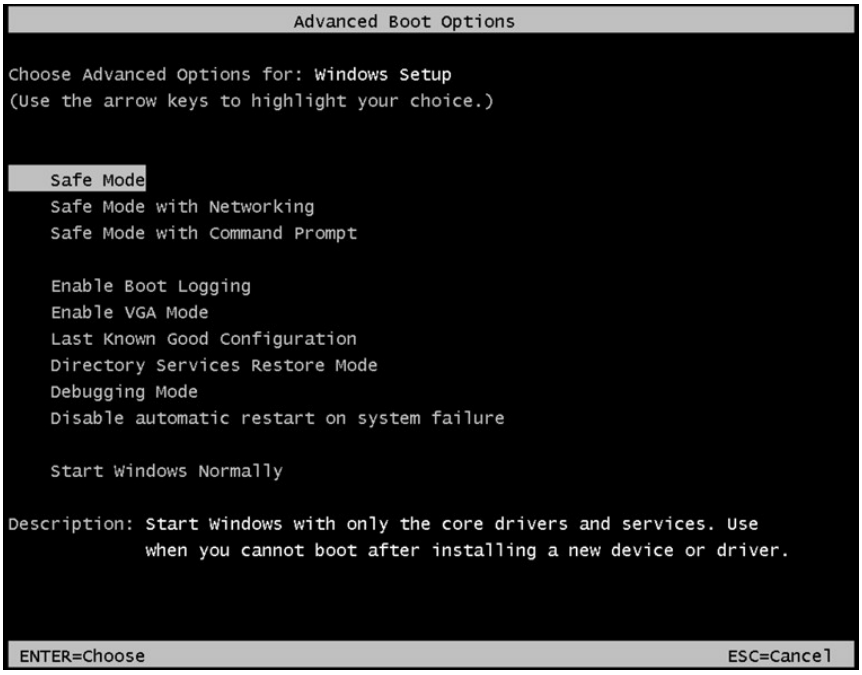
Szintén ugyanerről a helyről indíthatjuk a Windows Memory Diagnostics Tool-t, mely az operatív tár, vagyis a memóriamodulok épségét hivatott tesztelni. A korábban ismertetett memóriadiagnosztika a felügyeleti eszközökben is megtalálható, a teszt futtatásához azonban mindenképpen újra kell indítani a számítógépet.



2.19. ábra: *A memóriavizsgálatot csak újraindítás után érhetjük el*

Csökkentett mód

A korábbi rendszerekhez hasonlóan a Windows Vista is indítható úgynevezett Safe Mode-ban, azaz csökkentett módban, ahol csak a futáshoz legszükségesebb rendszerösszetevők és eszközmeghajtók töltődnek be. Csökkentett módban elvégezhetjük az esetleges hibás illesztőprogramok eltávolítását, vagy a rendszer helyreállítását a System Restore alkalmazással. Ha hálózati funkciókra is szükségünk van, rendelkezésre áll a hálózatos csökkentett mód [Safe Mode with networking *(Csökkentett mód hálózattal)*], illetve végső esetben – ha például a Windows Explorer sérült meg – a parancssoros üzemmód (Safe Mode with Command Prompt *(Csökkentett mód parancssorral),* ekkor nem jelenik meg az ablakkezelő, csupán egy parancsértelmezőt kapunk. A csökkentett mód beállításait a Windows indítása előtt közvetlenül leütött F8 billentyűvel érhetjük el a rendszerindító menüből.

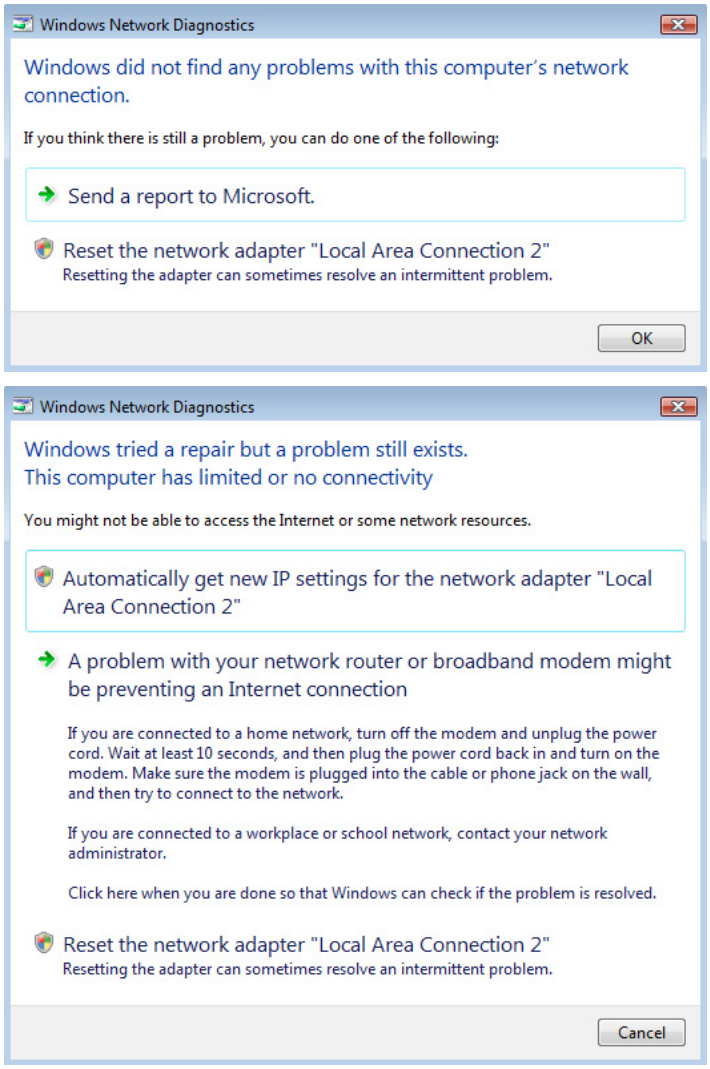


2.20. ábra: *Az indítómenü lehetőségei*

A csökkentett módról, illetve a rendszer indítómenü részleteiről a 6. fejezetben találhatunk további információkat.

Hálózati diagnosztika

Az első fejezetben a Network and Sharing Center *(Hálózati és megosztási központ)* ismertetésénél már néhány szó erejéig kitértünk a Vista integrált hálózati diagnosztikai eszközére. A szolgáltatás a háttérben fut és ha valamilyen problémát észlel a hálózati konfigurációban, vagy az adatátvitelben, automatikusan megvizsgálja az összeköttetést és a rendelkezésre álló lehetőségek szerint megoldási javaslatokat ad. A hálózati diagnosztika eszköz képes az olyan leggyakoribb konfigurációs hibákat önállóan megoldani, mint például rossz átjáró-cím megadása, IP-cím ütközés, sőt akár a biztonsági házirend korlátozásaira is felhívja figyelmünket, ha éppen az akadályozná a hálózat működését.

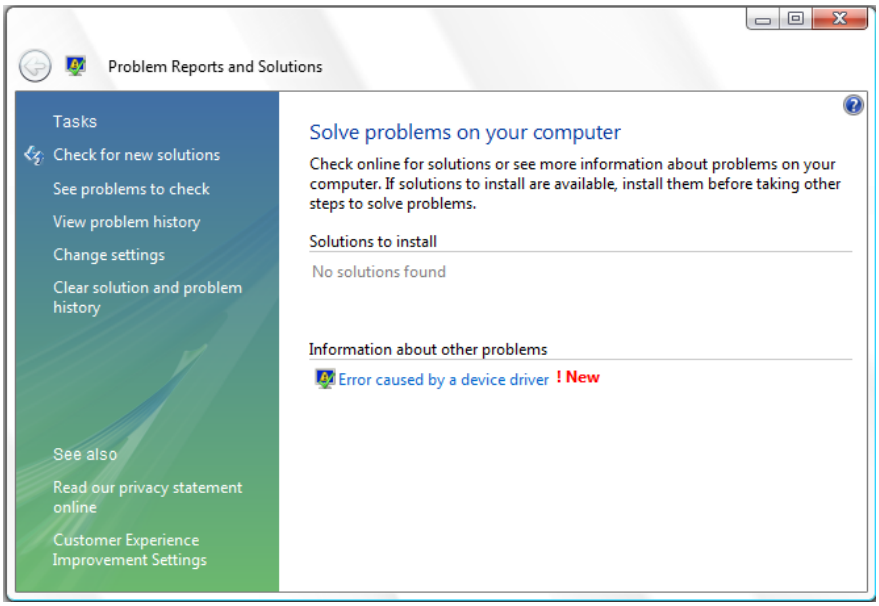


2.21. ábra: *A hálózati diagnosztika akcióban*

Hibajelentések

Míg Windows XP alatt, ha egy program vagy szolgáltatás hibába ütközött és leállt (lefagyott) akkor nem sok visszajelzést kaptunk a rendszertől, arról pedig kifejezetten keveset, hogy mégis mi okozhatta a problémát. A Windows Vistában viszont egy továbbfejlesztett hibajelentő mechanizmus került beépítésre. Az új Error Reporting *(Problémajelentések)* szolgáltatás nemcsak részletes jelentést küld a Microsoftnak az eseményről, hanem a korábbinál jóval intelligensebb módon, helyben értelmezi a hibát, majd megoldási javaslatokat

is nyújt a rendszergazdáknak, melyekkel gyorsabban – akár egy kattintással – elháríthatják a problémát. A Microsoftnál folyamatosan dolgoznak a leggyakrabban beérkezett hibák kijavításán, ezért fontos, hogy minél több hibajelentést küldjünk, hiszen ez nagyban segíti a programozók munkáját. Ha egy problémára idő közben sikerült megoldást találni, a hibajelentő szolgáltatás ezt közli velünk, és útbaigazít a teendőkkel kapcsolatban – például hivatkozást jelenít meg a program frissített verziójának letöltéséhez vagy akár egy eszközmeghajtó frissített változatára is felhívhatja a figyelmet.



2.22. ábra: *A hibajelentés/probléma megoldás szolgáltatás lényegesen intelligensebb lett*

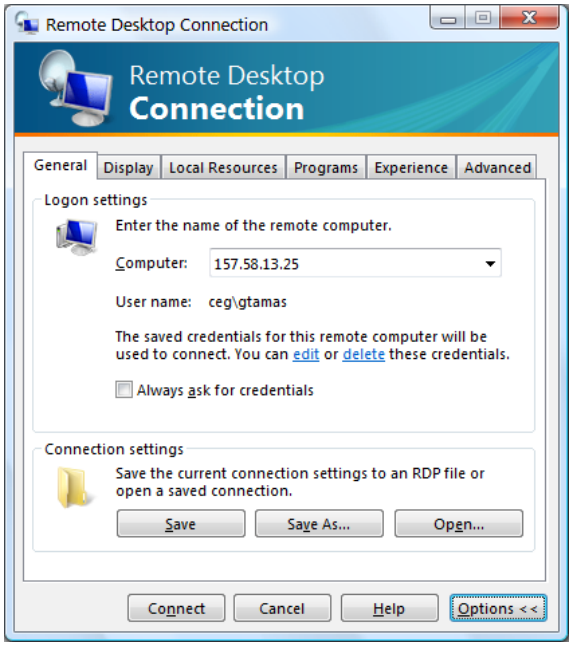
A hibajelentő szolgáltatás működése többféleképpen konfigurálható. Ha egy-egy programunk bizalmas információkkal dolgozik, felvehetjük azt egy kivétellistára, így a Windows az ezzel a programmal kapcsolatos hibákról csak alapvető információkat küld el a Microsofthoz, vagy – természetesen akár teljesen ki is kapcsolható a hibajelentés.

A távoli asztal

Hálózatunk számítógépeit nemcsak eléjük leülve helyben, hanem távolról is elérhetjük – akár az interneten keresztül is. A távoli gép teljes Asztalát magunk elé varázsolhatjuk, illetve az egérrel és a billentyűzettel is teljeskörűen vezérelhetjük. Ehhez a Remote Desktop Connection *(Távoli asztal)* alkalmazásra van szükség, amely ügyfelét egyszerűen elindíthatunk s saját gépünkön például a *Start / Run / mstsc.exe* paranccsal.

A távvezérelni kívánt géphez történő kapcsolódáshoz a távoli gépen a Terminal Services *(Terminálszolgáltatások)* szolgáltatás elindítása, valamint a 3389-es TCP port megnyitása szükséges, illetve engedélyezni is kell magát az RDP-t a rendszertulajdonságok között *(Control Panel \ System and Maintenance \ System \ Remote settings)*, és megadni azokat a felhasználókat, akik számára engedélyezett a távoli használat.

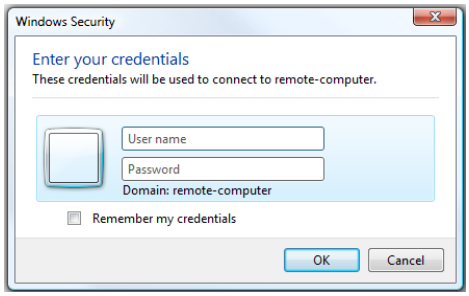
Ezután a távoli gép IP címét/nevét kell megadnunk, illetve esetlegesen az egyéb paramétereket beállítunk a megjelenítésre, a helyi erőforrások felcsatolására (pl. hang, mappák, nyomtatók stb.), az automatikusan elinduló alkalmazásokra vagy éppen a sebesség optimalizálására vonatkozóan. Ha mindent beállítottunk, célszerű az adott konfigurációt *.rdp* formátumban elmenteni, majd jöhet a kapcsolódás.



2.23. ábra: *Az új távoli asztal ügyfél*

Licenszelési okokból – mivel a Windows ügyfél operációs rendszerek egy időben egy felhasználó interaktív bejelentkezését teszik lehetővé – ha egy távoli asztal kapcsolattal rácsatlakozunk egy ügyfélszámítógépre, a helyileg bejelentkezett felhasználó asztala zárolódik (egy szerver operációs rendszer, pl. a a Windows Server 2003 esetén viszont 2 paralell +1 konzol típusú RDP kapcsolatunk is lehet egyszerre).

A Windows Vista a Remote Desktop Protocol 6.0-s verzióját tartalmazza, amelynek újdonságai a korábbi verziókhoz képest a következőek:



- Network Level Authentication *(NLA, a m. hálózati szint ellenőrzése)* – még a kapcsolat teljes felépülése előtt hitelesítenünk kell magunkat. Ez nagyban megnöveli a kapcsolat biztonságát, mivel már a bejelentkező képernyőig is csak az a felhasználó jut el, aki képes lesz bejelentkezni az adott gépre. Az NLA segít továbbá a szolgáltatásmegtagadásos (DoS) támadások kivédésében is, de alapesetben is kevesebb erőforrást igényel a kiszolgálótól.
- A hitelesítést elvégezhetjük akár SmartCarddal *(intelligens kártya)* is, mivel ez az eszköz is felcsatolhatóvá, azaz a távoli számítógép számára is láthatóvá vált.
- USB-csatlakozású, Plug&Play szabványt támogató eszközök felcsatlakoztatása, azaz, hogy a távoli gépen is elérhetővé váljanak – mindezt akár már kapcsolat közben is.
- A kiszolgálón (ez ebben az esetben a távoli gép) lehetőségünk van az RDP 6.0-nál korábbi ügyfelek kizárására.
- Kisebb erőforrásigény – az új ügyfél csak a képernyő aktuális változásait továbbítja, így csökkenti a számítógép és a hálózat terhelését.
- A Terminal Services Gateway (vagy RDP over HTTPS) támogatása – biztonságos, HTTPS-kapcsolaton és tűzfalakon keresztüli kapcsolódás lehetősége. Azaz a mi oldalunkon (ha mondjuk egy szállodában üldögélünk a laptopunkkal) egészen a hálózatunk tűzfaláig (amelyen tipikusan fut majd a TS Gateway kiszolgáló) nincs szükség az RDP-protokollra, a kapcsolat a mindenhol megengedett HTTPS-porton épül fel és bonyolódik.

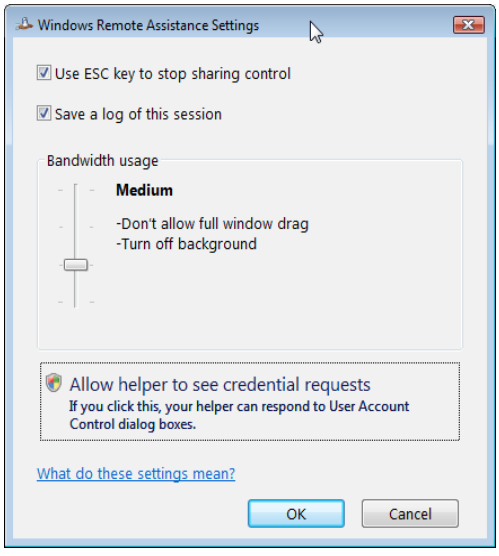
Persze, azt azért tudni kell, hogy a TS Gateway szerepkört csak a Windows Server 2008 bevezetése után használhatjuk majd, mindenesetre a Vista RDP kliense már most is fel van készítve arra, hogy ügyfele legyen ennek a szolgáltatásnak. Az RDP 6.0 frissítésként már Windows XP, illetve Windows Server 2003 rendszerekre is elérhető, erről a címről: *http://support.microsoft.com/kb/925876*, vagy akár a Windows / Microsoft Update szolgáltatáson keresztül is.

A távsegítség

Ha a felhasználóknak problémájuk akad a számítógép kezelésével, esetleg programhibába ütköznek és a rendszergazda nincs a helyszínen, a távoli segítségnyújtás remek megoldást kínál. A távsegítség szintén az imént tárgyalt RDP-t használja, a kapcsolat jellege szinte teljesen meg is egyezik, azzal a különbséggel, hogy ekkor a távoli gép előtt ülő felhasználó és a hálózatról felcsatlakozott segítségnyújtó is látja a képernyőn zajló eseményeket. A segítség a rendszergazda által nyújtható, de a felhasználó saját maga is kérheti, a meghívott fél viszont mindkét esetben csak akkor csatlakozhat fel a rendszerre, ha azt a helyi, a gép előtt ülő felhasználó jóváhagyja.

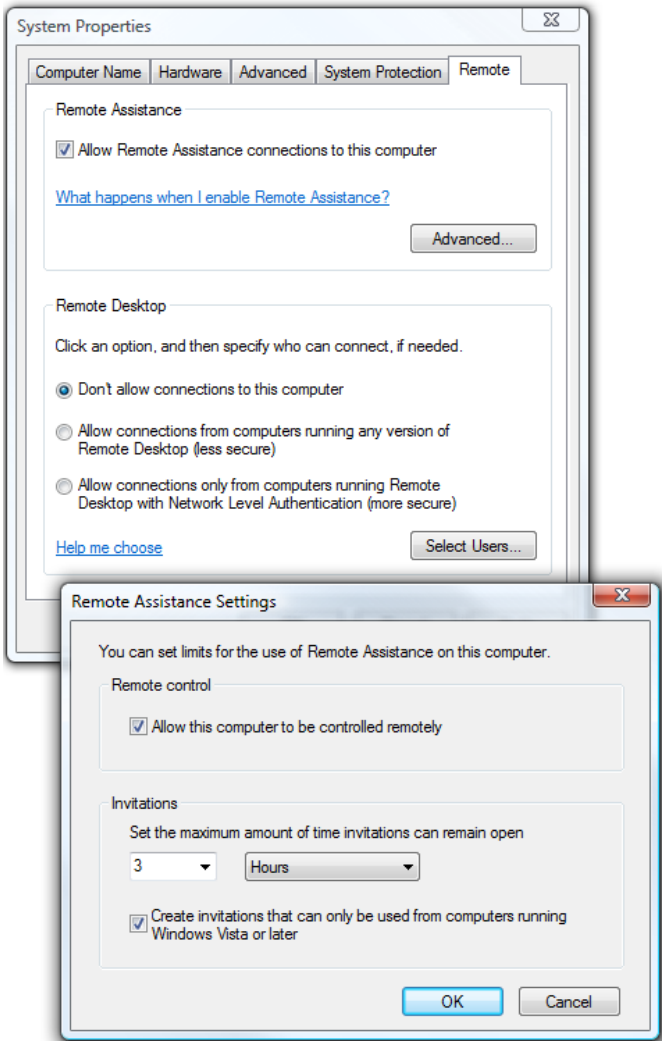
A meghívás többféle úton történhet, egyrészt a Windows Remote Assistance *(Távsegítség)* segédprogram által generált e-mailben vagy fájlban – mely a kapcsolódáshoz szükséges elérési útvonalat, paramétereket tartalmazza, vagy a Windows Live Messenger azonnali üzenetküldő szolgáltatáson keresztül, illetve akár a Windows Súgójából is.

A helyi felhasználó teljes mértékben kontrollálhatja a kapcsolatot, beállíthatja, hogy a meghívó mennyi ideig legyen érvényes, az asztal képe milyen részletességgel kerüljön átvitelre (ez kis sávszélesség esetén lehet szükséges), valamint bármikor megszakíthatja a kapcsolatot az „Esc” billentyű leütésével.



A Windows Vista új Remote Assistance *(Távsegítség)* szolgáltatása több biztonsági újdonságot is tartalmaz:

- Az NLA-hitelesítés alapján beállítható, hogy csak Windows Vista vagy újabb operációs rendszerről érkező kapcsolódást fogadhatunk el.
- „Pause” *(Szünet)* opció, arra az esetre, ha személyes adatokat kell megjeleníteni a képernyőn. Ekkor a távoli segítségnyújtó nem látja az asztalt, de a kapcsolat él.



2.24. ábra: *A távsegítség opciók*

- A User Account Control *(felhasználói fiók felügyelete)* hitelesítési ablakok blokkolhatók a távoli segítségnyújtó elől, így azokat csak a helyi felhasználó látja majd és tudja kezelni.
- A kapcsolat részletesebb naplózása mind a segítségnyújtó, mind az ügyfél gépén, ami az utólagos nyomkövetés miatt lehet fontos.

A Remote Assistance *(Távsegítség)* szolgáltatás beállításait a rendszertulajdonságok *(System Properties)* vezérlőpultelem bal oldali sávjában található Remote Settings *(Távoli beállítások)* hivatkozására kattintva érhetjük el.

A távsegítség *(Remote Assistance)*, és a távoli asztal *(Remote Deskop)*
Ez a két előadás a hasonló elven működő, de teljesen különböző célokból használt távfelügyeleti eszközök beállításairól és működéséről szól.
Fájlnév: I-2-2g-RA-RD.avi

A Windows-távfelügyelet (WinRM) és a távoli héj (WinRS)

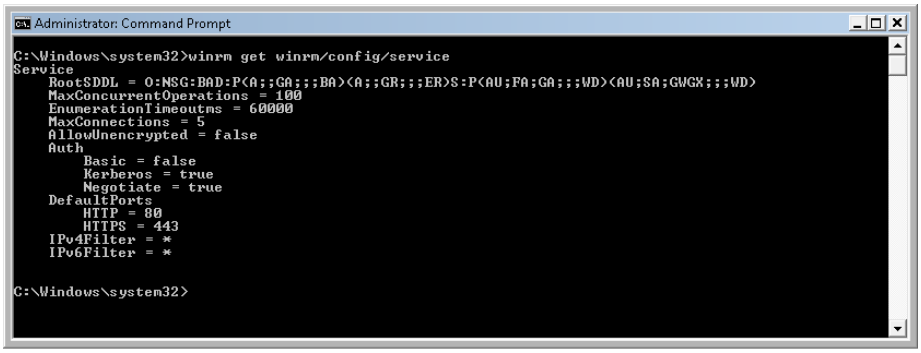
Az eseménynapló kapcsán pár szó erejéig már kitértünk a webalapú rendszerfelügyeleti szolgáltatásra, a WS-Managementre. A Windows Remote Management (WinRM) a WS-Management szabvány Microsoft által megvalósított implementációja, mely távoli számítógépek felügyeletét és menedzselését szolgálja – webprotokollokon keresztüli kommunikációja révén mindezt „tűzfalbarát" módon teszi lehetővé.

A Windows Remote Management *(Távsegítség)* komponens része a Windows Hardware Management szolgáltatásnak, mellyel teljeskörűen irányíthatjuk helyből vagy távolból a számítógépeket. A szolgáltatás implementálja a WS-Management-protokollt, hardveres diagnosztikát és ellenőrzést tesz lehetővé, emellett a kiszolgáló szoftveres távvezérlésére is alkalmas – a parancssorból.

A csatlakozás tűzfalbarát módon, biztonságos körülmények között történhet meg, HTTP, illetve HTTPS-protokollokon és többféle hitelesítési módszert (Basic, Digest, Kerberos) is alkalmazhatunk.

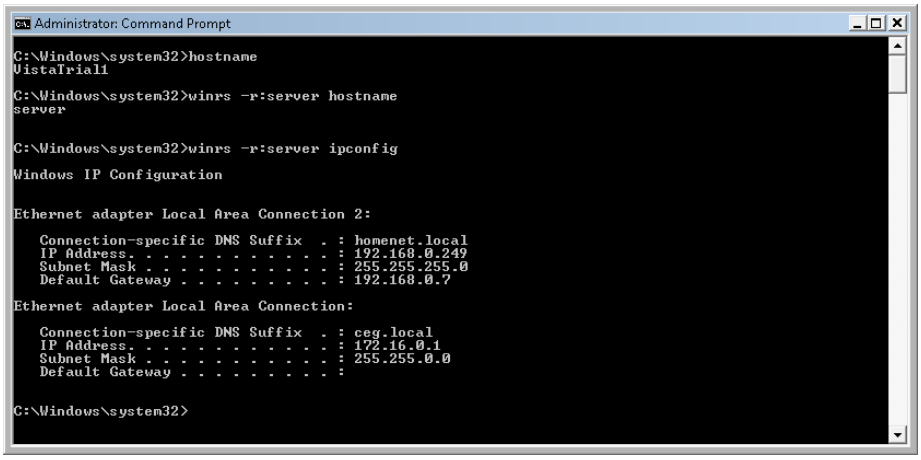
A Windows Vista tartalmazza a WinRM szolgáltatást, de annak használatához először élesíteni kell. A távoli parancssoros eléréshez szükséges automatikus beállítás a következő paranccsal történik: *winrm quickconfig*. Ezzel elindítjuk és automatikus indításúra állítjuk a WinRM-szolgáltatást, beállítunk egy úgynevezett „HTTP listener"-t a WS-Management-protokoll üzeneteinek fogadására.

A WinRM alapértelmezés szerint a Kerberos hitelesítést használja a 80-as HTTP-porton, erről – és több egyéb, a szolgáltatást érintő paraméterről – meggyőződhetünk a *winrm get winrm/config/service* paranccsal.



2.25. ábra: *A WinRM-szolgáltatás állapotának lekérdezése*

Ha sikeresen beállítottuk a WinRM szolgáltatást a távoli gépen, akkor lehetőségünk lesz a WinRS-sel (Windows Remote Shell) kapcsolódni ehhez a géphez. Így bármilyen parancssori vagy szkriptműveletet elvégezhetünk a (figyeljük meg a következő ábrát), mindössze annak host nevét, IP-címét, vagy WinRM-aliasát kell ismernünk. A WinRS (Windows Remote Shell) használatáról bővebb információt a parancs súgójában olvashatunk. („*winrs -?*”)



2.26. ábra: *A WinRS-sel képesek leszünk a távoli gépen parancsokat futtatni*

Bár a WS-Management eredetileg csak a Vista és a Windows Server 2003 R2 operációs rendszerek beépített képessége, nemrégen elérhetővé vált egy frissítés (azaz az 1.1-es verzió) Windows XP SP2-höz és az R2 bővítés nélküli Windows Server 2003-hoz is (*http://www.microsoft.com/downloads/details.aspx?familyid=845289ca-16cc-4c73-8934-dd46b5ed1d33&displaylang=en*), mely a korábbi operációs rendszerekkel is elérhetővé teszi a távoli kezelést. Ezt a frissítést egyébként célszerű a Windows Server 2003 R2-es gépekre is feltenni.

Távoli parancssoros felügyelet WinRM/WinRS segítségével
Ebben az előadásban – több különböző operációs rendszert felhasználva – behangoljuk a WinRM működését, és a WinRS segítségével ki is próbáljuk a parancssoros távvezérlést.
Fájlnév: I-2-2h-WinRM-WinRS.avi

A helyi házirend

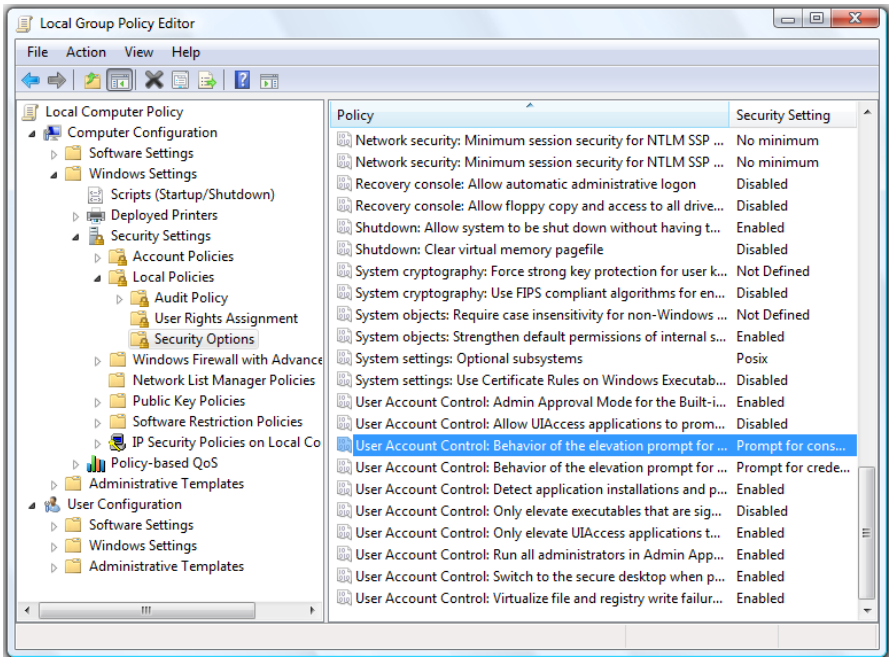
Windows operációs rendszerek esetén a házirend kiemelkedően fontos technológiának számít, az üzemeltetők és a cégek/szervezetek számára is létfontosságú az általa nyújtott biztonság és stabilitás. A házirend gyakorlatilag olyan szabálygyűjtemény, amelyet a felhasználók és a számítógépek beállítására, felügyeletére használunk. Egy korrekt módon felügyelt rendszerben a házirendek hatásainak nincs párja, ugyanis akár egyetlen helyről, a legelemibb részleteket tekintve is befolyásolhatjuk az egész infrastruktúránk működését. A segítségével többek között központilag konfigurálhatjuk a jelszó- és kizárási házirendet, az NTFS-mappák jogosultságait, az audit és eseménynapló beállításokat, a *logon/loggoff/startup/shutdown* szkripteket, a mappa átirányítást, és például a kihasználhatjuk a szoftvertelepítés vagy a központi nyomtatótelepítés előnyeit és ez csak egy nagyon szűk felsorolás. Vállalati környezetben, a Windows Server 2003 + Windows XP SP2 esetén az elérhető beállítások száma kb. 1800, míg a Vista ügyfélgépek esetén ez az érték 2400 körüli (összehasonlításul a Windows NT 4.0-ban mindösszesen 76 ilyen opció volt).

A statisztikák szerint a tartománnyal rendelkező vállalati rendszerek esetén a csoportházirend használata kb. 90%-os, kis- és középvállalati környezetben pedig 60%-nál is nagyobb mértékű.

Bár a házirendeket tipikusan nagy- és közepes vállalati környezetben alkalmazzuk, egészen kis szervezetek, speciális feladatú számítógépek (pl. internet kávézó, közös használatú oktatási gépek stb.), vagy akár szóló gépek esetén is jól használható a különféle biztonsági szabályok és megszorítások bevezetésére és fenntartására (pl. az Eszközkezelő *(Device Manager)* vagy a Feladatkezelő *(Task Manager)* tiltására, vagy a letöltött futtatható állományok elindítására, az Internet Explorer vagy éppen a tiltott alkalmazások futtatására).

A házirendekből két fő típust különböztetünk meg, az egyik a csak az adott számítógépre és az adott számítógép felhasználóira (helyi házirend), míg a másik egy szervezeti egység, tartomány, telephely határain belül, akár az összes gépre és felhasználóra vonatkozhat, függetlenül attól, hogy ki lép be az adott gépen, illetve attól is, hogy a felhasználó mely gépen lép be pl. a tartományba.

Mi a következőkben többnyire a helyi házirenddel foglalkozunk, a csoportházirendről viszont az 5. fejezetben olvashatunk további részleteket.



2.27. ábra: *A helyi házirend elemei a házirend-szerkesztőben (GPOE)*

Bár a Windows NT-k világában is volt lehetőségünk egyszerű házirendek létrehozására (System Policy), igazából a Windows 2000 óta használhatjuk a helyi házirendeket a mai módszerrel (bár a Vistával számos változás érkezett erre a területre is, lásd később). A helyi házirend kezeléséhez az ún. Group Policy Object Editort *(Csoportházirendobjektum-szerkesztő)* alkalmazzuk, amelyet különféle módon is el tudunk indítani. Egyrészt a *gpedit.msc* paranccsal pl. a Start menüből, vagy egy üres MMC-konzol elindításával és a Group Policy Object Editor bővítmény kiválasztásával. Ezek mellett az Administrative Tools *(Felügyeleti eszközök)* programcsoportban is találhatunk egy idevágó elemet, az ún. Local Security Policyt *(Helyi biztonsági házirend) (secpol.msc),* amely egy szűkebb halmaza az összes házirend opciónak, és amely – mint ahogyan a nevéből is kiderül –, elsősorban a biztonsági beállításokra koncentrál.

A házirendek működése a Windows regisztrációs adatbázisán alapul, az előzetes beállításaink alapján ennek „tetoválását” végzi el az adott felhasználó vagy számítógép belépésekor az operációs rendszer. A házirend-beállítások egy-egy úgynevezett csoportházirend-objektumban *(Group Policy Objects – GPO)* ta-

lálhatóak, amelyek egy-egy egyedi azonosítóval rendelkeznek *(Globally Unique Identifier GUID).* Akár a helyi akár a csoportházirendről van szó, a korrekt működéshez szükségesek az ún. házirend sablonok is *(.adm* kiterjesztéssel a *%windir%\inf* mappában találjuk meg ezeket – kivéve a Vistát, lásd később), amelyek alapesetben az operációs rendszer telepítésével kerülnek fel a gépekre, de frissülhetnek is pl. egy szervizcsomag telepítésekor, vagy akár manuálisan is bővíthetjük a saját sablonjainkkal a lehetőségeket.

Az általános bemutatás után, most érkeztünk el ahhoz a ponthoz, hogy a Windows Vista helyiházirend-megoldásával kapcsolatos változásokról ejtsünk szót.

Szerkezeti, működésbeli változások

Az elmúlt hét évben (a Windows 2000 kiadása óta) a házirendek működésében és szerkezeti felépítésében nem sok változás történt. A Vistában viszont (természetesen a Windows Server 2008-hoz hangolva) számos, az alapokat is érintő eltéréssel is számolhatunk. Az első, és talán az egyik legfontosabb változás az önálló Group Policy *(Csoportházirend)* rendszerszolgáltatás megjelenése, amely a korábbi, a winlogon processztől függő működést váltja fel. A szétválasztás miatt házirendek érvényesülése gyorsabb és kisebb terheléssel történik, újraindítás nélkül bővíthető a rendelkezésre álló opciókészlet, és pl. egy hibás működés apropóján a szolgáltatás (esetleges automatikus) újraindítása meg is oldhatja a problémákat.

A korábbi operációs rendszereknél a *winlogon* processz „egy menetben" és gyakorlatilag automatikusan csak a belépéskor töltötte be a gép indulásakor a GINA-t (Graphical Identification and Authentication – az interaktív belépés és a biztonságos hitelesítés szolgáltatása a Windows operációs rendszereknél, *msgina.dll)* egyéb esetleges belépési, illetve hitelesítésszolgáltatókat, illetve a házirend részeit is.

Egy másik rendszerszolgáltatás a Network Location Awareness (NLA) 2.0-ás változatának bevezetése is számos helyen tesz jó szolgálatot a házirendek feldolgozásánál. Az NLA működése miatt az operációs rendszer érzékennyé vált a hálózati körülmények változásaira, azaz pl. ha egy házirend feldolgozás az adott hálózati kapcsolat bizonytalansága miatt megszakad, akkor, ha újra detektálja a kapcsolatot, a feldolgozás képes automatikusan folytatódni, nem kell kivárni a szokásos 90 perce érvényesülése intervallumot, vagy a manuális kényszerítést (a *gpupdate* paranccsal). Az NLA miatt nincs szükség a korábban a kapcsolat detektálására használt ICMP-protokollra sem, amely a tűzfalak alkalmazása szemszögéből nézve is szerencsés újdonság, de az NLA rendelkezik még olyan lehetőségekkel is, mint automatikus sávszélesség de-

tektálás, illetve (mivel nemcsak a belépésnél működik, hanem menet közben is), pl. a VPN-ügyfelek kapcsolódáskor megkaphatják a rájuk vonatkozó házirendobjektumokat, amely a következő forgatókönyv szerint mehet végbe:

1. A VPN-ügyfél csatlakozásánál a Group Policy ügyfél detektálja a tartományvezérlő elérhetőségét
2. Ha a házirend frissítés ciklusa lejárt, vagy sikertelen volt, a GP-ügyfél háttérbeli frissítést kér a VPN-en keresztül [a User/Computer *(Felhasználó/Számítógép)* ágra egyaránt]
3. Így nincs szükség újraindításra vagy kijelentkezésre

Létezik egy másik, a házirendekkel kapcsolatos terület, amelynél még régebbi alapokon áll a rendszer, és ez pedig a házirend sablonok „világa", ahol gyakorlatilag a Windows NT4 óta „megállt az idő", ugyanazt az *.adm* kiterjesztésű, rugalmatlan felépítésű, kevésbé praktikust megoldást alkalmazza az operációs rendszer. Ennek a Vistával vége, mert ugyan a feldolgozás továbbra is a registryn keresztül zajlik, a sablonok XML-alapúvá lettek *(.admx)* és egyúttal a tartalmuk a szokásos 4 alapfájl helyett, több mint 130 különböző fájlban találhatóak meg. Az új formátum lehetővé teszi a nyelvfüggetlen működést is, ugyanis a semleges, neutrális részeket összeragaszthatjuk a nyelvspecifikus részekkel (attól függően, pl. hogy milyen az operációs rendszer nyelve, és milyen egyéb nyelvi csomag van telepítve a gépünkön), azaz a házirend elemek feliratainak és magyarázatainak fordításaival.

Az összes új sablont megtaláljuk az új helyén a %windir%\PolicyDefinitions mappában, a nyelvfüggő részeket pedig ugyanit egy <országkód> mappában, .adml formátumban.

A szerkezeti, működésbeli változások körében, meg kell említenünk még azt a pozitív fejleményt is, hogy a házirendek naplózásával és hibakeresésével kapcsolatos rettenetes erőfeszítéseknek is vége szakadhat. Ez azért lehetséges, mert a – valószínűleg sokak számára ismerős – *Userenv.log* féle követhetetlen naplózás helyett az új eseménynaplóban külön naplókategóriába került a házirendekkel kapcsolatos események egy része. Azért csak egy része, mert a Rendszernaplóban *(System log)* is megmaradnak a házirendekkel kapcsolatos, inkább az üzemeltetőkre vonatkozó események bejegyzései, viszont a konkrét működéssel kapcsolatos események leírása, érthető és értelmezhető formában (felhasználónév, GPO-lista, dátum, feldolgozási idő stb. felsorolással) az új kategóriában található meg.

A helyi házirendek
A Windows Vistában sokat változott helyi házirend általános bemutatása.
Fájlnév: I-2-3a-Helyi-hazirendek.avi

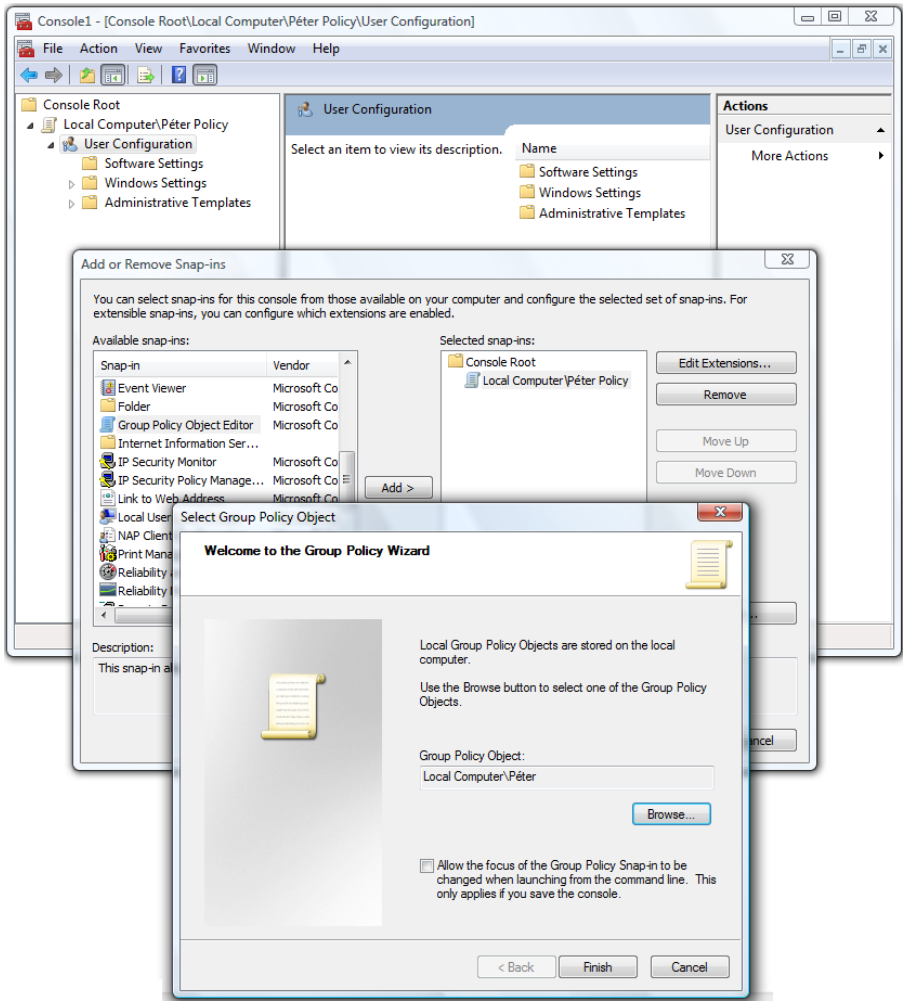
Felhasználókra és csoportokra érvényesíthető házirendek

Azok, akik már használták valaha egy-egy gép helyi házirendjét a különböző korlátozások bevezetésére, nagyon jól tudják, hogy akár a gépről, akár a felhasználókról volt szó, csak egyfajta házirend objektumot volt lehetséges létrehozni. Így aztán a létrehozó (általában *admin* jogosultságú) felhasználó ugyanúgy a házirend érvénye alá esett, ami ha pl. korlátoztuk a rendszereszközökhöz történő hozzáférést, alaposan visszaüthetett. Természetesen így nem volt lehetőségünk arra sem, hogy a rendszer további felhasználóit különféle módon korlátozzuk, sőt az előbb említett létrehozó *admin* felhasználó mentességét is csak spéci és rugalmatlan trükkökkel lehetett megoldani.

A Windows Vistában ez a helyzet is megváltozott, a rendszer összes felhasználójához akár külön-külön is tudunk saját házirendet rendelni, így az egyes fiókok más és más beállításokkal működhetnek –, illetve két csoportot is (Administrators és Non-Administrators) is megkülönböztethetünk a házirend-beállításokkal. A felhasználók VAGY az Admin VAGY a nem-Admin házirendet kapják, mindkettőt viszont értelemszerűen nem lehetséges érvényesíteni ugyanazon felhasználói fiókon.

Ennek megfelelően a házirendobjektumok feldolgozási sorrendje is módosult. Elsőként a felhasználó csoportjára vonatkozó beállítások jutnak érvényre, majd következnek a felhasználószintű beállítások. Ezek után (mellett) a számítógépre vonatkozó házirend is érvényesül (amelyből értelemszerűen továbbra is csak egyetlen egy lehet), végül – ha rendelkezünk kiszolgálóról működtetett tartományi házirenddel – akkor ez az objektum kerül feldolgozásra. A később alkalmazott házirendek mindig magasabb rendűek az előzőeknél, így egy helyi házirend sohasem írhat felül egy a tartományból, a tartományvezérlőkről érkező beállítást, sőt, egy tartományban – a Vista-ügyfelek esetén – a helyi házirend érvenyesülése akár teljes egészében le is tiltható („Exclude processing of all local GPOs") – a Csoportházirenddel.

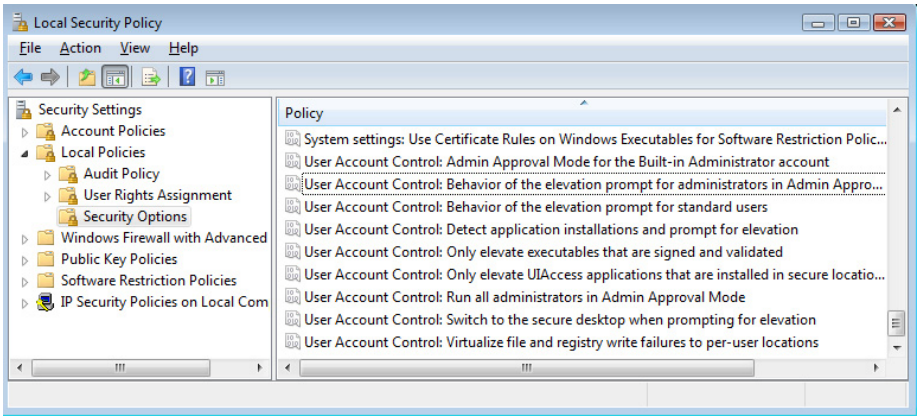
Felhasználószintű csoportházirend-objektum létrehozásához egy üres MMC-konzolt kell nyitnunk az *mmc.exe* paranccsal, majd a File *(Fájl)* menü Add/Remove Snap-in… *(Beépülő modul hozzáadása/eltávolítása)* menüpontjára kattintva nyissuk meg a rendszeren elérhető MMC beépülő modulok listáját. Válasszuk a Group Policy Object Editor *(Csoportházirendobjektum-szerkesztő)* modult, majd az Add -> *(Hozzáadás)* gomb megnyomása után tallózzuk be a kívánt felhasználói fiókot. Az így beállított konzolnézetet el is menthetjük egy *.msc* fájlba (pl. a felhasználó nevével), így a későbbiekben már nem kell ezt a műveletsort elvégeznünk.



2.28. ábra: *Innen indulhat a felhasználókra /csoportokra érvényes házirend készítése*

Gyakorlati példák

A helyi házirendben is sok-sok opció áll rendelkezésünkre a számítógép és a felhasználói profilok működésének testreszabásához, persze tisztában kell lennünk azzal a ténnyel, hogy az elérhető opciók száma nagyságrenddel alacsonyabb a helyi házirendek esetében mint a tartományi környezetben. Ennek az állításnak viszont némiképp ellentmond a Windows Vista, amelyben a helyi gép hatókörében alkalmazható lehetőségek száma is drasztikusan megnőtt.



2.29. ábra: *Helyi házirend*

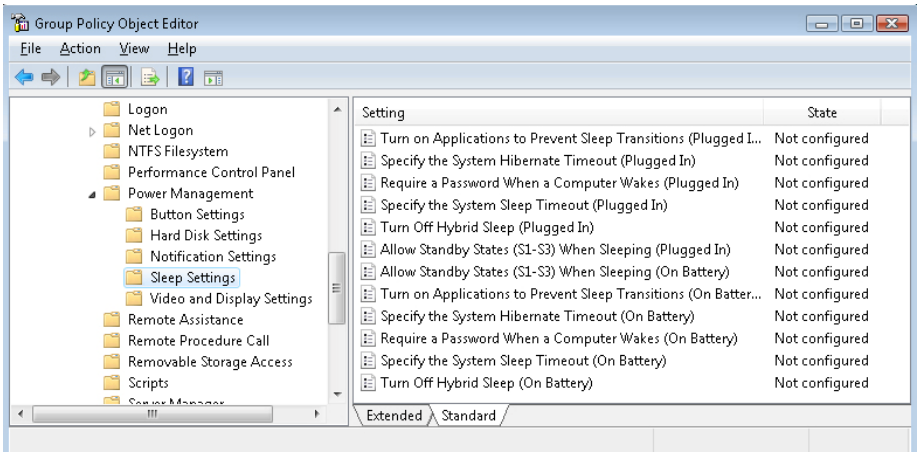
Az alábbi listában néhány további új, vagy megújult házirend opciót emelünk ki, a teljesség igénye nélkül, először a házirendből módosítható **biztonsági beállításokra:**

- Windows Defender
  - A szolgáltatás engedélyezése/tiltása
  - A szignatúrák letöltésének konfigurálása
- Internet Explorer biztonsági zónák konfigurációja
- Windows Firewall with Advanced Security
  - A tűzfal és az IPSec kapcsolatok beállításainak teljes lefedettsége
- Eszköztelepítések ellenőrzése
  - Engedélyezés/tiltás különböző feltételeknek megfelelően
  - Eszköz azonosító alapján (csak bizonyos típusok használhatók)
- User Account Control működésének beállításai
  - Jogosultsági szint emelésének módjai
  - Secure Desktop használata
  - Fájlrendszer- és registry-virtualizáció engedélyezése/tiltása

Következzen – csak a felsorolás szintjén –- néhány további példa az új vagy a megváltozott házirend opciókra.

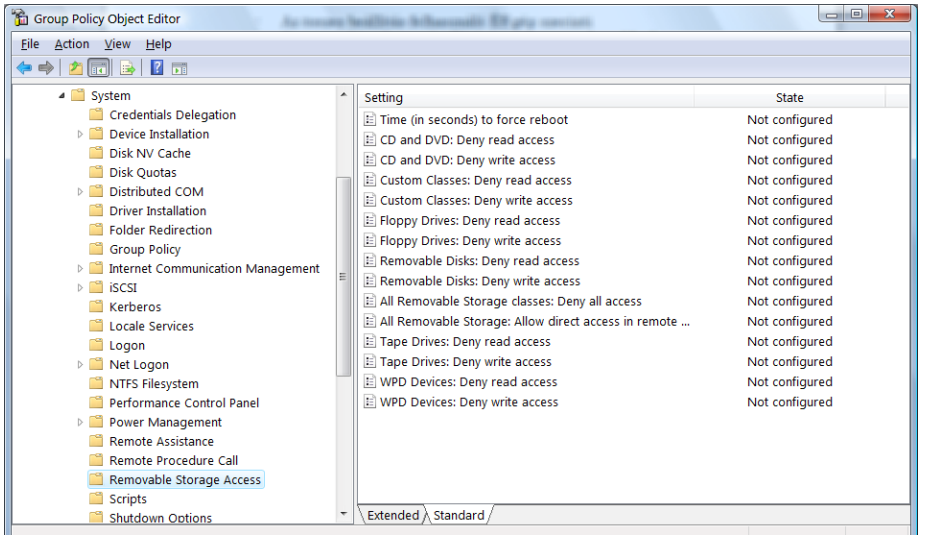
Energiaellátás

Az összes létező energiaellátási beállítás helyet kapott a Vista házirendekben, és persze van lehetőség egyéni sémák létrehozására is. Ez nem kevés anyagi megtakarítást jelenthet a cégek, szervezetek számára. Érdekesség a megoldásban, hogy a be nem lépett felhasználók számára is van szabály.



2.30. ábra: *Csoportházirend*

Tároló eszközök tiltása

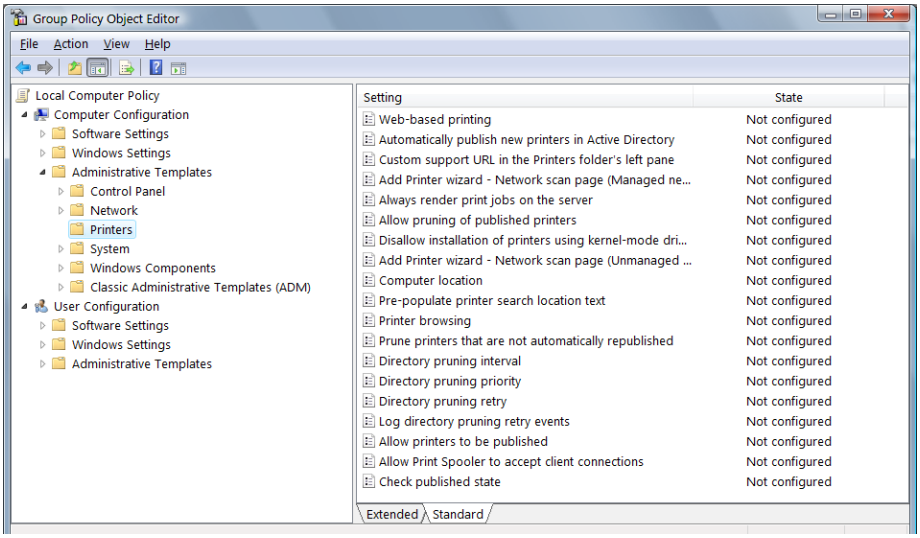


2.31. ábra: *Csoportházirend-szerkesztő – eltávolítható tárolók*

A házirenden keresztül tilthatóvá válik az USB-meghajtók, a CD-RW, DVD-RW és egyéb eltávolítható média használata. Írási és olvasási hozzáférés-típusok közül választhatunk és számítógépre, illetve felhasználóra is korlátozhatunk.

Nyomtatókkal kapcsolatos lehetőségek

Szintén teljesen új opció az adott nyomtató házirendből történő automatikus telepítése, illetve eltávolítása gépeknek, illetve felhasználóknak. Arra is van lehetőségünk, hogy a megbízható felhasználók számára delegáljuk a nyomtatók telepítését, illetve engedélyezzünk vagy tiltsuk a megbízható / nem megbízható illesztőprogram rendszerbe illesztését.



2.32. ábra: *Csoportházirend-szerkesztő – nyomtatók*

Gyakorlati példák a helyi házirendekre, eltérő felhasználói házirendek
Ebben az előadásban az új házirend opciók közül szemezgetünk, valamint megnézzük, hogyan lehet egy munkacsoportba tartozó gépen felhasználónként eltérő házirendet készíteni.
Fájlnév: I-2-3b-Helyi-hazirend-peldak.avi

HARMADIK FEJEZET

Az ügyfelek biztonsága

A fejezet tartalma:

Biztonság: általános bevezető

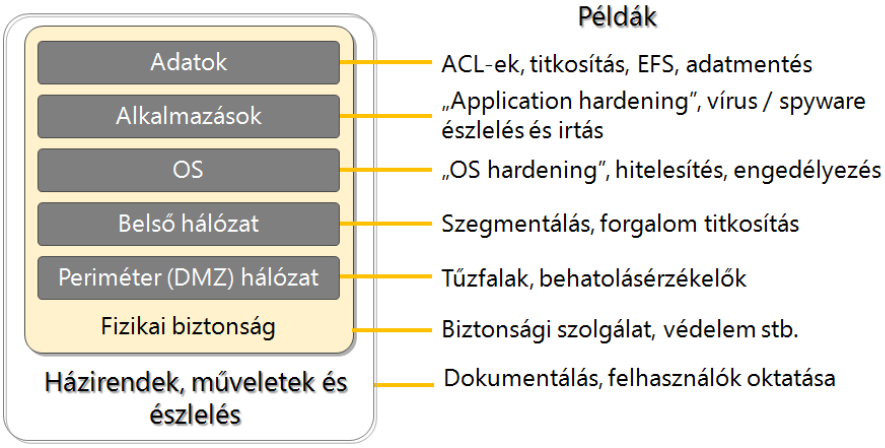
Ellentétben a régmúlttal, ma már sem az önálló számítógépek, sem a számítógép-hálózatok nem tekinthetők zárt rendszernek. A jelenben az informatikai eszközök milliói állnak egymással kölcsönös kapcsolatban (pl. az internet segítségével), illetve a szervezetek hálózatához nem egyszer külső szereplők (pl. szállítók, partnerek, ügyfelek) is hozzáférnek. Ennek következtében jogosulatlan személyek is hozzáférhetnek az e-mailben, kereskedelmi tranzakciókban és a szimpla fájlokban rögzített információkhoz. Mivel az informatika fejlődése és ezzel együtt az állandóan bővülő alkalmazása továbbra is robbanásszerű, a számítógépekre, tárolóeszközökre rengeteg adat és információ kerül, amelyek jelentős része érzékeny és fontos.

Ismerve az emberi természetet, azaz például a kényelem és a biztonság együttes teljesülésének esélyeit, figyelembe véve a fenyegetések fajtáinak fejlődését, valamint a számítógépek közötti kapcsolatok bővülését, a biztonsági visszaélések száma sohasem fog nullára csökkenni. Nagymértékben tompítani tudjuk azonban az illetéktelen felhasználás és számítógépes bűnözők kártékony hatását, ha megfelelő szakértelemmel rendelkezünk, alkalmazzuk a biztonsági alapelveket, és használjuk az elérhető, integrált biztonsági megoldásokat.

Ezek alapján tehát leszögezhetjük: bármilyen számítógépes munkakörnyezetben az egyik legfontosabb alapelv az adatok biztonságos tárolása, az erőforrások felügyelt publikálása valamint az ezekhez történő hozzáférés korlátozása,

illetve felügyelete. Az informatikai infrastruktúra biztonságossá tétele két alapvető célt kell, hogy kitűzzön maga elé: amennyire csak lehet, csökkenteni a külső és belső incidensek számát, valamint növelni az esetlegesen mégis előforduló hibák észlelési arányát. Ha ezt a két területet megfelelően ellenőrzésünk alatt tudjuk tartani, általában biztonságos környezetről beszélhetünk.

Mivel a teljes infrastruktúra is több szintből áll, a biztonsági megoldások is több rétegre bonthatók, így a fizikai biztonságtól (a helyiség őrzése) egészen az adatok képernyőn történő megjelenítéséig számos „kaput” építhetünk fel.



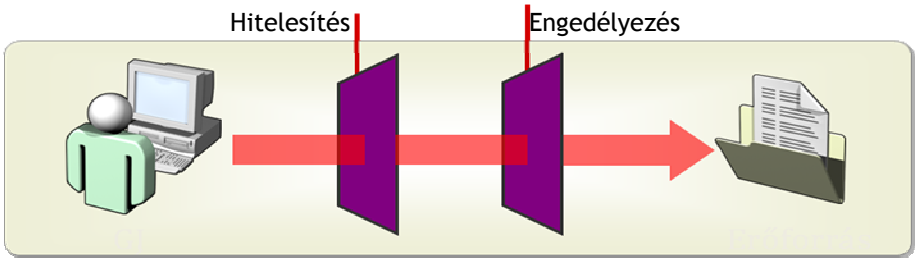
3.1. ábra: *Egy példa a biztonsági szintek általános kialakítására*

Szándékaink szerint ebben a fejezetben, (illetve a könyv más pontjain is) az első három szinttel foglalkozunk részletesen, azaz az adataink, az alkalmazásaink, illetve magának az operációs rendszernek a védelmére vonatkozó elveket és konkrét megoldásokat ismertetjük.

Az erőforrás-kezelés alapjai

A felhasználók (és a számítógépek) hozzáférését az adatokhoz és egyáltalán a rendszer egészéhez úgynevezett hitelesítési (autentikációs) folyamatokkal biztosítjuk. Akár szóló gépről van szó, akár hálózatról, minden felhasználónak célszerűen olyan egyedi azonosítója van, melynek segítségével egyértelműen azonosíthatóvá is válik. A **hitelesítést** – mely során megbizonyosodunk majd a bejelentkező fél identitásáról – az autorizáció, vagyis az **engedélyek megadása** követheti, amely alapja egy előzetes és eltárolt engedély meghatározása.

Általánosan elmondható, hogy a célunk mindig az elégséges, de mégis a lehető legkevesebb jogosultság kiosztása. Ennek az elvnek a betartása a napi gyakorlatban képes igazán kamatozni, hiszen, ha a felhasználók a feladataik elvégzéséhez szükséges összes jogosultsággal rendelkeznek, akkor az informatikai rendszer nem gátolja, hanem elősegíti a magas szintű munkavégzést. Ráadásul ha „csak" a minimálisan elégséges jogosultsággal rendelkeznek, akkor üzemeltetőként vagy a szervezet szempontjából nézve kevésbé kell számolnunk a vétlen vagy szándékos biztonsági problémákkal.



3.2. ábra: *A hitelesítési és engedélyezési folyamat általában egymást követi*

A hitelesítés

A hitelesítés folyamata feltételezi a hitelesítő jelenlétét is, amely a számítógépes környezettől függően többféle lehet, mi most három alappéldát emelnénk ki:

1. **Hitelesítés helyben, azaz interaktív belépéssel az adott számítógépen.** Ekkor a felhasználónak rendelkeznie kell az adott gépen érvényes belépési lehetőséggel, azaz, a gép saját felhasználói adatbázisában valamilyen módon szerepelnie kell a fiókjának. Ekkor tehát az adott gép a hitelesítő, és csak felhasználói fiókokat tud hitelesíteni.
2. **Hálózati hitelesítés**. Elsősorban munkacsoportos környezetben használatos, amikor egy másik a hálózaton jelen levő számítógépre jelentkezünk be (ezt mindig megelőzi a helyi gépre történő belépés). Ennek oka lehet egy megosztott mappa, vagy egy nyomtató elérése. Sok esetben a másik gépre nem ugyanazzal a felhasználónévvel és jelszóval lépünk be, mint helyben, hiszen ilyenkor a másik gép felhasználói adatbázisa a domináns, tehát eltérőek lehetnek a hitelesítő adatok. Ekkor tehát a másik gépet tekinthetjük a hitelesítőnek, amely szintén csak felhasználói fiókokat tud hitelesíteni.

3. **Tartományi hitelesítés**. A legkomplexebb megoldás, amely egyben a legtöbbet is nyújtja. Mivel létezik a tartomány, dolgozik a címtárszolgáltatás, a felhasználók fiókjainak és hitelesítő adatainak tárolása a címtár adatbázisban történik, az engedélyekkel és más információkkal együtt. Alapesetben akármelyik tartományi tagsággal rendelkező számítógépen bejelentkezhetünk a tartományba is (ez is az ajánlott, sőt, sok esetben a helyi belépés ilyenkor nem is lehetséges, nincs is szükség rá), hiszen a tartományvezérlőket ezekről elérjük, amelyek a rajtuk található címtár adatbázis segítségével, központilag képesek hitelesíteni bennünket. De nemcsak az interaktív belépés létezik, tartományban lehetőség van a számítógépfiókok létrehozására és tárolására, a tartománytag gépek rendelkeznek jelszóval is, így ezek is „belépnek", azaz képesek hitelesíteni is magukat. Tartomány esetén tehát a felhasználók és a gépek esetén is a címtárszolgáltatás, illetve ennek konkrét képviselője, a tartományvezérlő a hitelesítő elem.

Akár egy helyi gépről, akár egy hálózatról van szó, a hitelesítés folyamata során a felhasználó jelszavának biztonságos tárolása minden esetben alapvetően szükséges (erre később még visszatérünk). Az utóbbi esetben viszont számolnunk kell még azzal is, hogy adott hálózati forgalomban a legtöbb esetben a hitelesítő adatok szállítás közben védtelenek, azaz megfelelő szoftveres, vagy hardvereszközzel mások számára is hozzáférhetőek, ezért mindenképpen úgy kell „kinézniük", hogy egyáltalán ne jusson előbbre velük az, aki ellopja az adott forgalom részleteit. De e feltételek teljesülése előtt még egy fontos lépcsőfok van: rendelkeznünk kell a hitelesítő adatokkal.

A hitelesítés főszereplői

A rejtélyes cím mögött némiképp puritán tartalom áll, azaz ebben a fejezetben a Windows Vista felhasználói fiókjairól és csoportjairól lesz szó.

Ha nem tartományról beszélünk, hanem önálló vagy munkacsoportos környezetről, akkor a felhasználói fiók *(user account)* az adott gép – kizárólag csak helyben használható – felhasználóját személyesíti meg. A fiók objektum tárolja a felhasználó alapadatait (nevét, csoporttagságát, ikonját stb.), és a legfőbb feladat az, hogy a rendszer erőforrásaihoz hozzáférési jogosultságokat definiáljunk számára, illetve hogy a felhasználók tevékenysége (pl. belépés, fájlhozzáférés stb.) nevesítve jelenjen meg a naplófájlokban. Emellett természetesen az eltérő munkakörnyezet, illetve az egyedi beállítások elérése is célunk lehet, a különböző felhasználói fiókok létrehozása apropóján.

A helyi számítógép viszonylatában a fiókok, a jelszavaikkal, a csoportokkal és az egyéb, pl. biztonsági jellemzőkkel együtt egy speciális, ún. helyi biztonsági adatbázisban tárolódnak *(Security Account Manager)* és amely gyakorlatilag a rendszerleíró adatbázis egyik ágában található meg, de ami egyúttal a *Windows\System32\Config\SAM* fájl tartalma is.

Még mielőtt nekiesnénk a *regedit.exe*-nek, illetve az említett fájlnak, tudnunk kell, hogy kicsit nehezen vizsgálhatjuk meg ezeket még teljes körű rendszergazda jogosultsággal is, hiszen a registry ezen ágához *(HKLM\SAM)* csak a *SYSTEM* felhasználónak van jogosultsága, akinek viszont nincs interaktív belépési lehetősége a gépen. A *SAM* fájl pedig az operációs rendszer működése alatt – számunkra – nem nyitható meg.

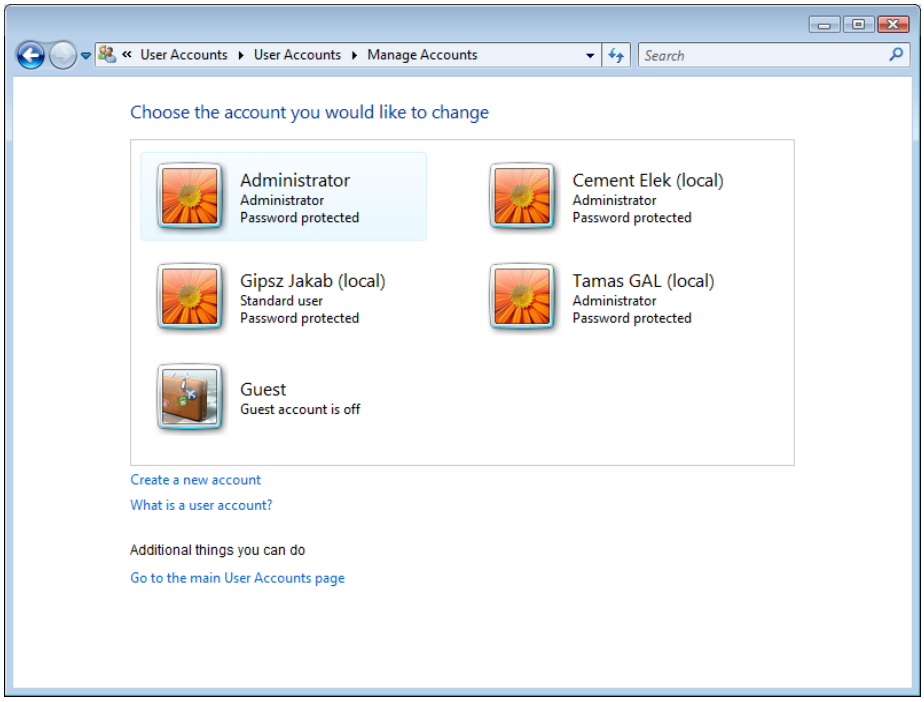
A felhasználói fiókokat mindig felhasználónévvel és, (nem kötelezően, de mégis ajánlottan), jelszóval különböztetjük meg egymástól, de további tulajdonságai is lehetnek – igaz egy helyi fiók esetén viszonylag kevés opcióval rendelkezünk ezen a területen (lásd ugyanebben az alfejezetben, később). Fontos jellemzője viszont az adott fióknak a típusa, amelyből a Windows Vistában két fő, és egy, csak nagyon extrém esetben használtat ismerünk:

1. **Administrator *(Rendszergazda)* fióktípus**: Az Administrators *(Rendszergazdák)* csoport tagjai, magas jogosultsággal használhatják a gépet. Alapértelmezés szerint a telepítés során megadott fiók is ebbe a csoportba kerül, és csak e csoport tagjaként hozhatunk létre, változtathatunk és törölhetünk további felhasználói fiókokat. A teljesség igénye nélkül, nézzük meg, hogy melyek a legfontosabb további műveletek, amelyre csak egy admin fiók birtokában leszünk képesek:
    - bármely felhasználó jelszavának megváltoztatása;
    - alkalmazásokat telepíteni és eltávolítani;
    - a hardver eszközök eszközmeghajtóit telepíteni vagy eltávolítani;
    - mappákat megosztani;
    - engedélyeket és jogosultságokat beállítani más felhasználóknak (vagy önmaguknak);
    - a kötetek összes állományát elérni, más felhasználók fájljait is beleértve;
    - fájlok és mappák tulajdonjogát átvenni;
    - a *Program Files* és a *Windows* mappákba írni;
    - lementett rendszerfájlokat visszaállítani;

- a rendszeridőt és a naptárt beállítani;
- a Windows Tűzfalat konfigurálni;
- beállítani a biztonsági frissítéseket, illetve manuálisan biztonsági frissítéseket telepíteni.

2. **Standard *(Általános jogú)* fióktípus**: A Users *(Felhasználók)* csoport tagjai a korábbi operációs rendszereknél csak egy alapszintű jogosultságcsokorral voltak kénytelenek beérni. A Windows Vista esetében jelentős haladás történt: itt már egy standard felhasználó gyakorlatilag mindenre képes, ami a számítógép napi használatához szükséges – de ha mélyebb, a rendszer biztonságát, működését alapjaiban megváltoztató műveletet szeretnénk elvégezni, akkor rendszergazda segítségére (vagy jogosultságra) lesz szükségünk (részletesebben ezzel a kérdéskörrel a felhasználói fiókok felügyelete *(User Account Control, UAC)* alfejezetben lesz szó). Lássunk néhány konkrét lehetőséget – főképp a viszonyítás kedvéért – amelyekre a Vistán egy standard felhasználó képes:
   - saját jelszó megváltoztatása;
   - a telepített programok használata;
   - hardvereszközök eszközmeghajtóinak telepítése, (ha külön kapunk rá engedélyt);
   - a jogosultságok megtekintése;
   - fájlok létrehozása, változtatása és törlése a saját Dokumentumok mappában, illetve a saját, megosztott mappákban;
   - a személyesen lementett fájlok visszaállítása;
   - a rendszeridő és naptár megtekintése, az időzóna megváltoztatása;
   - az energiaellátási opciók beállítása;
   - belépés csökkentett módban.
3. **Guest *(Vendég)* fióktípus**: A Guests *(Vendégek)* csoportba tartozó fiókok megszemélyesítői nagyon minimális jogosultságokkal rendelkeznek, mélyen a standard felhasználók jogosultsági szintje alatt. Ideiglenes jelleggel és/vagy nagyon korlátozott hozzáférés céljából használjuk. Jó példa erre, hogy az azonos nevű Guest *(Vendég)* fiók tulajdonosa még a saját jelszavát sem hozhatja létre, a Users *(Felhasználók)* csoportnak sem tagja, és alapesetben ez a fiók le is van tiltva.

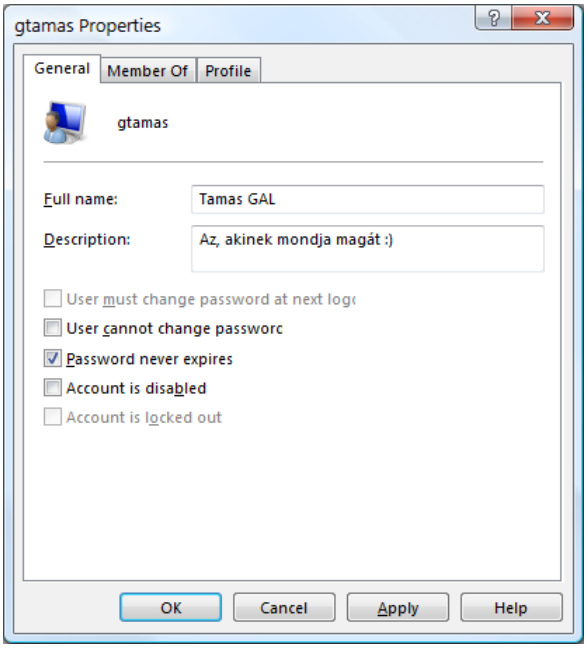
A felhasználói fiókok kezelése többféle helyen is történhet a Vistában. Az általános opciókat a Control Panel *(Vezérlőpult)* / User Accounts *(Felhasználói fiókok)* alatt találjuk. Önálló vagy munkacsoportos környezetben itt hozhatunk létre új fiókokat, törölhetjük, átnevezhetjük ezeket, megváltoztathatjuk a típusukat és a jelszavakat, vagy akár – megfelelő jogosultsággal – más helyi felhasználók beállításait is korrigálhatjuk. Kapunk lehetőséget a profilunk, a hálózati jelszavaink (lásd egy későbbi alfejezetben) vagy a fájlok titkosításához szükséges tanúsítványok kezelésére is. Ha viszont a gépünk nem önálló, hanem tagja egy tartománynak, akkor itt jóval kevesebb lehetőséget találunk a helyi felhasználói fiókok kezelésére.



3.3. ábra: *Munkacsoportos környezetben így (is) láthatjuk a fiókokat*

A haladó és egyben a klasszikus beállításokat innen – munkacsoportos környezetben – nem érjük el, ellenben a megfelelő MMC-konzol segítségével már igen, méghozzá az első fejezetben már ismertetett Computer Management MMC részeként (Local Users and Groups – *Helyi felhasználók és csoportok).* Ezen a felületen már több lehetőségünk is lesz, például a Users *(Felhasználók)* szakaszon belül, az alapértelmezés szerint egyformán letiltott Administrator *(Rendszergazda)* es Guest *(Vendég)* fiókok mellett meg fogjuk találni a telepítéskor általunk létrehozott fiókunkat is. E fiók tulajdonságlapja körülbelül ugyanúgy néz ki, mint a következő képen.

A Vista különböző változatai alig térnek el a felhasználói fiókok és a csoportok kezelését illetően, különbség maximum az esetleges tartományi tagság miatt a felszínen, azaz a grafikus felületen adódhat. Mivel csak a Business, az Enterprise, illetve az Ultimate változatot léptethetjük be tartományba, ezért a szövegben említett különbség is csak ezeknél a változatoknál fellelhető. Jó tudni viszont, hogy a Vista Home Basic, illetve a Home Premium változata alatt a Local Users and Groups MMC konzol nem elérhető.



3.4. ábra: *Egy felhasználói fiók tulajdonságai*

Itt a név és a leírás mellett a fiók jelszavára vonatkozó beállításokat is láthatunk, ezek a következőek:

- User must change password at next logon *(A következő bejelentkezéskor meg kell változtatni a jelszót)* – A soron következő (vagy akár a legelső) belépéskor a felhasználónak meg kell változtatnia a jelszavát. Ennek értelme akkor van, ha rendszergazdaként nem akarunk jelszót meghatározni a felhasználónak, vagy akkor, ha kifejezetten kényszeríteni szeretnénk arra, hogy megváltoztassa.
- User cannot change password *(A jelszót nem lehet megváltoztatni)* – Ha nem akarjuk, a felhasználó nem változtathatja meg a saját jelszavát. Ritkán, esetleg a közösen használt fiókok esetén van értelme ennek a beállításnak.

- Password neves expires *(A jelszó sohasem jár le)* – A Vista alapbeállítás szerint 42 naponként automatikusan kéri a felhasználótól a jelszó megváltoztatását. Ha itt kikapcsoljuk, akkor mentesülhetünk ettől.

A maradék két lehetőség közül az első a fiók letiltására *(Account disabled)* vonatkozik, ami gyakorlatilag teljesen felfüggeszti, de nem távolítja el a rendszerből az adott fiókot. A második pedig a fiók (többnyire ideiglenes, pl. több helytelen jelszó megadás miatt automatikus) kizárására vagy a már megtörtént kizárás feloldására vonatkozik.

E panel két további füle is fontos tulajdonságokat hordoz:

- A **Member Of** segítségével állíthatjuk be az adott fiók csoporttagságát (ha van hozzá jogosultságunk).
- A **Profile** fülön a felhasználó komplett profiljának lelőhelye szerepel (ha eltér az alapértelmezett, többnyire a *\Users\felhasználó_neve* mappától), illetve a logon szkriptjének (belépési parancsfájl) neve, amely a felhasználó belépésekor lefutó általában kötegelt (pl. *.bat)* állomány megnevezése.
- **Home folder** *(Kezdőmappa):* a felhasználó alapkönyvtárának helye, ez általában a parancssori ablak *(cmd.exe)* kezdőkönyvtára is.

Önálló gép vagy munkacsoport esetén az utóbbi opciókat (a jelszóra vonatkozóakat is beleértve) tipikusan egyáltalán nem használjuk, ezek elsősorban tartományi környezetben alkalmazott beállítások. Igaz, ebben az esetben viszont nem a helyi gépeken, hanem központosítva, a címtárban tárolt felhasználói fiók beállításainak szabályozzuk ezeket a lehetőségeket.

Ennek az alfejezetnek a másik fő témája a már kényszerűségből többször is említett felhasználói csoportok. Az előző rész alapján már tisztában vagyunk azzal, hogy egy helyi gép esetén milyen fő típusok állnak rendelkezésre ezekből (Administrators, Users, Guests), illetve azt is láthattuk, hogy egy-egy felhasználó esetén hol állíthatjuk a csoporttagságot. Tekintsük át most a csoportokkal kapcsolatos további részleteket!

Az összes operációs rendszerben – így a Windows Vistában is – a csoportok létrehozásának célja elsősorban a felhasználók fiókjainak összegyűjtése, közös kezelése. Ha létrehozunk egy csoportot és hozzárendelünk felhasználókat, akkor pl. a jogosultságokat, vagy az engedélyeket egy lépésben, minimális energiával képesek leszünk beállítani az adott felhasználói kör számára. Ezen kívül az objektumokhoz csatolt jogosultsági listák is kisebb méretűek lesznek, tehát gyorsabban dolgozza fel, értékeli ki ezeket az operációs rendszer.

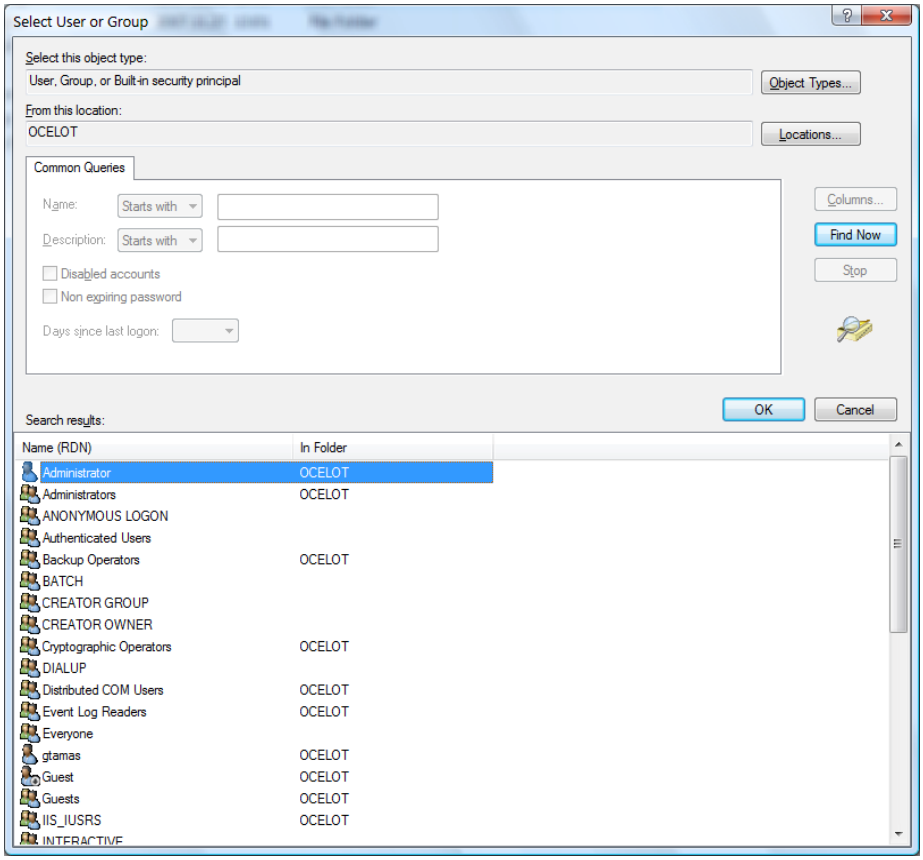
A Windows operációs rendszerek tartalmaznak egy sereg beépített, a telepítés után már elérhető csoportot, ezek fajtáit a következő felsorolásban mutatjuk be (a Vista-specifikus csoportokról, illetve az elsősorban biztonsági okokból történt felhasználói és csoportváltozásokról egy későbbi alfejezetben nyújtunk majd egy részletes áttekintést).

- **Administrators** *(Rendszergazdák):* A rendszergazdák csoportja, elvileg majdnem az összes művelet és feladatkör birtokosa az operációs rendszerben.
- **Backup Operators** *(Biztonságimásolat-felelősök):* E csoport tagjai biztonsági mentéseket és visszaállításokat végezhetnek el, azaz ebből a célból a kötetetek összes objektumához hozzáférnek.
- **Guests** *(Vendégek):* minimális jogkörrel rendelkező, speciális csoport, egyetlen tagja alapértelmezés szerint a már említett Guest fiók.
- **Network Configuration Operators** *(Hálózat-beállítási felelősök):* A hálózati szolgáltatások közül bizonyos – egyébként rendszergazdai – műveletek (TCP/IP -konfigurálás, hálózati kapcsolatok engedélyezése, DNS-cache ürítése, RAS-kapcsolatok legyártása, törlése stb.) ellátására is képesek lesznek e csoport tagjai.
- **Remote Desktop Users** *(Asztal távoli felhasználói):* Az első fejezetben említett Remote Desktop *(Távoli asztal)* szolgáltatás felhasználói, akik jogosultak elérni az adott gépet a Remote Desktop ügyfélprogrammal.
- **Replicator** *(Replikáló):* Fájlok, mappák tartományon belüli replikációját teszi lehetővé a csoport tagjai számára.
- **Users** *(Felhasználók):* A már többször említett csoport tagjai az átlagos, standard típusú felhasználói fiókok. Minden új fiók alapértelmezett tartózkodási helye is ez a csoport.

Ha alaposan megvizsgáljuk az operációs rendszert példaképpen az adható jogosultságok és engedélyek kapcsán, akkor további, sok esetben nagyon ritkán használt, speciális csoportokra is rábukkanhatunk.

Ezek a csoportok nem láthatóak a Local Users and Groups *(Helyi felhasználók és csoportok)* MMC-ben, és a tagsági viszonyaikat sem állíthatjuk be a felhasználói felületről (az operációs rendszer végzi ezt el helyettünk), viszont szükség esetén adhatunk ki számukra fájlokra és mappákra jogosultságokat, illetve kaphatnak egyéb engedélyeket is. Ezeket a jogosultság- vagy engedélyhozzárendeléseket viszont általában nem nekünk kell manuálisan megtennünk, a gyári alapbeállítások tartalmazzák e csoportok hozzárendelését a szükséges erőforrásokhoz, objektumokhoz, illetve folyamatokhoz. Tekintsük meg e csoportok listáját is, egy-egy rövid jellemzéssel kísérve a felsorolást:

- **Everyone** *(Mindenki):* Ennek a csoportnak az összes felhasználói fiók és egyéb, speciális felhasználó tagja (az Anonymous Logon csoport tagjai kivételével). Tisztában kell lennünk azzal a ténnyel, hogy ha ennek a csoportnak adunk pl. egy mappán jogosultságot, akkor az az összes helyi, vagy távoli hozzáférés esetén érvényes lesz. Épp ezért e csoport használata (még ha igen kényelmes is), nem ajánlott. Még akkor sem, ha a Windows XP-ben e csoport számára általánosan megkapott Read *(Olvasás)* jogosultság a Vistában már nem biztosított.



3.5. ábra: *A speciális, csak a jogosultság kiosztáskor használatos csoportok*

- **Authenticated Users** *(Hitelesített felhasználók):* az Everyone, illetve a Users csoportokhoz képest egy zártabb csoport, amely egyrészt az Everyone-nal szemben nem tartalmazza a Guest *(Vendég)* felhasználót, az Usersszel szemben pedig csak a valóban hitelesített felhasználókat tartalmazza. Minden felhasználó tagja lehet, aki helyben jelentkezett be, a hálózatból vagy telefonos kapcsolaton keresztül használja a szá-

mítógépet. Íratlan szabály, hogy manuális jogosultságkiosztásnál, ha minden interaktív felhasználónak akarunk jogot adni, egy erőforráshoz, akkor azt mindig ezen a csoporton keresztül tesszük meg.

- **Anonymous Logon** *(Névtelen bejelentkezés):* E csoport tagjai szerény lehetőségekkel vannak felvértezve, mivel olyan „felhasználókról" van szó, akik nem azonosították magukat névvel és jelszóval. Ilyen „felhasználó" viszonylag kevés van, ide tartozik pl. az ún. *null session*ön keresztüli elérés (pl. a gépek kommunikációja esetén az IPC$ megosztás használata, lásd később). Helyi alkalmazása alapértelmezés szerint viszont tiltott.
- **Batch** *(Köteg):* Azon felhasználók, akik a nélkül indíthatnak el parancsfájlokat, hogy interaktívan bejelentkeznének (pl. egy program futtatásának időzítése).
- **Creator Owner** *(Létrehozó tulajdonos),* Creator Group *(Létrehozó csoport):* Az erőforrások alapértelmezett jogosultsági listájában rendszeresen találkozhatunk e fiókkal, illetve csoporttal, amelyek az adott objektum tulajdonosát jelölik, azaz azt a felhasználót, aki létrehozta az erőforrást. A Creator Group használata a Windows operációs rendszerekben nem jellemző, elsősorban a POSIX kompatibilitás miatt szükségesek.
- **Dialup** *(Telefonos):* Azokat a felhasználókat jelöli meg az operációs rendszer ebbe a csoportba tartozó tagnak, akik aktuálisan a telefonos hálózaton keresztül csatlakoznak a számítógéphez.
- **Interactive** *(Interaktív):* Azon felhasználók a tagjai ennek a csoportnak, akik képesek manuálisan (a felhasználónév/jelszó párossal) belépni az operációs rendszerbe, beleértve a Remote Desktop *(Távoli asztal)* szolgáltatást használókat is.
- **Network** *(Hálózat):* A hálózaton keresztül kapcsolódó felhasználók, akik tipikusan a helyi gép egy megosztott erőforrásához kapcsolódnak.

A felhasználók és a csoportok kezelése a parancssorból is megoldható. A *net user* és a *net localgroup* parancsoknak számtalan, jól használható paramétere van.

A hitelesítés protokolljai

A hitelesítést többféle protokoll segítségével bonyolíthatjuk le, ezek különbsége elsősorban a hitelesítés során használt jelszavak tárolási módszerében, kisebb számú esetben a továbbításuk módszerében jelentkezik. Az eléggé elterjedt hiedelemmel ellentétben a Windows operációs rendszerek nem tárolják el a jelszavakat, pontosabban nem a jelszavakat tárolják el, hanem az ezekből

speciális tördelőalgoritmusokkal képzett kivonatokat, más néven hash-eket. Egy ilyen kivonat mindig teljesen egyedi, így használható a jelszó helyett, viszont magából a kivonatból semmilyen körülmények között nem lehetséges visszaállítani az adott jelszót.

Egy adott hash birtokában egyetlen módszerünk a jelszó kitalálására a próbálgatás és összehasonlítás, azaz sok-sok jelszó kivonatának elkészítése, majd az ezek összehasonlítása a feltörendő jelszó kivonatával. Ezt a szaknyelvben „brute force" módszernek hívjuk.

A jelszavak tárolási módszere tehát kulcsfontosságú a hitelesítés szempontjából. A régebbi hitelesítési megoldások mellőzésének oka pontosan az, ami általában a legfőbb kritérium is ezekkel a módszerekkel szemben: mennyi ideig képesek ellenállni a feltörés kísérletének. Mivel a feltöréshez szükséges szoftverek kódjában matematikai műveletek dominálnak, ahogy nő az ezekhez szükséges hardverelemek (CPU, RAM stb.) teljesítménye, úgy csökkenhet a törésre fordított idő. Mikor tekinthetünk egy módszert tényleg biztonságosnak? Erre kivételesen van általános érvényű szabály: ha a védett adatok megszerzéséhez szükséges idő (nagyságrendekkel) több, mint amennyi ideig biztonságban szeretnénk tudni az adott adatokat.

A következő lista elemei közül néhány már nincs, vagy alig van használatban, de esetleg a kompatibilitás miatt szükségesek lehetnek.

- **LAN Manager (LANMAN)** – Eléggé egyszerű jelszótárolással (LM hash) operáló hitelesítési módszer, a régebbi Windows 3.1x/95/98/Me, illetve MS-DOS operációs rendszerekben volt használatos. A jelszavak kivonatának elkészítése során olyan kényszerű hiányosságokkal rendelkezik, amelyek miatt ma már egyszerűen és gyorsan lehetséges a megfelelő teljesítményű hardverrel feltörni. A példa kedvéért nézzük meg, hogyan készül el egy LM hash:

    1. A jelszó nagybetűsítése (tehát teljesen mindegy, hogy felváltva használunk-e kis- és nagybetűket!)
    2. A jelszó kiegészítése szóközökkel, 14 bájt hosszúságra (tehát, ha egy 9-karakteres jelszavunk van, akkor gyakorlatilag egy 7 és egy 2 karakterből álló részt kell feltörni, mivel az utolsó 5 karakter tuti, hogy szóköz lesz!)
    3. A 14-bájtos jelszóból ($14 \times 8 = 112 = 2 \times 56$ bit) 2 db DES kulcs készül.

4. A két 56-bites DES kulccsal titkosítunk egy mindig állandó (!) sztringet *(KGS!@#$%)*.
5. Az eredmény 2 × 8 bájt, összesen tehát egy 16-bájtos hash.

Látható, hogy több furcsa anomália is jellemző erre tárolási módszerre, amelyek nagyban segítenek a brute force alkalmazásoknak, hogy pillanatok alatt elérjék a céljukat, ezért aztán a LANMAN hitelesítés ma már tényleg teljesen elavultnak számít és veszélyes a használata.

- **NTLMv1** (NT LAN Manager v1) – Kérdés-válasz *(Challenge/Response)* elven működő autentikációs protokoll. Az NTLM használatakor a hitelesítést kérő ügyfél egy véletlenszerűen generált 8-bájtos „kihívást" *(challenge)* kap a kiszolgálótól, melyet aztán a felhasználó jelszavával titkosít és visszaküld, némiképp feltupírozva, összesen 2 × 24 bájtban. Az NTLMv1 protokollt tipikusan a Windows NT 4 SP4 előtti rendszerekben alkalmazták, és ma már szintén nem nyújt elégséges védelmet, hiszen amellett, hogy egyrészt az MD4 (Message Digest 4) algoritmust használja az NT hash elkészítéséhez (ami anno elég erős titkosításnak számított), az iménti ismerős, az LM hash is ugyanúgy része lesz a válasznak, és így nem jutunk sokra vele.
- **NTLMv2** – Az első verzió kriptográfiailag megerősített változata, a Windows NT 4 SP4 javítócsomag óta használhatjuk, a későbbi rendszerek természetesen már alapértelmezésben tartalmazzák. Ha nem áll rendelkezésre a Kerberos protokoll (pl. webes hitelesítésnél vagy tartományon kívül, vagy ha IP-cím alapján kell hitelesíteni), akkor tökéletesen megfelelőnek tekinthető, hiszen „erősségét" tekintve gyakorlatilag az NTLMv2 számít az összes módszer közül a legjobbnak: 128-bites kulcsteret használ, külön-külön kulcsokkal az üzenet hitelesség és integritás biztosítására, és az MD4 helyett a HMAC-MD5 kivonatokkal operál.

Egyes hash-algoritmusok lehetővé teszik, hogy paraméterezzük őket, azaz a kimenetüket kicsit megváltoztathatjuk, amelyet sózásnak *(salted)* is hívnak. Ez a módszer lehetővé teszi, hogy a hash mindig egy kicsit másmilyen legyen, ezzel is nehezítve az ellopás lehetőségét. A korábban említett 8-bájtos kihívás pontosan erről szól, de ez csak a kezdet. Ma az egyik legjobb „sószóró" a HMAC algoritmus (Hash Message Authentication Code), melyet úgy terveztek, hogy a meglévő és bevált algoritmusokkal változtatás nélkül együttműködjön. Így jöhet létre a HMAC-MD5, amely nevéből kitalálható, hogy a HMAC egy komoly preparálást végez az adatokon, s ennek az eredményét juttatja el az eredeti MD5 algoritmushoz.

Mindkét NTLM-hitelesítési protokoll közös hátránya viszont a relatíve nagyobb hálózati forgalom generálása, amely például a kivonatok minden egyes alkalommal történő elküldésében nyilvánul meg, és ez egyben emiatt nagyobb sebezhetőséget is jelent.

- **Kerberos V5** – A Microsoft a Kerberost (pontosabban ennek V5-ös verzióját) választotta a címtárszolgáltatás alapértelmezett hitelesítési protokolljává a Windows 2000 Serverben, és ez azóta sem változott. A Kerberos főbb előnyei közé tartozik a platformfüggetlenség (mivel egy RFC-ben rögzített típusú hitelesítési módszerrel állunk szemben), a minimális hálózati plusz forgalom, valamint a biztonsági házirendből történő konfigurálhatóság.

- A Kerberos V5 nélkülözhetetlen szolgáltatása a kulcsszolgáltató központ *(Key Distribution Center – KDC),* mely Active Directory címtárszolgáltatás részeként minden tartományvezérlőn fut. A KDC felel a jegyek küldésekor használt titkosítókulcsok generálásáért és folyamatos üzemeltetéséért. A KDC az összes további a tartományvezérlőkön futó biztonsági szolgáltatással integrálva van, illetve az AD adatbázisát, (illetve a globális kalatógust is) használja saját adatbázisaként.

  A Kerberos V5 hitelesítési folyamata egyszerűsítve a következőképpen működik (természetesen az egész hitelesítési folyamat láthatatlan a felhasználó számára):

  1. Az ügyfélgépen belépni szándékozó felhasználó – jelszó és/vagy intelligens kártya használatával – hitelesíti magát a szintén a tartományvezérlőkön futó összetevő, a hitelesítésszolgáltató *(Authentication Service – AS)* felé.

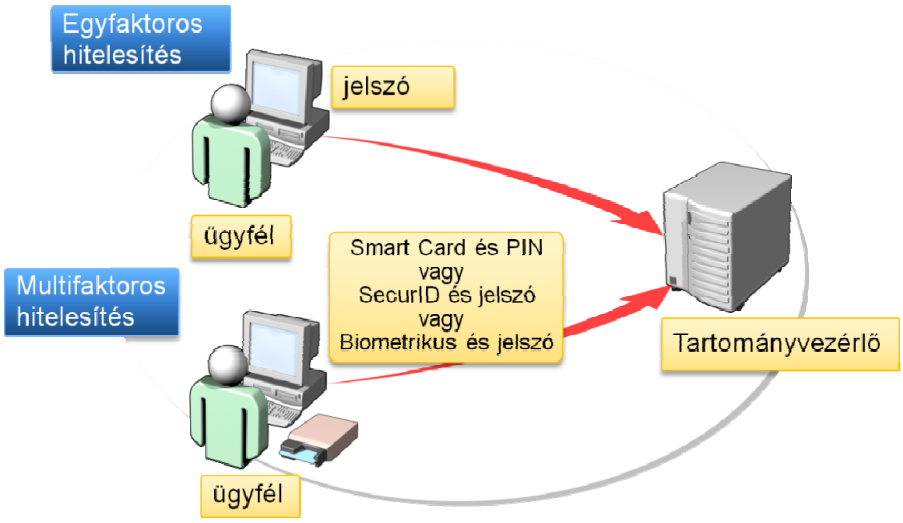
  2. Az AS leellenőrzi a felhasználót az AD segítségével, majd felveszi a kapcsolatot a KDC-vel az új kulcs legyártása érdekében.

  3. A KDC egy egyedi *(session)* kulcsot biztosít az ügyfélnek. Az AS ezt egy speciális jeggyel *(Ticket Granting Ticket – TGT)* együtt küldi el a felhasználónak. A TGT azért is fontos (az ügyfél el is tárolja), mert a további jegyeket is ezzel lehet majd kérni, immár anélkül, hogy a jelszóra/felhasználónévre szükség lenne. Ez a kedvezmény persze nem tart örökké, alapbeállítás szerint mindösszesen csak 10 óráig.

  4. Az ügyfél a nála lévő TGT felhasználásával jegyet kér és kap a harmadik fontos kiszolgálóoldali komponenstől, a Ticket Granting Service-től (TGS).

5. Végül az ügyfél ezt a jegyet mutatja be a kért hálózati szolgáltatásnak (azaz az NTLM-mel ellentétben nem utazik minden alkalommal a jelszó kivonat a hálózaton!), pl. jelen esetben a tartományi belépést kontrolláló tartományvezérlőnek, és kap engedélyt a tartományi belépésre. Ha ezek után az adott 10 órán belül valamilyen más szolgáltatás esetén újra igazolnia kell magát, akkor a letárolt TGT-vel megint kér egy szolgáltatásjegyet, és aztán csendben ezt bemutatja a kérő felé.

A Kerberos V5-szolgáltatás minden tartományvezérlőn, a Kerberos-ügyfél pedig minden munkaállomáson alapértelmezésként telepítve van, és aktív. Minden tartományvezérlő kulcsszolgáltatóként működik, az ügyfelek hitelesítéskor DNS-lekérdezéssel keresik meg a legközelebbi tartományvezérlőt. A bejelentkezés során ez a megtalált tartományvezérlő szolgál kulcsszolgáltatóként a felhasználó számára. Ha az elsődleges kulcsszolgáltató elérhetetlenné válik, a rendszer új kulcsszolgáltatót keres a hitelesítés végrehajtásához. Ha egyetlen kulcsszolgáltató sem elérhető, a belépés meghiúsul.



3.6. ábra: *A multifaktoros hitelesítés előnyei könnyen beláthatók*

A felhasználók hitelesítése egy- vagy többfaktoros módszerrel is történhet. Többfaktoros hitelesítésnek nevezzük azt az azonosítási metódust, ahol nem csak egy név/jelszó párossal, hanem egyéb rendelkezésre álló eszközökkel, például intelligens kártyával, vagy egyéb hitelesítő hardverkulccsal (pl. SecurID-eszközök), egyaránt azonosítjuk magunkat.

A multifaktoros hitelesítés lényegesen biztonságosabb belépést tesz lehetővé, hiszen a felhasználót nemcsak jelszava, vagy kódja azonosítja – mely esetleg kitalálható, vagy más egyszerű módon megszerezhető – hanem a fizikailag birtokolt eszköz is. Ilyenkor tehát nemcsak „tudunk valamit" (a jelszót), hanem a „van valamink" elv is érvényesül.

Az intelligens kártya (SmartCard) használata esetén a felhasználónak a kártya PIN-kódját kell csak ismernie, és a bejelentkezéskor szükséges a kártya is. A PIN-kód lehet egyszerű is (pl. 4 karakter), de ez nem gond, mivel nem megy át a hálózaton, hanem a Crypto API-n egyenesen áthaladva a kártyához tartozó Crypto Service Provider segítségével lejut az eszközbe. Ez az útvonal eléggé biztonságos, gyakorlatilag lehallgathatatlannak tekinthető.

Ráadásul a kártyák általában rendelkeznek „önmegsemmisítő" szolgáltatással, vagyis X darab sikertelen bejelentkezés után használhatatlanná válnak, illetve le is járhatnak, azaz Y idejű inaktivitás után szintén nem használhatóak.

A Windows világban a kiszolgáló és ügyfél oldali operációs rendszerek és alkalmazások (Active Directory címtár, ISA Server, Vista stb.) többféleképpen támogatják a multifaktoros hitelesítési típusokat is, van, amelyiket teljesen integráltan (pl. az intelligens kártyák), és van, amelyeket csak közvetítő, továbbító közegként, egy-egy külső, külön telepíthető alkalmazás felé (pl. RSA SecurID).

A jogosultságok

A jogosultságok definiálják a hozzáférés típusát egy erőforráshoz, vagy másképp fogalmazva, a sikeres hitelesítés után a jogosultságok alapján határozhatjuk meg, hogy például a felhasználó vagy a számítógép az adott objektumokkal milyen műveleteket végezhet. Tehát az engedélyezés (autorizáció) folyamatának az alapját jelentik. A jogosultságokat mindig az objektumokon érvényesítjük, melyek listáját az alábbi felsorolásban foglaltuk össze (a következő alfejezetekben pedig részletezzük is ezeket):

- NTFS-lemezeken tárolt fájlok és mappák;
- mappamegosztások a hálózat felhasználói számára (a helyi felhasználóknak is lehetséges, csak kevés értelme van);
- megosztott nyomtatók helyi és hálózati felhasználók számára.

Jogosultságokat a lista elemein kívül beállíthatunk más rendszerobjektumok esetén is, pl. a rendszerfolyamatok (processzek), rendszerszolgáltatások (szervizek), a registrykulcsok és -bejegyzések, vagy akár tartomány esetén a címtárszolgáltatás objektumain is.

Az azonosítás (pl. a rendszerbe való belépés) után a felhasználó egy testre szabott ún. *access token*t kap, ami tartalmazza jogosultságait, csoporttagságát stb. A különböző szolgáltatást nyújtó eszközök később ezt az access tokent ellenőrzik, majd ennek tartalma alapján döntik el, hogy a felhasználó hozzáférhet-e egy erőforráshoz (megosztott fájlhoz, számítógéphez stb.), vagy sem. Az egy-egy objektumhoz rendelt hozzáféréseket úgynevezett hozzáférési listákban *(Access Control List – ACL)* rögzítik. Az operációs rendszer az ACL-ek alapján engedélyezi vagy tagadja meg a hozzáférést az objektumokhoz, az ACL-ek pedig úgynevezett Security Identifierek (SID) segítségével azonosítják a felhasználót vagy a számítógépet. Az egyedi SID-eket a hitelesítő információkat tároló kiszolgáló generálja, azaz például a helyi gép, vagy éppen a tartományvezérlő.

A Security Identifierek felépítése a következőképp alakul: (például: *S-1-5-12-7623811015-3361044348-030300820-1013*, részeit egy táblázatban foglaljuk össze).

S	A karakterlánc biztonsági azonosító voltát jelöli
1	Felülvizsgálati szint, az értéke állandó
5	Az azonosító hozzáférési értéke
12-7623811015-3361044348-030300820	A tartományi vagy helyi számítógép-azonosító
1013	A relatív ID (RID), minden nem beépített (tehát létrehozott) felhasználó vagy csoport RID-je 1000-nél nagyobb lesz.

Ahogyan már említettük, a Windowsban több előre definiált felhasználói-, szolgáltatásfiók, illetve felhasználói csoport is létezik, ezek SID-jei minden esetben állandóak, így a gyakorlottabb rendszergazdák akár a név láthatósága nélkül is azonosíthatják ezeket (például eseménynaplókban, hibakereső szoftverekben). A legfontosabb „közismert" (más néven: *well-known)* SID-ek a következők:

S-1-5-18	LocalSystem szolgáltatásfiók
S-1-5-19	LocalService szolgáltatásfiók
S-1-5-20	NetworkService szolgáltatásfiók

S-1-5-21- <tartomány hash-e> -500	Administrator (Rendszergazda) felhasználó
S-1-5-21- <tartomány hash-e> -501	Guest (Vendég) felhasználó
S-1-5-21- <tartomány hash-e> -512	Domain Admins (Tartománygazdák) csoport
S-1-5-21- <tartomány hash-e> -514	Domain Guests (Tartományi vendégek) csoport

A beépített *(built-in)* felhasználók és csoportok SID-jének teljes listáját a Microsoft KB243330 számú tudásbáziscikke sorolja fel. (http://support.microsoft.com/kb/243330)

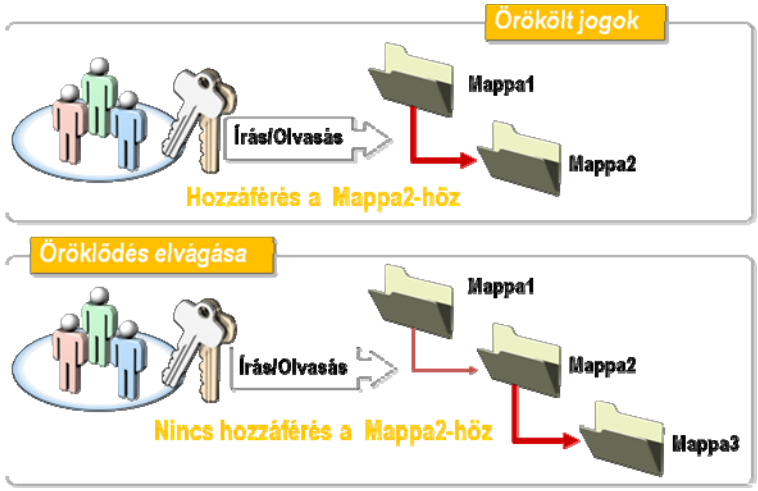
A SID-ek lekérdezésére használhatjuk az integrált *whoami* parancsot, többféle paraméterrel is, pl. a *whoami/user* az aktuális felhasználó SID-jét mutatja meg. Az objektumok ACL-jeit és minden egyéb jogosultsággal kapcsolatos információját az ún. Security Descriptor tárolja. Egy objektum Security Descriptorja a következő elemeket foglalja magába:

- tulajdonos SID-je;
- csoport SID-je (az objektum elsődleges csoporttagságát adja meg, a Windows általában nem használja);
- hozzáférési listák:
    - DACL (Discretionary Access Control List): a felhasználók és csoportok konkrét jogosultsági szintjeit határozza meg, azaz, hogy ki, mit tehet meg pl. az adott fájllal.
    - SACL (System Access Control List): a hozzáférések naplózási módját határozza meg, azaz, hogy kinek milyen sikeres vagy éppen sikertelen, az objektumon végzett műveletét kell naplózni.
- bejegyzések *(Access Control Entry, ACE):* egy-egy konkrét jogosultsági bejegyzés az adott hozzáférési listában (például: *Everyone – Read).*

A fájlrendszer-jogosultságok

A Windows operációs rendszerek tipikus fájlrendszere, az NTFS esetén a jogosultságokat több különböző szempont szerint csoportosíthatjuk, ezek egyike a művelet típusa, melyekre a következő példák hozhatóak fel:

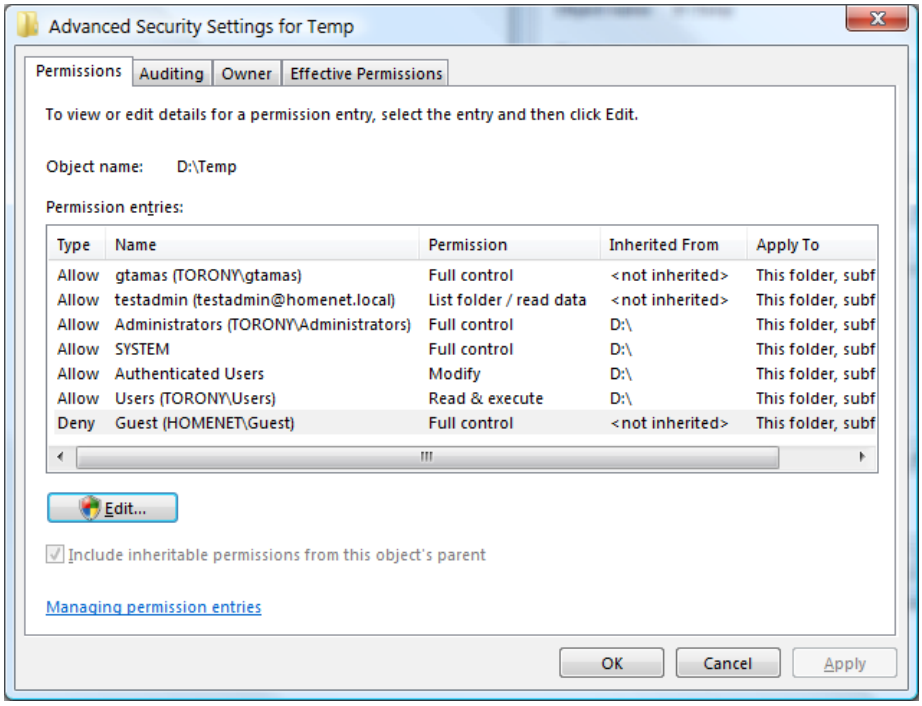
- **Engedélyezett**: az adott felhasználó/gép számára az objektumhoz az adott művelet engedélyezett.
- **Megtagadott**: A tiltás mindig magasabb rendű, mint az engedélyezés, ezért, ha mindkét opció be van jelölve, a tiltás érvényesül.
- **Nincs megadva**: a jogosultság alapértelmezésként nincs definiálva, hatása egyenértékű a tiltással.
- **Öröklött:** az objektum a szülőobjektum (egy vagy több szinttel feljebb lévő gyűjtőobjektum) jogosultságaival rendelkezik. Az öröklött jogosultsági beállításokat általában kiszürkített vagy teli jelölődobozok mutatják. Az öröklődési ágat megszakíthatjuk, azaz egy alsóbb objektumnál egyéni hozzáférést konfigurálhatunk, ekkor az alsóbb objektumnál exkluzív módon adhatunk hozzá, vagy vehetünk el jogosultságot.



3.7. ábra: *Az alapértelmezett jogosultság öröklődés megszüntethető*

A fájlrendszer-jogosultságokat elsősorban a grafikus felhasználói felületről kezeljük – amennyiben megvan a kellő hozzáférésünk az objektumhoz. A változtatáshoz egyszerűen kattintsunk jobb gombbal az elemre, majd válasszuk a Properties *(Tulajdonságok)* parancsot és váltsunk a Security *(Biztonság)* fülre. Itt az egyes hozzárendelt felhasználókat és azok alapvető érvényes jo-

gosultságait tekinthetjük és változtathatjuk meg, de áttekinthetőbb és kezelhetőbb listát kapunk az összes biztonsági beállítással együtt, ha az Advanced *(Speciális)* gombra kattintunk. Nézzünk egy konkrét példát, azaz egy mappa jogosultsági listáját



3.8. ábra: *Példa a jogosultsági listákra*

1. A *TORONY\gtamas* felhasználónak teljes jogosultsága *(Full control)* van a mappán, és nem örökölte *(not inherited)* hanem manuálisan kapta. Ez a mappa egy tartományba léptetett gépen található, ennek ellenére a helyi gép *(TORONY)* egy csoportjának vagy felhasználójának is adhatunk jogosultságot

2. A *testadmin* felhasználó tartományi felhasználó, de ettől függetlenül ő is kaphat jogokat a helyi gépen, de neki csak olvasási joga van, írás nincs, valamint az is látható, hogy az ő jogosultsága sem öröklődő.

3. *TORONY\Administrators* csoportnak szintén teljes jogosultsága van az adott mappán. Az érdekes ebben az, hogy ebbe a csoportba beletartozik a *testadmin* felhasználó is, ergo az előző sor teljesen felesleges. Emellett az is látszik, hogy ez a csoport a *D:* meghajtó gyökerétől kapja öröklés útján ezt a jogosultságot, automatikusan.

4. A *SYSTEM* nevű fiók magát az operációs rendszert, pontosabban a rendszerszolgáltatásokat testesíti meg, ennek megfelelően minden jogosultsága megvan, ami csak létezik *(Full Control)*.
5. Az Authenticated Users *(Hitelesített felhasználók)*: Ez a csoport az adott mappán módosítási joggal rendelkezik, tehát egy fokkal magasabbal, mint a szimpla Users csoport.
6. A *TORONY\Users* csoport tagjainak olvasási joga van. Nem látszik a képen, de ebbe a csoportba beletartozik a *gtamas* es a *gjakab* nevű felhasználó is. Mégis különbözőek lesznek a jogaik, mert a második sorban külön, engedékenyebb szabályzást kapott a *gtamas*, míg a *gjakab* nem, tehát rá a csoportnak adott egyszerű olvasási jog vonatkozik csak.
7. A *HOMENET\Guest* csoport tagjainak nem öröklődő, viszont mindent tiltó jogosultsága van. Ez akkor is így lenne, ha egy másik sorban kapott volna bármilyen engedélyt is ez a csoport, hiszen a tiltás „mindent visz".

Egy fontos dolgot – amelyről már volt szó korábban – immár konkrétan is megfigyelhetünk: a jogosultságokat általában a csoportoknak osztjuk, jelen példában csak a jobb magyarázhatóság kedvéért vettem fel a listába a *testadmin* és a *gtamas* felhasználókat, egyébként alapértelmezés szerint is csak csupa csoportot láthatnánk. Ennek az elvnek alapos oka van, ti. lényegesen könnyebb utólag bevenni egy felhasználót egy csoportba, mint 10, 20 stb. helyen egyesével berakni a szükséges jogosultsági listákba.

Egy másik megfontolandó, és szintén íratlan szabály az, hogy az átláthatóság és az egyszerűbb kezelés miatt nem fájloknak, hanem a fájlokat tároló mappáknak osztunk engedélyeket. Az öröklődést viszont a legritkább esetben kapcsoljuk ki, inkább tervezzük meg alaposan a hatását. Szintén csak indokolt esetben használatos az explicit tiltó (Deny) jogosultság, általában bőven elegendő, ha az adott csoport/felhasználó implicit tiltást kap, azaz nem szerepel a jogosultsági listában.

Ha viszont nem ragadunk le a Permissions *(Engedélyek)* első jogosultsági ablakánál, akkor több érdekes és fontos lehetőségre is rábukkanhatunk ezen az ablakon belül, nézzük meg ezek részleteit is:

- **Permissions fül / Edit...** *(Szerkesztés)* – A jogosultságok részletes beállítására, valamint például az öröklődés megváltoztatására is lehetőségünk nyílik. Két opciónk van itt:
    - **Include inheritable permissions from this object's parent** *(Szülőobjektum örökölhető engedélyeinek hozzávétele)* – A jelenlegi, örökölt jogosultságok teljesen eltávolíthatóak, vagy lemásolhatóak és szerkeszthetőek szabadon.

- **Replace all existing inheritable permission on all descendants with inheritable permissions from this object** *(A meglévő örökölhető engedélyek lecserélése az ezen objektumtól örökölhető engedélyekre az összes gyerekobjektumon)* – azaz az adott szinten lévő jogosultságok „lefelé" (almappákba és fájlokra) történő erőszakos kikényszerítése.

- Ha erről a pontról visszalépünk egyet, akkor elnavigálhatunk az Auditing *(Naplózás)* fülre is, ahol az adott mappa vagy fájl hozzáférésének naplózását állíthatjuk be. Néhány tudnivaló ehhez a lehetőséghez:
  - Alapértelmezésben csak a rendszergazda-csoport tagjaként tehetjük meg az auditálás beállítását.
  - A lista kialakítása ugyanúgy működik, mint a jogosultságoknál.
  - Az öröklődés elvágása és kikényszerítése is ugyanazt a módszert követi.
  - Az eredményt az eseménynaplóban találjuk, konkrétan a Security *(Biztonság)* naplóban.
  - A fájlrendszer hozzáféréseinek naplózásához nem elég itt beállítani a paramétereket, globálisan is engedélyezni kell ezt a lehetőséget. Ezt a helyi vagy a csoportházirendben tehetjük meg, a Audit Policy *(Naplórend)* opciók között az Audit object access *(Objektum-hozzáférés naplózása)* beállításával.
- Lépjünk tovább, és tekintsük meg az Owner *(Tulajdonos)* fül tartalmát.
  - Itt megvizsgálhatjuk, illetve megfelelő jogosultsággal módosíthatjuk az adott objektum tulajdonosi viszonyait, lévén minden egyes erőforrásnak (a hálózati megosztások kivételével) létezik tulajdonosa is. Ha például a felhasználó létrehoz egy mappát, akkor automatikusan ő válik a tulajdonossá.
  - Érdekes jellemző, hogy annak ellenére, hogy a tulajdonosi viszonnyal nem feltétlenül jár együtt a legmagasabb jogosultság, (ha van egyáltalán bármilyen is), viszont a jogokat gond nélkül kioszthatja másoknak.

Rendszerfelügyeleti szempontból lényeges dolog, hogy a tulajdonos „ész nélküli" jogosultságosztogatási lehetőségét fékezve, a rendszergazdacsoport tagjai rendelkeznek a Take Ownership *(Saját tulajdonba vétel)* jogosultsággal. Ez akkor is így van, ha a tulajdonos letilt bennünket. Ez azért fontos, mert néha – mikor mint üzemeltetők nem szerepelünk a jogosultsági listában és nem vagyunk tulajdonosok sem – ezzel a joggal felvértezve, a saját tulajdonbavétel lesz a mentsvárunk a fájl biztonsági beállításainak megváltoztatására.

- A következő fül, az Effective Permission *(Hatályos engedélyek)* egy kifejezetten hasznos eszköz, amellyel egy a rendszerben lévő tetszőleges felhasználó vagy csoport konkrét és aktuális jogosultságait kilistázhatjuk, az adott mappára vonatkozóan. Ezzel pillanatok alatt kiderülhet, hogy az esetlegesen jól összekuszált csoport-, illetve egyénileg kapott jogosultságok halmazának mi a végeredménye.

A fájlrendszer hozzáférés szabályzása

Minden objektum egyedi, rá jellemző hozzáférési listával rendelkezik, amelyek beállítási részleteit és lehetőségeit már bemutattuk. A konkrét jogosultságok ismertetése viszont még hátravan. Ebben az alfejezetben a mappák, és a fájlok jogosultságairól lesz szó, de a hálózati és a nyomtatási jogosultságokra is kitérünk a következő részekben.

A fájlrendszerhez, (csak az NTFS-ről beszélünk), kapcsolódó jogosultságoknál viszont szét kell választanunk a fájlokra és a mappákra vonatkozó lehetőségeket. Ezen a területen a mappákra vonatkozó opciók szélesebb körűek, ennek oka elsősorban az, hogy azok további mappákat, illetve fájlokat is tartalmazhatnak, azaz összetettebb felépítésűek. Ha jó alaposan megnézzük a 3.8. ábrát (117. oldal), akkor azt vehetjük észre, hogy az összes kiosztott jogosultság az adott mappára, az almappáira és a bennük lévő fájlokra érvényes – ez részben kiderül az *Apply to* oszlopból. De nem feltétlenül kell, hogy ez így legyen, tetszés szerint szűrhetjük a jogosultságokat e szerint a hármas tagozódás szerint, bármelyik szinten a mappák között.

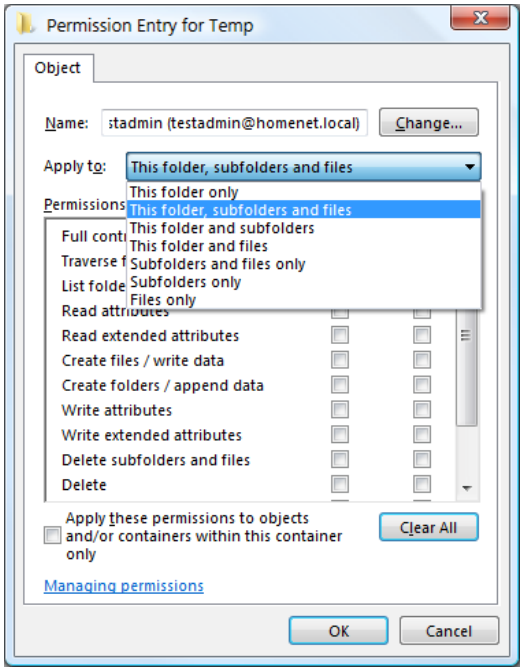
A mappákon állítható alap jogosultságok a következőek:

- **Write** *(Írás):* Fájlok, almappák létrehozása, módosítása, attribútumaik megváltoztatása, írás meglévő fájlokba.
- **Read** *(Olvasás):* A mappa tartalmának listázása, fájlok, mappák és attribútumok olvasása.
- **List Folder Contents** *(Mappa tartalmának listázása):* A Read jog, plusz a könyvtár „bejárása”, valamint az ACL-listák elolvasása.
- **Read and Execute** *(Olvasás és végrehajtás):* Az előző két jog együttese, plusz a fájlok futtatása

- **Modify** *(Módosítás):* A Write + a Read and Execute együttese
- **Full Control** *(Teljes hozzáférés):* Minden létező jogosultság

Azt is tisztán kell látnunk, hogy ezek gyakorlatilag jogosultságcsoportok, amelyeknek további konkrét elemeik is vannak, azaz ennél sokkal finomabban is szabályozhatunk, ha a következő képen látható, részletes mappa jogosultságokat használjuk.

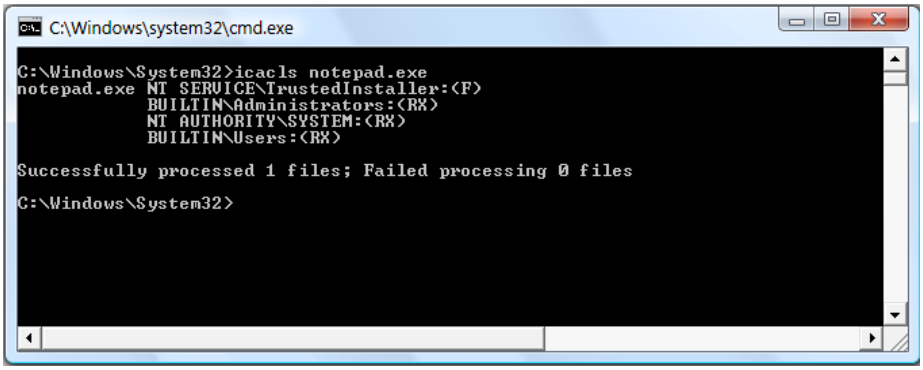
A fájlokkal kapcsolatban ugyanezeket az alapjogosultságokat kapjuk, azonban a jogosultságuk egyszerűbb, hiszen például egy Delete Subfolders and Files *(Almappák és fájlok törlése)* részletes jogosultságból csak az egyik rész lehet érvényes esetükben.



3.9. ábra: *A mappák részletes jogosultságai, illetve a hatókör lehetőségei*

Fájlrendszer jogosultságok kezelése a parancssorból

A jogosultságok parancssorból is kezelhetők, így igény szerint szkriptelhető és automatizálható is a folyamat. A Windows korábbi verzióiban használatos *cacls* (Change Access Control Lists) parancsot a Vistában a továbbfejlesztett, több lehetőséget nyújtó *icacls* váltja fel. Az elérhető paraméterek ismertetéséhez használjuk az *icacls /?* utasítást.



3.10. ábra: *A jogosultság kiosztó parancssori eszköz szintén univerzális*

Jogosultságkezelés alapok
Ebben a screencastban az operációs rendszer partíció, fájl- és mappa szintű hozzáféréseinek szabályzásáról lesz szó, részletes példákon keresztül.
Fájlnév: I-3-1a-Jogosultsagkezeles.avi

A hálózati megosztások jogosultságai

Ha egynél több számítógépet használunk egy szervezetben, már felmerülhet az igény bizonyos erőforrások, például a fájlok és a mappák közös használatára. A Windowsban lehetőség van ezeknek az erőforrásoknak a megosztására, így – megfelelő jogosultságok birtokában – távolról is egyszerűen elérhetjük őket. A megosztott objektumokat általában egy helyen, az első fejezetben bemutatott Computer Management MMC konzolból kezelhetjük, itt például felvehetünk, törölhetünk megosztásokat, illetve módosíthatjuk a meglévők biztonsági beállításait, de gyakorlatilag minden mappa tulajdonságai között is megtaláljuk ezt a lehetőséget [Share… *(Megosztás…)*].

A Windows Vistában további kétféle módon, varázslókkal is megoszthatunk mappákat: adott egy egyszerűsített megoldás, illetve a klasszikus változat is a rendelkezésünkre áll. Az, hogy melyiket kapjuk, azon múlik, hogy a vezérlőpulton a Folder Options *(Mappa beállításai)* alatt, a View *(Nézet)* fülön bekapcsolva hagytuk-e az alapértelmezett Sharing Wizardot *(Megosztás varázsló)*. Ha igen, akkor az egyszerűsített változattal is dolgozhatunk, ha nem akkor csak és kizárólag a klasszikussal.

A mappamegosztás engedélyezése esetén a számítógépünk egyből fájlkiszolgálóvá változik (azért nem úgy, mint egy valódi hálózati kiszolgáló operációs rendszer, részletekért lásd a 4. fejezetet) – míg a megosztáshoz kapcsolódó másik gépből ügyfél lesz. Fontos körülmény, hogy a mappamegosztásokat

nem az egyes felhasználók végzik (viszont csak az emelt szintű jogosultsággal rendelkező felhasználók indíthatják a megosztás folyamatát), hanem az operációs rendszer. Ez azért fontos, mert ennek megfelelően a hálózati megosztás eléréséhez elég a számítógép bekapcsolt állapota, nem szükséges egy-egy felhasználó interaktív belépése. Ebből az is következik, hogy a konfigurált megosztások a rendszer újraindítása után is megmaradnak és a következő alkalommal is elérhetőek lesznek.

A megosztások beállításához és működéséhez a File and Printer Sharing *(Fájl- és nyomtatómegosztás)* szolgáltatásnak engedélyezve kell lennie az adott hálózati profilban. Ezt a Network and Sharing Centerben *(Hálózati és megosztási központ)* tudjuk ellenőrizni.

Általában szükséges és elvárt lépés a megosztásokhoz jogosultságokat is kiosztani. Ez esetben mindenképpen hitelesítenie is kell magát az ügyfélgép felhasználójának. A mappamegosztásoknál alapvetően csak három jogosultsági szint létezik, amelyek az engedélyek szintje szempontjából gyakorlatilag teljesen megegyeznek az NTFS ugyanilyen nevű jogosultságaival:

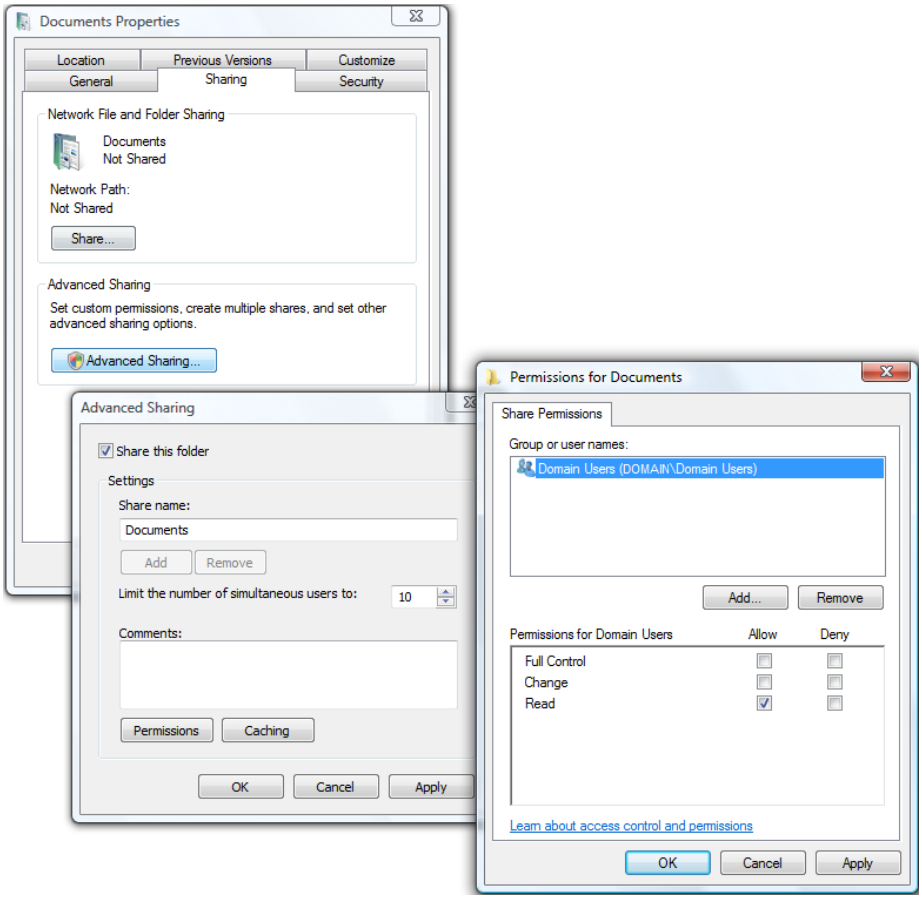
- Read *(csak olvasás),*
- Modify *(módosítás),*
- Full Control *(teljes hozzáférés).*

Fontos tudni azt is, hogy a helyi fájlrendszeren (NTFS) érvényes és a hálózati megosztásnál megadott jogosultságok közül – párhuzamosság esetén – mindig a szigorúbb, (más szóval a különböző jogosultságok metszete), lesz az érvényes, tehát ha az egyik ponton csak olvasást, a másikon pedig írást is engedélyezünk az objektumhoz, akkor csak olvasásra férhetünk majd hozzá.

Szemléltessük ezt egy példa segítségével: a *gtamas* felhasználó tagja a Users, illetve a HaladoUsers csoportnak is. A *D:\Temp* mappához emiatt aztán többféle NTFS-jogosultsága is van, illetve mivel ez egy megosztott mappa is egyben, és más gépről is el kell érnie, megosztási joggal is rendelkezik a csoporttagsága révén.

Felhasználó/ csoport	NTFS jogok	Megosztás jogok	Érvényes jog
gtamas	Full Control	Read	
Users	Modify	–	
HaladoUsers	Modify	Read	
Összegzés	**Full Control**	**Read**	**Read**

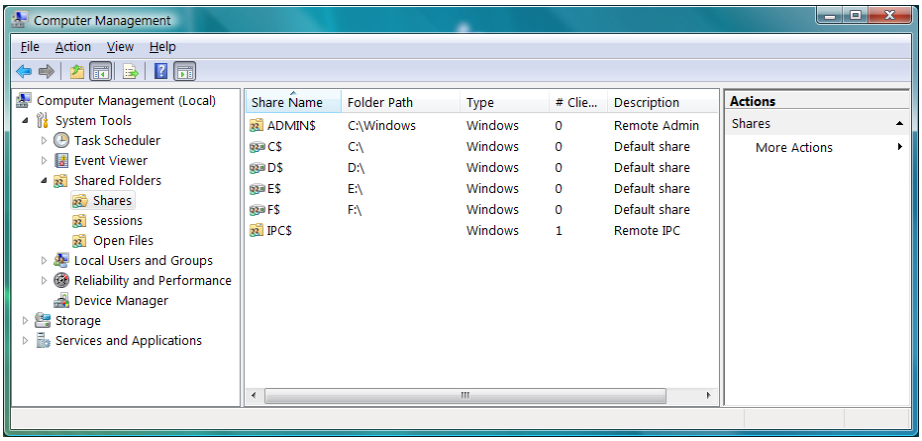
A megosztásokat a grafikus felhasználói felületen kívül parancssorból is kezelhetjük a *net* parancs *use* paraméterrel történő használatával. Az aktuális hálózati megosztások listájához csak egyszerűen, egyéb kapcsolók nélkül adjuk ki a *net use* utasítást.



3.11. ábra: *Jogosultságok a Windows Vista egy megosztott mappáján*

Speciális megosztások

A Windows operációs rendszerekben hagyományosan és alapértelmezés szerint léteznek speciális megosztások is, elsősorban a rendszergazdák munkájának könnyítése, illetve a számítógépek és alkalmazások egyszerűbb kommunikációja okából. Ezeket Default Administrative Shares-nek *(alapértelmezett felügyeleti megosztásoknak)* hívjuk, és a már többször említett Computer Management MMC-ben tekinthetjük meg ezek listáját, de a *net share* parancs is képes ugyanerre.



3.12. ábra: *Jogosultságok a Windows Vista egy megosztott mappáján*

Ezen megosztások közös jellemzője, hogy a nevük a $ karakterrel kezdődik, amely gyakorlatilag annyit jelent, hogy a gépünk hálózatból történő tallózásnál nem fognak látszani, csak direktben, közvetlenül a teljes megosztási név *(\\gép\megosztas$)* formájában lehet ezekre hivatkozni. Viszont mi magunk is hozhatunk létre a *$* jellel rejtett megosztásokat. Az is látható az ábrából, hogy mindegyik partíció rendelkezik alapértelmezés szerint, (anélkül, hogy megosztanánk), egy-egy ilyen megosztással. Ezen kívül a következő speciális mappák rejtett megosztások is egyben:

- ADMIN$: Az adott operációs rendszer rendszerkönyvtára, általában a *C:\Windows* mappa.
- IPC$: Hálózatban, a gépek közötti kommunikációt szolgáló megosztás *(Inter-Process Communication).*
- Print$: nyomtató esetén, a nyomtatómeghajtó program lelőhelye lesz ez a megosztás, általában a *C:\Windows\system32\spool\drivers* mappa.

Erőforrás-megosztás
Ebben a screencastban a Windows Vistával kivitelezhető erőforrás-megosztásról, azaz a fájl- és nyomtatókiszolgálókénti működés lehetőségeit mutatjuk be.
Fájlnév: I-3-1b-Eroforras-megosztas.avi

A megosztott nyomtatók jogosultságai

A Vistában természetesen van lehetőségünk a géphez illesztett nyomtatók megosztására, tipikusan egy másik felhasználó által, a hálózatból történő használatra. Ebben az esetben viszont szükséges lesz jogosultságokat meghatározni az adott nyomtató lehetőségeivel kapcsolatban. A fájlrendszer- vagy a megosztásjogosultságokkal összehasonlítva a nyomtatási jogosultságok lényegesen szűkebb körűek, gyakorlatilag az összeset tartalmazza a következő táblázat.

Jogosultság	Részletek
Print *(Nyomtatás)*	dokumentumok nyomtatása; saját dokumentumok nyomtatási jellemzőinek beállítás; saját dokumentumok nyomtatásának megállítása, újraindítása és törlése.
Manage Printers *(Nyomtatókezelés)*	a nyomtató megosztása; a nyomtató tulajdonságainak megváltoztatása; a nyomtató eltávolítása; a nyomtatási jogosultságok megváltoztatása; a nyomtató leállítása és újraindítása.
Manage Documents *(Dokumentumok kezelése)*	az összes – a nyomtatási sorban lévő – dokumentum nyomtatásának megállítása, újraindítása, mozgatása és törlése.

Ha megosztunk egy nyomtatót, akkor a jogosultsági listájába alapértelmezés szerint bekerül az Everyone csoport, a szimpla nyomtatás joggal, továbbá a jogosultsági listában szerepel még az Administrators csoport is, az összes elérhető nyomtatási jogosultsággal.

A felhasználói engedélyek

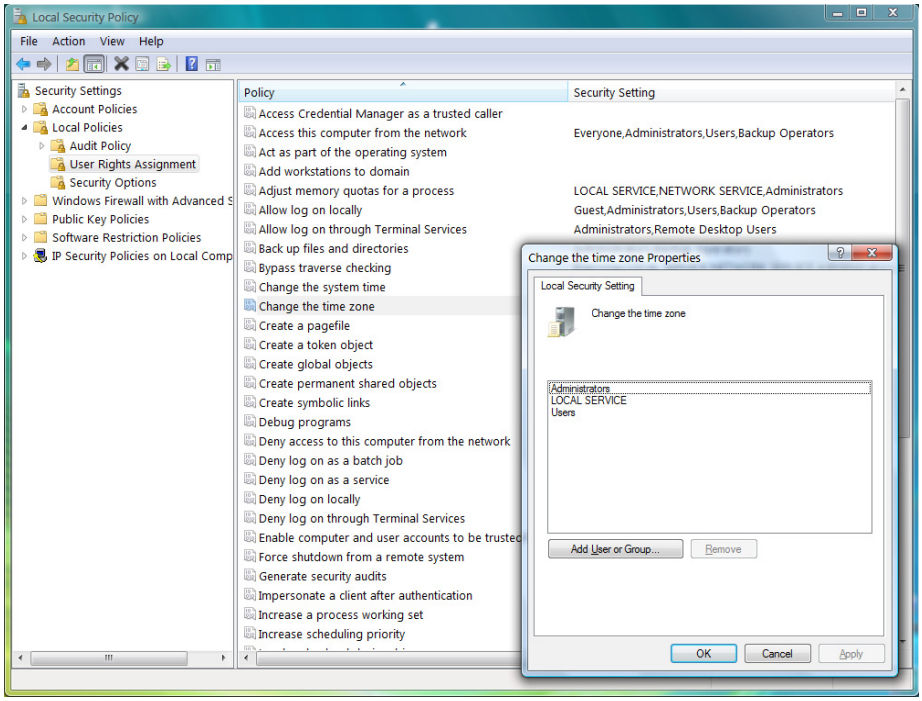
Ha szeretnénk tisztában lenni az erőforrás-kezelés témakörrel, akkor világosan kell látnunk, hogy a hitelesítést követő engedélyezés folyamata (autorizáció) nemcsak a sokkal inkább a szemünk előtt lévő fájl-, megosztás-, vagy pl. a nyomtatási jogosultságokra vonatkozhat, hanem az egész számítógépet érintő engedélyekre is. A különbség éppen a hatókör, azaz az engedélyek tárgya kö-

zött van, mert amíg a jogosultságok általában egy-egy objektumot érintenek, az engedélyek az operációs rendszer működésével kapcsolatosak, ráadásul többnyire eléggé komoly hatást kifejtve.

Ezen engedélyek meghatározása, illetve változtatása általunk is befolyásolható, még ha ezt általában tényleg csak indokolt esetben szükséges elvégezni. Ahhoz, hogy megtekinthessük a gépre vonatkozó engedély listát, indítsuk el a Local Security Policy *(Helyi biztonsági házirend)* MMC-konzolt.

Ezt az MMC-t csak a Business, Enterprise, vagy az Ultimate változatoknál érjük el, viszont ezeknél képesek vagyunk elindítani egyszerűen is: gépeljük be *Start/Run* mezőbe vagy a parancssorba a *secpol.msc* parancsot.

Ezután navigáljunk el a *Security Settings\Local Policies\User Rights Assignment (Biztonsági beállítások\Helyi házirend\Felhasználói jogok kiosztása)* pontra, ahol az összes opciót egy tetszetős, csoportosított listában, az MMC-konzol jobboldali keretében láthatjuk.



3.13. ábra: *Az engedélyeket a házirenden keresztül szabályozhatjuk*

Rögtön látható, hogy jó pár opció esetén már az alapbeállítás, azaz a megfelelő felhasználói fiókok, illetve a csoportok hozzárendelése megtörtént, ami azért logikus, mert pl. az Allow Log On Locally *(Helyi bejelentkezés engedélyezése)* engedély nélkül senki sem használhatná az operációs rendszert. Ha alaposan megnézzük a lista elemeit, akkor azt is észrevehetjük, hogy néhány esetben az engedélyek eleve tiltás formájában is szerepelnek, egy közös Deny (magyarul viszont több, különféle nyelvtani módszerrel megoldott) előtaggal:

- Deny Access This Computer From The Network (A számítógép hálózati elérésének megtagadása)
- Deny Allow Log On Through Terminal Services (Terminálszolgáltatások használatával történő bejelentkezés tiltása)
- Deny Log On As A Batch Job (Kötegelt munka bejelentkezésének megtagadása)
- Deny Log On As A Service (Szolgáltatáskénti bejelentkezés megtagadása)
- Deny Allow Log On Locally (Helyi bejelentkezés megtagadása)

Ezeknek az opcióknak mindig van tehát engedélyező változata is, azaz kétfajta módon is tudjuk finomhangolni a hozzájuk tartozó lehetőséget. Alapértelmezés szerint pl. a helyi belépés engedélyezve van a helyi Guest fióknak, illetve az Administrators, Backup Operators, és Users csoportoknak. Ha valamely felhasználótól szeretnénk elvenni a helyi belépés jogát – annak ellenére, hogy pl. a Users csoport tagjaként ez jár neki –, akkor a tiltó opció alá felvehetjük, konkrétan nevesítve a fiókját. Mivel az tiltás „erősebb" lehetőség, a felhasználó nem fog tudni belépni az operációs rendszerbe.

Ezen engedélyek kiosztása tehát a gyári beállításon alapul, de akár mi magunk is változtathatunk ezen a helyzeten, illetve a rendszer némiképp egy automatizmussal is színesíti lehetőségeket. Egy példa: ha hálózati megosztásokat engedélyezzük a Network and Sharing *Centerben (Hálózati és megosztási központ)*, és egyúttal a jelszóval védett hozzáférést kikapcsoljuk (lehetőleg ne tegyünk ilyet, ez csak egy példa), akkor a Guest fiók kikerül a korábban említett Deny Allow Log On Locally *(Helyi bejelentkezés megtagadása)* engedély opcióból.

Az engedélyek listája terjedelmes (kb. 45 db), értelmük és felhasználási területeik gyakran mély ismereteket igényelnek magáról az operációs rendszerről. Ennek a könyvnek nem szándéka az engedélyek egyenkénti alapos bemutatása, annyit viszont mindenképpen célszerű megjegyezni, hogy ha bármelyik opciót megnyitjuk, akkor az Explain *(Magyarázat)* fülön egy-egy frappáns értelmezést kaphatunk az adott engedély jelentéséről, illetve az esetleges verzió függőségekről is.

A magyarázatoknak a legtöbb esetben része a biztonsági felhívás is, amely szerint óvatosan bánjunk a gyári beállítások konfigurálásával vagy az esetleges törlésekkel, hiszen súlyos, esetleg visszaállíthatatlan sérüléseket is okozhatunk a nem átgondolt változtatásokkal.

Windows XP Service Pack 2 biztonsági változások

A „kényelem + biztonság mindig = 1" tétel miatt kompromisszumok nélküli biztonságról sohasem beszélhetünk. A Windows asztali operációs rendszerek esetén korábban – főként a kompatibilitás és az egyszerű, kényelmes használat okán – némiképp háttérbe szorult a biztonságosság. Hozzátartozik a visszatekintéshez persze az a tény is, hogy nem is kellett olyan mértékű veszélyeztetettséggel számolnunk, mint napjainkban, amikor például az internet révén, a rendszereinket szinte minden oldalról folyamatos támadások érik. A Windows XP 2001-es kiadását követően viszont egyre több problémát okozott a sérülékenységek, illetve a rendszerek elleni incidensek számának növekedése, egyre szükségszerűbbnek látszott az alapos és mélyre hatoló korrekció. A Microsoft ekkor megtette az első szükséges lépéseket annak érdekében, hogy a számítógépes munkakörnyezet ebben az új, veszélyesebb világban is biztonságos és stabil legyen, akár az ügyfél oldali, akár a kiszolgáló oldali operációs rendszerekre gondolunk. Mi most az ügyféloldalra fókuszálva, az XP SP2 változásairól szeretnénk ebben a részben némi ízelítőt adni.

A redmondi szoftverfejlesztők új stratégiája, az úgynevezett Trustworthy Computing *(megbízható számítástechnika)* jegyében végül 2004 augusztusában megjelent a Windows XP második javítócsomagja, a Service Pack 2, mely szinte kizárólag a biztonságról szólt és több olyan újítást is bevezetett, melynek köszönhetően szinte újjászületett a rendszer. A megújult Windows tűzfal például alapértelmezésként bekapcsolásra került, az Internet Explorer pedig – mely mindig is központi téma volt, ha Windows-biztonságról esett szó – az előugró ablakok blokkolásával és a különböző letölthető beépülő modulok továbbfejlesztett kezelésével jeleskedett. A rendszerben az egyre gyakoribbá váló puffer-túlcsordításos támadások elleni védelemként bevezetésre került a Data Execution Prevention (DEP/NX), mely az operatív tár védelmét hivatott szolgálni oly módon, hogy az adatok számára fenntartott memóriacímeken tiltja a kódvégrehajtást. További újdonság volt még a DCOM-rendszerkomponensek és az azokat koordináló RPC-szolgáltatás (távoli művelet végrehajtás) biztonsági szintjeinek emelése.

3.14. ábra: *Security Center*

A felhasználói felületen nem sok minden változott, az egyetlen szembe tűnő újdonság a Security Center *(Biztonsági központ)* megjelenése volt, mely a Windows beépített és a külső fejlesztők által telepített biztonsági szolgáltatások (tűzfal, antivírus, automatikus frissítések) állapotát felügyeli.

Könyvünkben a Windows XP SP2-ben megjelent Security Center bemutatása a Vista Security Centerrel együtt történik meg, a következő alfejezetben.

Újdonságok a Vista biztonsági rendszerében

A Microsoft a Windows Vista készítésének idejére már teljesen új alapokra fektette szoftverfejlesztési stratégiáját, azaz a biztonság – nagyon előkelő helyen – bekerült az elsődleges szempontok közé. Ennek megfelelően az új operációs rendszer soha nem látott technológiaarzenált vonultat fel, melyek mind-mind a rendszer és az adatok védelmét szolgálják. A következőkben a Windows Vista biztonsági szolgáltatásait ismertetjük, az alapoktól egészen a felhasználók számára is tapasztalható megoldásokig.

Védekezés a mélyben

Ebben a részben a Windows Vista olyan felszín alatti, gyakran általunk nem is befolyásolható, beállítható komponenseinek és szolgáltatásainak az áttekintését kíséreljük meg, amelyek majdnem 100%-osan újdonságnak számítanak. Úgy gondoljuk, hogy függetlenül attól, hogy a napi szintű üzemeltetésben nem találkozunk konkrétan ezekkel a megoldásokkal – hanem általában csak maximum az előnyeiket élvezzük –, tájékozottnak kell lennünk a biztonságos működés megteremtésének minden részletével. Ennek megfelelően a jelen fejezetbe a *programkód*, a *kernel*, a *rendszerfájlok*, és a *memória* védelmével, sérthetetlenségével és működési specialitásaival kapcsolatos tudnivalókat szerkesztettük össze.

A programkód integritásának védelme

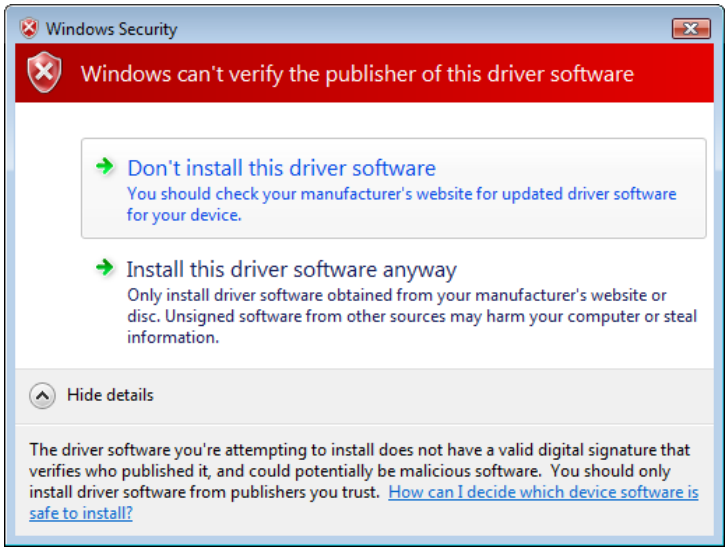
A Windows rendszerfájlok védelme az illetéktelen módosítások és cserék ellen alapvető fontosságú a rendszer stabilitása és megbízhatósága szempontjából. A rendszerkomponensek védelmére már a korábbi verziókban is volt eszköz (System File Checker, SFC), a Windows Vista azonban már a rendszerbetöltő és a kernel szintjén tartalmaz egy szolgáltatást, mely a kritikus rendszerfájlok kód-aláírását ellenőrzi.

A 64-bites operációs rendszerek támogatása apropóján új hardverek, új eszközmeghajtók, és új alkalmazások jelennek meg, ezért a Microsoft számos új – a kompatibilitás megőrzése miatt eddig megvalósíthatatlan – megoldást épít be 64-bites termékeibe, melyek így végre „tiszta lappal”, az alapoktól kezdve biztonságosként épülhetnek meg.

A Windows Vista 64-bites támogatása az x64-es rendszerek esetben értendő, Itaniumra készült változatot a Microsoft nem adott ki. A 64-bites operációs rendszerekről részletesebb információt a következő TechNet Magazin cikkből érhetünk el: http://download.microsoft.com/download/a/1/a/a1ac3b96-011e-4cca-9dba-78973187567d/26-29.pdf vagy http://tinyurl.com/2q22jz

A 32-bites világgal egyelőre természetesen fenn kell tartani a kompatibilitást, a kód integritás védelem így a 32- és a 64-bites platformokon némiképp eltérően működik.

- **x64**
  - Minden kernelmódban futó kódot digitális aláírással kell ellátni. Ez biztosítja, hogy a fájl bizonyíthatóan a saját kiadójától származzon. Ha a komponens nincs aláírva, a Windows megtagadja az állomány futtatását.
  - A külső kódoknak – illesztőprogramok, segédalkalmazások stb. – WHQL-kompatibilitási és minőségi, illetve Microsoft Certificate Authority tanúsítvánnyal kell rendelkezniük. Ez alól semmilyen program nem lehet kivétel.
- **x86**
  - A kompatibilitás fenntartása érdekében a 64-bites platformhoz képest több kompromisszumra is kényszerült a Microsoft. A digitális aláírást csak illesztőprogramok esetén ellenőrzi a rendszer, de ha a kód nem rendelkezik ilyennel, a Windows akkor is engedélyezheti a telepítést, ami házirend, vagy beállításfüggő opció is lehet, tehát egy vállalati hálózatban megkövetelhetjük a csoportházirenden keresztül a kötelező aláírást. A Microsoft által szállított, beépített eszközmeghajtók természetesen mind rendelkeznek aláírással.
  - Az alkalmazásszinten futó programoknál nem követelmény sem a digitális aláírás, sem a WHQL-tanúsítvány, ez azonban szintén a biztonsági házirendből szabályozható, tehát a rendszergazda opcionálisan engedélyezheti a védelmet.



3.15. ábra: *Figyelemfelhívás eszközmeghajtó telepítéskor*

A Vista rendszervédelem

A Vista Windows Resource Protection (WRP) megoldását sokszor a korábbi Windows File Protection (WFP) megoldással azonosítják. A WFP a Windows 2000-rel és egy hasonló megoldás, a System File Protection (SFP) pedig a Windows Millennium Editionel lett bevezetve. Mindkettő hasonlít a WRP-re de szignifikáns eltérések vannak a megvalósításban.

A WFP csak fájlokat figyel, míg a WRP a kritikus fájlokat, mappákat és a regisztrációs adatbázis bejegyzéseit is védi. A WFP/SFP csak a védett rendszerfájlokat érintő módosításokat figyeli. Amennyiben ezek a változások nem hitelesítettek, a WFP/SFP visszacseréli a módosult állományokat egy korábbi megbízható mentésből. A leggyakoribb figyelmeztetés, amit a WFP korábban adott, egy felhasználói figyelmeztetés, vagy egy eseménynapló-bejegyzés volt.

A WRP tovább erősíti a rendszererőforrások védelmét, kiterjesztve a védelmet a regisztrációs adatbázisra és rendszermappákra is. A Vista esetében a Rendszergazdák *(Administrators)* csoport tagjai sem módosíthatják a rendszererőforrásokat. Alapértelmezés szerint csak a Windows Trusted Installer security principal jogosult módosításokra a Windows Module Installer szolgáltatáson keresztül. Ezt használja a Windows Installer, a *hotfix.exe*, és az *update.exe* is.

A rendszergazdáknak azonban jogukban áll módosítani és tulajdonba venni a védett rendszererőforrásokat is, és teljes jogot adniuk maguknak, így módosítani vagy törölni is rendszer számára kritikus állományokat. A WFP-vel ellentétben a WRP viszont nem állítja helyre automatikusan a védett állományokat megbízható mentésből, csak újraindítás során állítja vissza a rendszer indulásához szükséges állapotot.

Ahhoz, hogy a WRP visszaállítsa az összes védett erőforrást (ami hasznos lehet egy hibakeresés során) futtassuk a következő parancsot: *sfc /scan now*. A védett fájlok eredeti állapotának visszaállításához szükséges lehet a Vista telepítőmédia is.

Kernel-patch Protection (PatchGuard)

A kernel, vagyis a rendszermag a legalacsonyabb szintű komponense az operációs rendszernek. A rendszerindítási folyamat során elsőként töltődik be, majd olyan feladatokat lát el, mint a programok indítása, memória-, és a fájlrendszer kezelése. A kernel teszi lehetővé, hogy az egyes alkalmazások „beszélgethessenek" a hardvereszközökkel, így a mag sebessége és megbízhatósága alapvető fontosságú a rendszer egészére nézve.

A kernel külső eszközökkel történő módosításával szükségszerűen megbomlik a mag integritása, ami kihatással lehet a Windows stabilitására, de akár biztonságára is. A különböző védelmi programok (antivírusok, antispyware alkalmazások) gyártói a múltban gyakran alkalmazták ezt az eljárást, hogy elejét vegyék egy-egy fertőzésnek azáltal, hogy közvetlenül kernelszinten akadályozták meg egyes ártalmas programoknak, hogy bizonyos rendszerfüggvényeket hívjanak meg. Sajnos azonban nemcsak az antivírus cégek alkalmazták a kernelmódosítást, hanem a különböző vírusokat készítő programozók is, hiszen ilyen módon akár a fájlkezelők elől is elrejtőzni képes, úgynevezett rootkiteket is bejuttathattak a rendszerbe, amelyek aztán szabadon garázdálkodhattak, anélkül, hogy bármely védelmi program tudomást szerzett volna jelenlétükről.

A kernelmódosítás elleni védelem nem újkeletű, először a Windows XP és a Windows Server 2003 64-bites változataiban találkozhattunk vele az x64-es AMD64 és Intel EM64T processzorok bevezetésének ideje körül. A 64-bites Windows Vistában azonban megkerülhetetlen lett a technológia – amint a Windows jogosulatlan kernelmódosítást érzékel, automatikusan leállítja a rendszert.

Azért, hogy a biztonságtechnikai cégek különböző védelmi programjai a továbbiakban is együttműködhessenek a rendszerrel, a Microsoft olyan további technológiákat bocsát a cégek rendelkezésére, melyekkel a kernel módosítása nélkül is megfelelő kiegészítő védelemmel láthatják el a felhasználókat:

- **Windows Filtering Platform** *(Windows szűrőplatform)* – olyan hálózati műveletek engedélyezése, mint a csomagelemzés, például harmadik féltől származó tűzfal működésének támogatásához.
- **File System Mini Filter** – programok hozzáférésének biztosítása a fájlrendszer-műveletek figyeléséhez.
- **Registry Notification Hooking** – a Windows XP-ben bemutatott, de a Vistában továbbfejlesztett eljárás, mely lehetővé teszi a programoknak, hogy valós időben kövessék a rendszerleíró-adatbázis módosulásait.

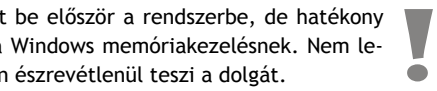
Address Space Layout Randomization (ASLR)

Az Address Space Layout Randomization hasznos rendszerszintű újítás a Windows Vistában. A technológia lényegében egy memóriavédelmi megoldás, mely azáltal, hogy véletlenszerűen megkeveri a memóriacímeket, nagyban megnehezíti a káros programok működését.

Az eljárás lényege, hogy a Windows egy-egy program vagy folyamat kulcsterületeit (futó kód, könyvtárak, heap, vermek stb.) minden alkalommal véletlenszerűen meghatározott memóriacímekre tölti be, ellentétben a régebbi, ASLR nélküli eljárással, amikor a rendszerfüggvények minden esetben ugyanarra a memóriacímre kerültek, tehát közismertté vált a tartózkodási helyük. Ha egy vírus káros kódot szándékozik injektálni a memóriába, először megpróbál meghívni egy rendszerfüggvényt, majd vár ennek a függvénynek a visszatérési értékére. Mivel az ASLR véletlenszerűen (és külön-külön) mozgatja a függvényeket a memóriában – egészen pontosan 256 különböző helyre töltheti be őket minden egyes alkalommal –, a vírusnak 1/256-od esélye van, hogy éppen eltalálja azt a memóriacímet, ahol a kiszemelt érték tartózkodni fog. Ez a technika megnehezíti egy lehetséges külső támadó dolgát, mert egyrészt nem jósolható meg előre a konkrét memóriacím, másrészt a kiszámítása (helyesebben próbálgatása) sem túlságosan kifizetődő módszer. Az ASLR hatóköre a következőkre terjed ki:

- visszatérési verem;
- heap- (vagy halom-) memória;
- az operációs rendszer részeként települő összes bináris állomány.

Az ASLR viszonylag későn, a Beta 2-es verzióban került be először a rendszerbe, de hatékony védelemnek bizonyult, így végül szerves részévé vált a Windows memóriakezelésnek. Nem lehet kikapcsolni, de engedélyezni sem kell – a háttérben észrevétlenül teszi a dolgát.



Az alábbi ábra néhány rendszerkomponens memóriában történő elhelyezkedését mutatja két indítási folyamat után.

- user32.dll (0x779b0000)
- kernel32.dll (0x77c10000)
- gdi32.dll (0x77a50000)

- user32.dll (0x770f0000)
- kernel32.dll (0x77350000)
- gdi32.dll (0x77190000)

Data Execution Prevention (DEP/NX)

A helytelen memóriahasználat azt jelenti, hogy valamilyen program egy nem futtatható kódot tartalmazó memóriaterületet erővel kódfuttatásra akar használni. Tipikusan ilyenek azok a rosszindulatú programok, amelyek egy esetleges puffer-túlcsordulásos sérülékenységet kihasználva tárolnak le futtatható gépi utasítások sorozataként értelmezhető adatokat (=program) verem-, adat-, heap- stb. területként kijelölt memóriába, majd az így betöltött kódnak adják át a vezérlést.

A DEP úgy védekezik az effajta támadások ellen, hogy az adatszegmensek számára fenntartott memóriacímeket *nem futtatható*-ként jelöli meg, így ezekről a területekről nem indítható kód. A DEP működéséhez vagy operációsrendszer- vagy processzorszintű támogatás szükséges, így beszélhetünk hardveres, illetve szoftveres DEP-ről is.

- **Hardveres DEP** – A legtöbb ma kapható processzor (az összes 64-bites CPU, valamint egyes 32-bites Intel és AMD processzorok is) már rendelkezik ezzel a képességgel. Az erre alkalmas processzorok a memória kezelésekor belsőleg használt lapozótábla-bejegyzések utolsó bitjét NX (No eXecute) mutatóként értelmezik: 0 esetén a hivatkozott területen lehetséges, 1 értéknél tilos a kód futtatása. (Megjegyzendő, hogy az NX az eredeti AMD-s elnevezés, az Intel terminológiájában XD bitről – eXecute Disable – beszélünk.)
- **Szoftveres DEP** – A DEP NX vagy XD bittől független, szoftveres megvalósítása kicsit bonyolultabb, de nem lehetetlen. Az eljárás neve – Safe Structured Exception Handling (SafeSEH), vagyis biztonságos *struktúrájú kivételkezelés* – már mutatja, hogy a memóriavédelem ez esetben a Windows kivételkezelő mechanizmusán keresztül valósul meg. A SafeSEH követelményeinek eleget tevő programoknak futtatáskor regisztrálniuk kell saját kivételkezelő eljárásukat. Régebbi, a DEP-et nem támogató alkalmazások használatakor a rendszer a kivételnek megfelelő funkció hívása előtt megvizsgálja: maga a kivételkezelő kód futtatható memóriaterületen van-e.

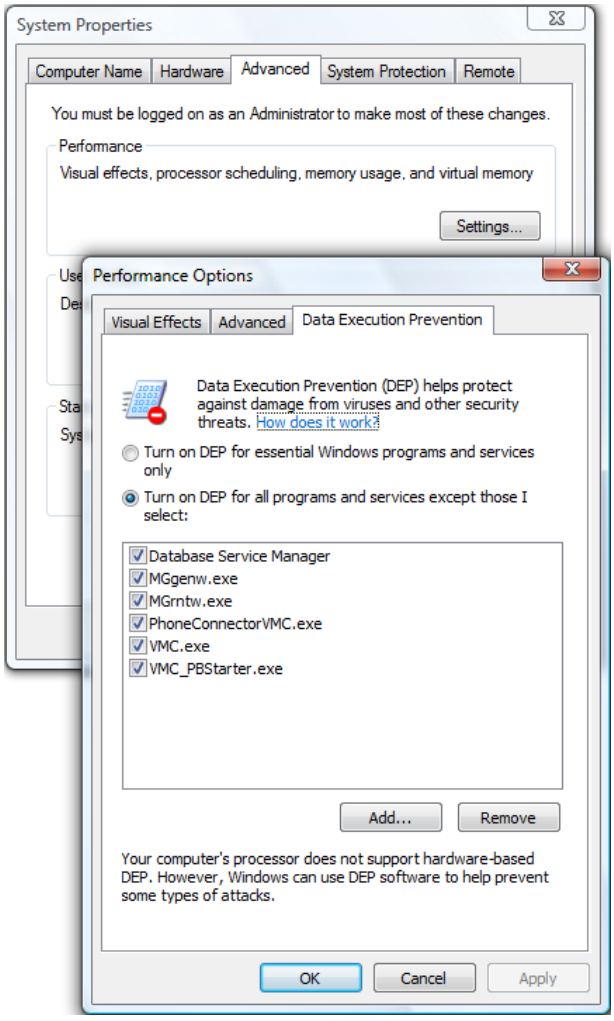
Akár hardveres, akár szoftveres DEP-ről van szó, a rendszer nem javítja ki például a puffer-túlcsordulásos sérülékenységeket, és nem akadályozza meg memóriaterületek felülírását. Amikor azonban a vezérlés adatterületre kerülne, akkor vagy hardveres kivétel generálódik, vagy a kivételgenerálást az operációs rendszer szoftveres úton végzi el, mely során az ártó kódok lefülelhetők.

A DEP beállításait Windows XP, illetve Windows Server 2003 esetében a rendszerbetöltés indításáért felelős *boot.ini* konfigurációs fájlban határozhatjuk meg, mely a rendszerpartíció gyökérkönyvtárában foglal helyet. Az operációs rendszer bejegyzésének végén található */noexecute* kapcsolónak négy állása van: *AlwaysOn, AlwaysOff, OptIn* és *OptOut*.

- AlwaysOn – A DEP engedélyezve van, kivétel nélkül minden futtatható állományra.
- AlwaysOff – A DEP le van tiltva.
- OptIn – A DEP csak a Windows saját futtatható állományaira vonatkozik. Ez az alapértelmezett beállítás.

- OptOut – A DEP minden futtatható állományt felügyelete alatt tart, de a rendszergazdák a *Control Panel/System/Performance* lapján kivételeket képezhetnek a memóriavédelmi eljárás hatóköre alól.

A felsorolt kapcsolók mindegyike érvényesül hardveres és szoftveres DEP-nél egyaránt. A rendszer a *boot.ini*-be írt explicit */noexecute= OptIn* kapcsolóval települ, illetve amennyiben a *boot.ini*-ből valamilyen okból eltávolítják a */noexecute* kapcsolót, akkor a Windows úgy viselkedik, mint ha a */noexecute=OptIn* lenne érvényben.



3.16. ábra: *Akcióban a DEP, a lista szereplői pedig a kivételek a hatása alól*

Mivel a Windows Vista már nem használja a *boot.ini* állományt, (sem az NTLDR rendszerbetöltőt), az új Boot Configuration Data (BCD) szerkesztésével konfigurálhatjuk a DEP-et. Ehhez használjuk a beépített *bcdedit* parancsot, mely paraméterek nélkül tájékoztatást ad a DEP pillanatnyi állapotáról.

A DEP *bcdedit*-tel történő beállításához a következő parancsokat használhatjuk (a paraméterek jelentése megegyezik a korábbiakkal):

- bcdedit /set nx OptIn
- bcdedit /set nx OpOut
- bcdedit /set nx AlwaysOn
- bcdedit /set nx AlwaysOff

A szolgáltatások megerősítése: Service hardening

A Windows szolgáltatások kedvelt támadási célpontjai a különböző vírusoknak és egyéb kártevő programoknak, mert ezek a folyamatok többnyire rendszerjogosultsági szinten futnak, tehát lényegében bármihez korlátozás nélkül hozzáférhetnek. A Vista ezen a téren is újít, a szolgáltatások zöme immár nem a *LocalSystem* fiók nevében fut, így nincs is teljhatalma a rendszer fölött.

Néhány szó a szolgáltatásfiókokról

A szolgáltatásfiókok előre definiált hozzáférési lehetőségek a Windows beépített szolgáltatásainak futtatásához. A Windows Vista három ilyen fiókkal rendelkezik (miként a korábbi operációs rendszerek is).

A „legerősebb" ún. *LocalSystem* fiók nem rendelkezik jelszóval, mégis teljes hozzáférése van a rendszer egészéhez, magában foglalja a beépített Administrators *(Rendszergazdák)* csoport jogosultsági körét is, hálózati környezetben pedig ez a szolgáltatás testesíti meg magát a „számítógépet", tehát a hálózati hitelesítés is ezen a fiókon keresztül történhet.

A szolgáltatások korábban szinte kivétel nélkül a *LocalSystem* fiók használatával futottak, így sokszor szükségtelen jogosultságokat kaptak, ami az előbb leírtakat figyelembe véve komoly biztonsági aggályokat vethet fel. A Windows Vistában az XP-hez képest a szolgáltatások töredéke fut helyi rendszerfiókkal, a többségük átkerült a csökkentett jogosultságokkal rendelkező *LocalService*, illetve *NetworkService* fiókokba.

Viszont a szolgáltatás működéséhez néha azért elengedhetetlenül szükséges, hogy rendszerjogosultságokat élvezzen, ezért a Microsoft programozói egy trükköt vetettek be: ezeket a szolgáltatásokat egyszerűen „kettévágták", és a kódnak csak a privilegizált műveleteket végző része fut a *LocalSystem* fiók

alól, a többi továbbra is a *LocalService* hatókörében marad. A biztonság további fokozása érdekében a megosztott szolgáltatások két része közötti kapcsolathoz hitelesítés szükséges.

Emellett a szolgáltatások a felhasználókhoz hasonlóan saját egyedi biztonsági azonosítót kaptak, melyek az alábbi formátumban tárolódnak:

S-1-80-<a szerviz logikai nevének SHA-1 hash-e>.

Szintén a felhasználókhoz hasonlóan az egyes szolgáltatásoknak is csak adott műveletekhez van jogosultságuk. Ezeket a privilégiumokat a Registry tárolja, a *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* kulcs alatt, a *RequiredPrivileges* értékben. A szolgáltatásfiókokhoz természetesen ACL is tartozik, így minden egyes szolgáltatásnak gondosan kijelölt munkaterülete van, melyen kívül nem tevékenykedhet, így még ha egy esetleges vírustámadás során a kártevő kód át is venné az irányítást a szolgáltatás fölött, akkor sem okozhat helyrehozhatatlan kárt. A szolgáltatások számára biztosított privilégiumok megfelelően kordában tartják a folyamatokat, korlátozzák a fájlrendszer és a registry használatát, valamint a Windows tűzfal által a hálózati kommunikációt is.

Hogy egy gyors példával demonstráljuk az új szolgáltatáskorlátozás jelentőségét, tekintsünk kicsit vissza az időben, 2003 augusztusára, amikor a *Blaster/Sasser* féregvírus globális problémákat okozott a Windows vehemens támadásával. A *Blaster* a rendszer egyik alapvető szolgáltatását, a Remote Procedure Call (RPC – *távoli eljáráshívás)* kerítette hatalmába, és a Windows folytonos újraindításával okozott fejfájást a felhasználóknak. A féreg ma már szinte semmilyen kárt nem tudna okozni, mert a Windows Vistában az RPC-szolgáltatás is átesett a fenti változásokon így:

- nem cserélhet le rendszerfájlokat,
- nem módosíthatja a registryt,
- nem befolyásolhat más szolgáltatásokat, és nem módosíthatja azok beállításait (például antivírus szoftverekét).

A szolgáltatások biztonsági konfigurálása a Windows telepítése során automatikusan megtörténik, azonban csak a rendszer saját beépített összetevőire érvényes, a külső és utólag telepített szolgáltatásokra nem.

Service Hardening
A rendszerszolgáltatások megerősítése fontos pont a Vista biztonságosságával kapcsolatban. Ebben a mini előadásban ezzel kapcsolatban mutatunk be részleteket.
Fájlnév: I-3-3a-Service-Hardening.avi

Változások a felhasználó fiókok és csoportok kezelésében

Ezen a területen az egyik legfontosabb változás a beépített Administrator *(Rendszergazda)* azaz a helyben egyetlen 500-as RID-del (a SID utolsó blokkja, 3-4 számjegy, normál felhasználók/csoportok esetén 1000-sel kezdődik) rendelkező fiók letiltása. Erre azért volt szükség, mert a gondatlanabb felhasználók és rendszergazdák a Windows telepítésnél általában nagyon gyenge jelszóval (pl. *123456*, *password*) látták el ezt a fiókot, vagy egyszerűen nem is adtak meg jelszót. A tiltás viszont passzol a Vista biztonsági modellhez, mert például egyrészt az UAC (lásd következő alfejezet) hatása nem terjed ki erre a fiókra, másrészt a hétköznapi munkára ne használjuk ezt a fiókot, mert nem erre való, ahogyan más rendszerekben sem.

Viszont néha mégiscsak szükségünk lehet erre a fiókra is, de ha le van tiltva, akkor hogyan érjük el? Mindig le van tiltva? Nem, speciális körülmények között, három esetben biztosan megkapjuk majd automatikusan az Administrator fiókot:

1. Csökkentett mód.
2. Startup Repair mód (a Vista DVD-ről indítva a rendszert).
3. Frissítő telepítés után (pl. XP > Vista).

Viszont mindegyik esetben csak és kizárólag akkor „él" automatikusan ez a fiók, ha nincs egy másik, a helyi Administrators csoportba tartozó fiók is a rendszerben, akár tartományban van a gép fiókja, akár nem.

Ide tartozik még az az újdonság is, hogy amennyiben egy új fiókot hozunk létre a rendszerben, az alapértelmezésként korlátozott felhasználói jogosultságokat kap.

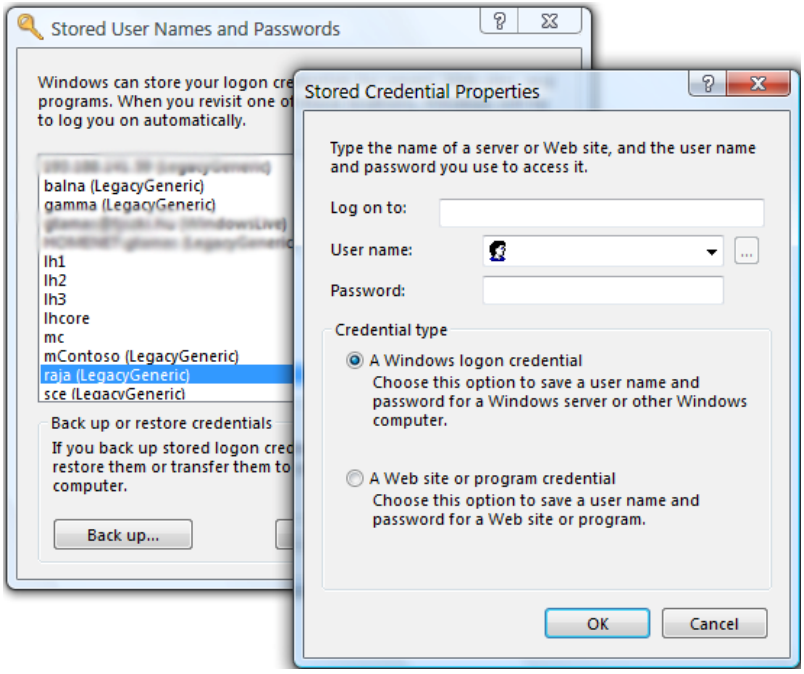
A felhasználói fiókokat érintő változások közül meg kell említenünk a korábbi a Windows XP-ben okban alapértelmezés szerint jelenlévő *Support* és a *Help* fiókok megszüntetése.

A csoportokról szólva, a legnagyobb változás a Power Users *(Kiemelt felhasználók)* csoport hatóköre gyakorlatilag megszűnt. Mivel a nevével ellentétben megtévesztően sok jogosultsággal rendelkeztek ennek a csoportnak a tagjai, így a rendszergazdák előszeretettel osztogattak efféle jogköröket a felhasználóknak – sok esetben teljesen feleslegesen. Két működő jogosultsági szint maradt tehát: Standard felhasználók (Users csoport), és a Rendszergazdák *(Administrators)* csoport.

Ezen kívül, a változó igényeknek megfelelően új csoportjaink is vannak, lássunk néhány példát:

- Cryptographic Operators: a PKI-val, IPSec-kel kapcsolatos feladatok jogosultságainak birtokosai.
- Distributed COM users: jogosultság az elosztott COM-objektumok eléréséhez, kezeléséhez.
- Event Log Readers: A csoport tagjai megnézhetik az Eseménynapló bejegyzéseit.
- IIS_IUSRS: lecseréli a korábbi IUSR_<gépnév> fiókot, azaz az anonim, webkiszolgálóhoz intézett kérések fiókjával egyenértékű, annak ellenére, hogy egy csoportról van szó.
- Performance log / Performance monitor users: a nevéből adódóan a Performance Monitor használatához kaphatnak (nem teljes körű) jogosultságot az e csoportba bekerülő felhasználók.

Tárolt hálózati nevek és jelszavak



3.17. ábra: *A jelszókezelő eszköz lényegesen komfortosabb lett*

A Windows Vista képes a hálózatban, valamint a weboldalakon használt jelszavaink tárolására. Ezt már a Windows XP-vel is megvalósíthattuk, de sokkal kevésbé komfortosan. A Vistával könnyedén előkészíthetjük a felhasználók számára például az intranetes szolgáltatások használatához szükséges belépési hitelesítő adatokat, és elmenthetjük ezeket.

Szükség szerint az esetleg tévesen bevitt hitelesítési információkat is törölhetjük, illetve teljes újdonságként a jelszavainkat el is menthetjük *.crd* kiterjesztéssel. A jelszavak tárolásának és beállításainak eléréséhez navigáljunk el a *Control Panel / User Accounts / Manage your network passwords* pontra.

A felhasználói fiókok felügyelete (UAC)

Egyértelműen belátható, hogy nemcsak a korábban említett rendszerszolgáltatások, hanem a rendszer interaktív felhasználói, azaz mi magunk is rendszeresen szükségtelenül magas jogosultsággal dolgoztunk a korábbi ügyfél operációs rendszereken. Ezért Vista esetén a Microsoft drasztikus változtatásokra szánta el magát ezen a területen is. Az új működési elv tömören: **mindenki standard felhasználó jogosultságú, senki sem rendszergazda, még akkor sem, ha annak látszik!** Ez az állítás elsőre bizonyára kissé meghökkentőnek tűnik, de a gyakorlatban működik, nézzük tehát lépésről lépésre a kiváltó okokat és a változásokat.

1. A régebbi rendszerekben a létrehozott felhasználói fiókok alapértelmezésként rendszergazdai jogosultságot kaptak, kezdve a telepítéskor létrehozott saját felhasználói fiókkal. Így a tapasztalatlan felhasználók kezében már a kezdetektől könnyen (ön)veszélyes fegyverré válhatott az operációs rendszer.
2. A Windows korábbi verzióival szerzett tapasztalatok azt mutatják, hogy a legtöbb olyan felhasználó, aki egyedül felügyeli számítógépét, mindenképpen rendszergazda-jogosultságú fiókkal használja azt, és nem sokat törődik a biztonsági figyelmeztetésekkel. Az ideális állapot természetesen az lenne, ha mindenki korlátozott felhasználóként lépne be a Windowsba, majd rendszerbeállítás módosításakor, vagy program telepítésekor átjelentkezne a rendszergazda fiókba, vagy a Run as… *(Futtatás mint...)* opciót használná. Az igazság azonban az, hogy jóval kényelmesebb eleve rendszergazdaként működtetni a rendszert, mert így szinte sosem fogunk ellenállásba ütközni.

3. Egy szigorú vállalati hálózatban is előfordulhat az, hogy egy ügyfélgépen jogosultságkezelési szempontból rosszul megírt, de kötelezően használt alkalmazás miatt muszáj a felhasználókat szükségtelenül magas szintű jogosultsággal ellátni, amely általában úgy zajlik, hogy a rendszergazda a helyi Administrators *(Rendszergazdák)* vagy a korábban említett, szintén túlságosan „erős" Kiemelt felhasználók *(Power Users)* csoportba beemeli a felhasználót.

Ezen helyzetek kiváltó oka egyrészt a tudatlanság, viszont másrészt a kényelem, amely ugyan szintén fontos szempont, de tudnunk kell azt is, hogy a rendszergazda-jogosultság teljes hozzáférést ad az operációs rendszerhez és a számítógép minden komponenséhez, lehetővé téve olyan módosításokat, amelyek a rendszert működésképtelenné tehetik, vagy kárt tehetnek más felhasználók adataiban. Sőt, az óvatlan használattal a kívülről érkező kártevők, vírusok, férgek, spyware-ek sem ütköznek túl sok akadályba – hiszen, amint bejutnak a gépre, rögtön rendszergazda-jogosultságot szerezhetnek. Valamint, üzemeltetőként azt a tényt is célszerű ismernünk, hogy a rendszereket érintő biztonsági incidensek közel 70%-a a belső hálózat felhasználóitól származik. Ezek ismeretében bizonyára el fogunk gondolkozni azon, hogy megéri-e az emelt szintű jogosultsági vakmerő használata.

A Vistában viszont nem kell sokat ezen gondolkoznunk, alapértelmezés szerint kész helyzet elé vagyunk állítva, amely talán kevésbé kényelmes, viszont annál hasznosabb. A kész helyzet szállítója az ún. User Account Control (UAC, *Felhasználói fiókok felügyelete),* amely egy összetett megoldás, ez a következő alfejezetek közül több is ennek a technológiának a részletezésével foglalkozik majd.

Ha például a mindennapos használat közben adunk hozzá felhasználókat, akkor azok immár csak a standard felhasználói jogokkal bírnak majd. Ha a telepítéskor elsőként létrejövő fiókot nézzük, az természetesen továbbra is rendszergazda-jogosultságú lesz, de neki is – mind minden a helyi rendszergazdacsoportba tartozó fióknak – csökkentett, standard felhasználó szintű környezetet tölt be a Windows, a rendszermódosításhoz szükséges jogokat külön kell kérnie.

Egy szó mint száz, alapesetben a jogosultságok túlzó kiosztása miatt kevesebbet kell aggódnunk, de mi a helyzet akkor, ha mégis szükség van rendszergazdaként működtetni a gépet. Mert ugyan az is fontos és kissé talán fordított előjelű (de nem veszélyes) változás, hogy számos olyan funkció vagy beállítás került be a standard felhasználók jogosultsági körébe, amelyekre korábban nem volt lehetőség, (ezt később bővebben is kifejtjük), de azért még mindig maradt rengeteg, amelyhez ennél több jogosultság szükséges.

Ha olyan műveletre kerül sor, amikor valóban hozzá kell nyúlni bizonyos rendszerbeállításokhoz, vagy olyan védett mappákba kell programot telepíteni, mint a *\Windows* vagy a *\Program Files*, a Vista interaktivitásra készteti a felhasználót, azaz egy úgynevezett „eleváló" promptot, jogosultság-jóváhagyó kérdést küld a felhasználónak. Azaz a standard felhasználónak külön engedélyeznie kell, mikor a rendszergazda jogaival élni szeretne. Ez lehetőséget biztosít a felhasználónak, hogy eldöntse, egy alkalmazás élhet-e ezekkel a jogokkal. Ez egyben azt is jelenti, hogy a felhasználó minden esetben információt kap arról, milyen alkalmazások indulnak el, amelyek rendszergazdai joggal futnak.

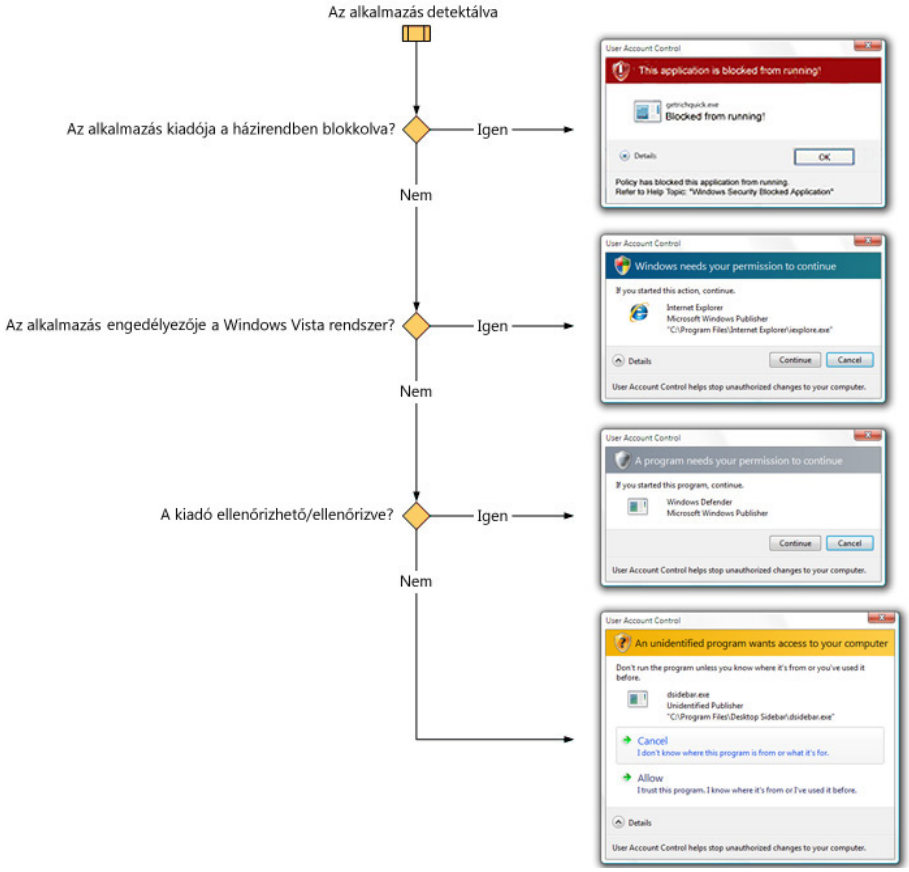
A technikai magyarázat lényege, hogy amikor egy felhasználó bejelentkezik, az UAC két biztonsági tokent hoz létre. Egy „normál" felhasználói tokent és egy olyan tokent, amely tartalmazza a rendszergazda jogokat. Az elindított folyamat akkor nem kapja meg az utóbbi jogokat, ha a felhasználó a folyamat indulásakor nem engedélyezi az UAC felületén keresztül. A létrejött „normál" felhasználói tokenben az alábbi különbségeket fedezhetjük fel – szemben a rendszergazdai tokennel (az ismeretlen fogalmakra később visszatérünk):

- Kilenc rendszergazda-szintű jog nincs benne.
- A felhasználó integritási szintje *Medium*, és nem *High*.
- Alkalmazódik rá egy alapesetben mindent tiltó SID.
- Megjelenhet számára az UAC engedélyező ablak *(consent.exe)*.
- Fájl- és regisztrációs adatbázis virtualizáció alkalmazódhat rá.

Az UAC különféle helyzeteknek megfelelően többfajta engedélyező ablakot jeleníthet meg. Ha az alkalmazás, vagy annak kiadója a biztonsági házirend szerint blokkolva van, egy piros fejléccel rendelkező figyelmeztető ablak jelenik meg, a program futtatása pedig nem lehetséges. Kékes-zöldes színű ablakot láthatunk, ha a jogosultsági szint emelését a Windows egyik beépített komponense kéri. Külső programok esetén szürke színkódú UAC-promptot kapunk, ha az állomány rendelkezik digitális aláírással, így az valószínűleg megbízható forrásból származik, figyelemfelkeltőbb, sárga színűt pedig, ha nem található aláírás – ez esetben csak akkor futtassuk az alkalmazást, ha ismerjük származási helyét és teljesen megbízunk abban.

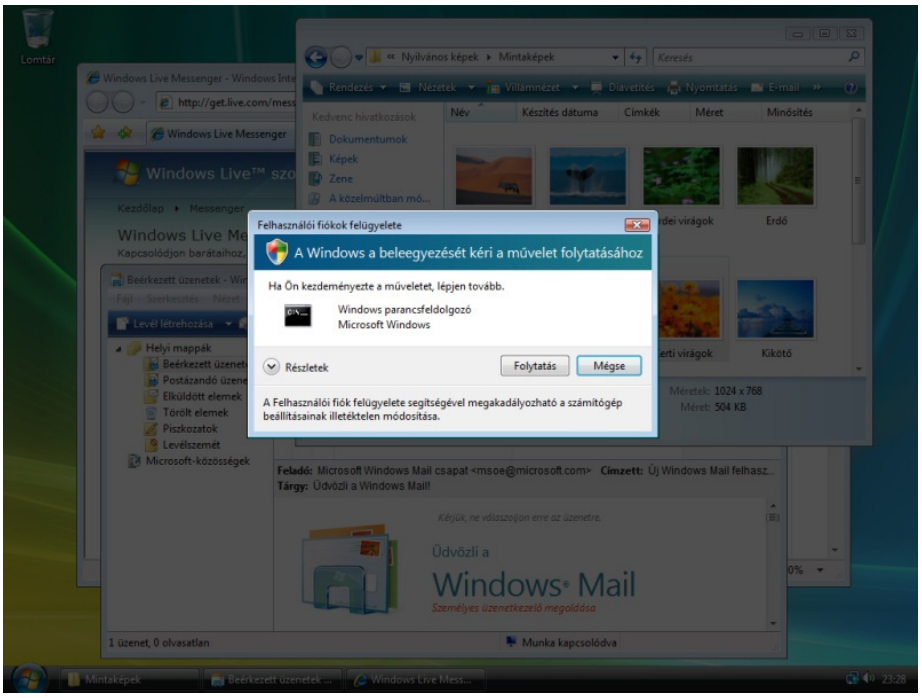
A User Account Control részletes beállítása a helyi biztonsági házirendből történhet. A finombeállítások között megadhatjuk például, hogy a figyelmeztető kérdés rendszergazda-jogosultságú felhasználó esetén csak egy igen/nem választási lehetőségből, vagy akár teljesen egy figyelmezetés nélkül történjen, vagy például azt is, hogy egy standard felhasználó esetén egyáltalán ne legyen lehetőség a név/jelszó páros megadására, hanem csak az elutasításra.

Történetesen még azt is beállíthatjuk, hogy az UAC a kérdőablak megjelenítésekor átkapcsoljon-e az úgynevezett *Secure Desktop* módba. A házirendből (és a *Control Panel / User Accounts* pont alól) akár ki is kapcsolhatjuk az UAC-t, de ez természetesen nem ajánlott.



3.18. ábra: *A különböző UAC-párbeszédablakok a kód ellenőrzésének folyamata szerint*

A Secure Desktop a felhasználó munkafolyamatában, de elszeparált asztalként jön létre, ráadásul csak a rendszer által írható, így a biztonsági asztalt semmilyen külső, a felhasználó asztalán futó folyamattal nem lehet befolyásolni. Ez szinte tökéletesen megbízhatóvá teszi a Secure Desktopon megjelenített ablakokat, vagyis biztosak lehetünk benne, hogy maga a rendszer és nem pedig egy vírus küldte a megtévesztő üzenetet.



3.19. ábra: *A Secure Desktop állapot*

Az alábbiakban azon események (nem teljes) listáját láthatjuk, amikor az UAC szolgáltatás közbelép:

- Alkalmazások telepítése és eltávolítása.
- Eszközmeghajtó programok telepítése és eltávolítása.
- ActiveX-vezérlők telepítése.
- Windows-frissítések telepítése.
- A Windows Update beállításainak módosítása.
- A Windows tűzfal beállításainak módosítása.
- A Felhasználói fiókok felügyelete (UAC) beállításainak módosítása.
- Felhasználói fiókok létrehozása és törlése.
- Felhasználói fiókok típusának megváltoztatása.
- A szülői felügyelet konfigurálása.
- A feladatütemező megnyitása.

- Rendszerfájlok biztonsági mentésből történő visszaállítása.
- Más felhasználó mappájának megnyitása vagy megváltoztatása.

A korlátozott jogkörben dolgozó felhasználók alapértelmezésként az UAC felügyelete alatt dolgoznak, mely esetükben a fenti felsorolásban szereplő műveleteknél nem egy egyszerű engedélyező ablakot jelenít meg, hanem egy rendszergazda jogosultságú felhasználó hitelesítő adatait kéri be (de – ahogyan korábban említettük – ez a működés a biztonsági házirendből megváltoztatható). Anélkül, hogy az UAC-cal találkoznának, a standard jogú felhasználók az alábbi műveleteket végezhetik el (szintén nem teljes a lista):

- Vezeték nélküli hálózat konfigurálása.
- Energiaellátási opciók változtatása.
- VPN-kapcsolatok konfigurálása.
- Nyomtató és egyéb eszközök hozzáadása (házirendből szabályozva).
- Windows Update használata.
- Windows Defender használata.
- Lemezdefragmentálás, Disk Cleanup futtatása.
- Időzónaváltás.
- Eseménynapló megtekintése (kivéve persze a Security naplót).

Ha egy program futása közben szükségtelenül generál szintemelést kérő párbeszédablakot, a Microsoft alkalmazáshibaként tekint az esetre, tehát (ha pl. az *Error Reporting*-szolgáltatás révén beérkezik), úgy kezeli a helyzetet, mintha a program hibásan működne. Ezzel magas prioritást kapnak az efféle problémák, tehát a fejlesztők is hamarabb reagálhatnak rá, ezért egyre biztosabbak lehetünk abban, hogy valóban csak akkor jelenik meg az UAC-prompt, amikor tényleg szükség van rá – feleslegesen nem bukkan fel.

A Vista további praktikus megoldásokkal is segíti az UAC-prompt esetlegesen indokolatlanul zavaró és állandó megjelenését:

- Lehetővé teszi a rendszergazdáknak, hogy meghatározzák, a nem rendszergazda-jogú felhasználók milyen meghajtóprogramokat, eszközöket, ActiveX-vezérlőket telepíthetnek. Így, adott esetben, a nem rendszergazdai jogú felhasználók is telepíthetnek nyomtatókat, VPN-szoftvereket stb.

- Alap hálózati konfigurációk elvégzéséhez a felhasználót elegendő hozzáadni a Network Configurations Operators csoporthoz. Ennek a csoportnak joga van az IP-címek megváltoztatásához, DNS-cache ürítéséhez stb., vagyis a nélkül végezhetők el ezek a feladatok, hogy a felhasználó az Administrators *(Rendszergazda)* csoporttagságra lenne szükségük.
- Az UAC-fájlrendszer és regisztrációs adatbázis virtualizációja és a beépített alkalmazás kompatibilitási sémák segítségével sok rendszergazdai jogokat igénylő alkalmazás futtatását teszi lehetővé, számos problémán segít (a részleteket lásd a következő alfejezetben).

Az UAC tervezésekor felállított programozási irányelvek kimondják, hogy a felhasználónak mindig előre tudnia kell róla, ha a művelet jogosultsági szintemelést követel. Ezt a gombokon és hivatkozások mellett elhelyezett kis pajzsok ( ) jelzik, egyértelművé téve, mely műveletekhez szükséges emelt szintű hozzáférés.

A fiókváltozások és a User Account Control (UAC)
Ebben az előadásban a Vista felhasználói fiókjaival és csoportjaival, illetve a talán legfontosabb a biztonságot érintő változással, az UAC-lal kapcsolatos részleteket tárjuk fel.
Fájlnév: I-3-3b-Fiokok-es-UAC.avi

Fájl- és registryvirtualizáció

A User Account Control egy másik fontos feladata a szoftverkörnyezet virtualizálása azon alkalmazások számára, melyek nem lettek felkészítve a többfelhasználós rendszerekre, vagy nem kezelik jól a jogosultságokat. Egyelőre meglehetősen sok olyan program létezik, amely vagy nem veszi figyelembe, hogy többfelhasználós környezetben működik, vagy egyszerűen nem is hajlandó futni, csak és kizárólag rendszergazdai jogosultságokkal. Az UAC ezért detektálja az alkalmazás fájlrendszerbe és a registrybe való írási kéréseit, és ennek megfelelően – minden felhasználói fiókban egyéni – virtuális környezetet (úgynevezett „homokozót") hoz létre a programnak.

A rendszergazda-jogosultságot megkövetelő programok így tulajdonképpen „azt hiszik", hogy tudnak írni a pl. a *\Windows*, vagy a *\Program Files* mappákba, esetleg a rendszerleíró adatbázis kritikus részeibe is, ám valójában egy, a számukra létrehozott virtuális valóságban működnek – immáron gond nélkül. A virtualizált mappákat a védett rendszerkönyvtárak tallózásakor megjelenő *Compatibility Files* gombra kattintva nyithatjuk meg, ezek fizikai helye a felhasználó profilkönyvtárában található az alábbi útvonalon: *\Users\<felhasználónév>\AppData\Local\VirtualStore*.

A regisztrációs adatbázist érintő írási műveletek pedig a *HKCU\Software\Classes\VirtualStore* kulcs alá kerülnek.

Mint az útvonalakból is látható, mind a két hely a felhasználó profilja alatt helyezkedik el, így a felhasználónak van rá írási joga. Ha felhasználónkénti szabály nem definiálja másképp, az olvasás elsőként a globális helyről történik. A fájlrendszer virtualizációja egy filter driver *(luafv.sys)* segítségével valósul meg, a regisztrációs adatbázisé pedig beépítetten.

A fájl- és regisztrációs adatbázis virtualizáció meggátolja az írásokat a nem adminisztrátori jogú (nem elevált) folyamatok számára, de csak az alábbi helyekre:

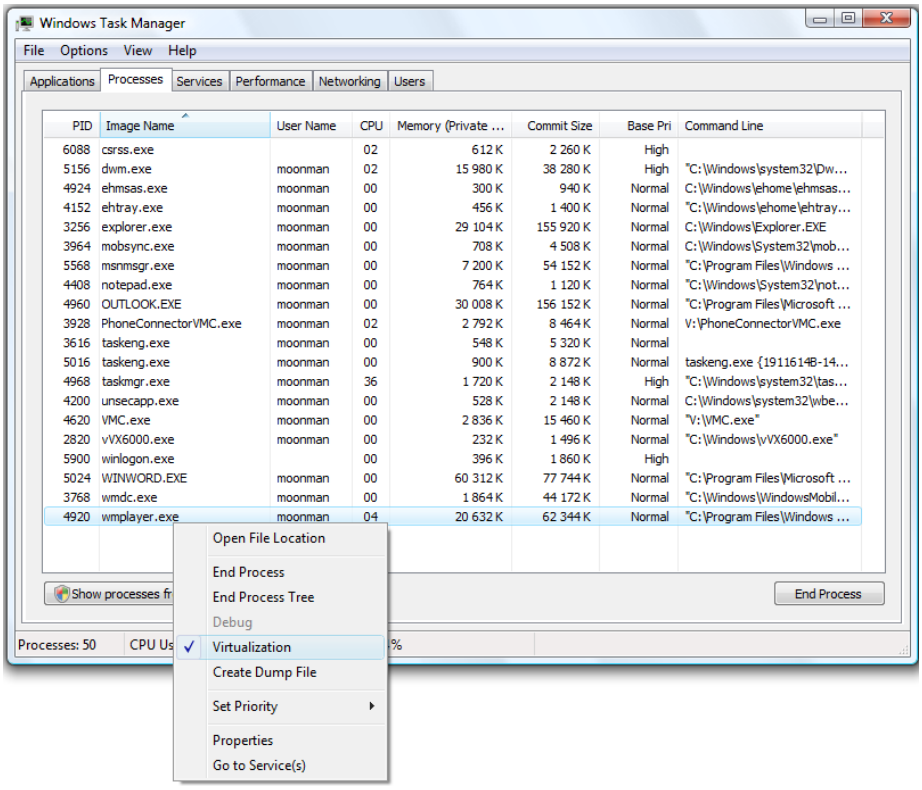
- *\Program Files* és az almappái.
- *\Program Files* (x86) 64-bites rendszereken.
- *\Windows* és almappái, beleértve a System32-t is.
- *\Users\%AllUsersProfile% \ProgramData*
- *HKLM\Software*

Az alábbi objektumok azonban soha sem kerülnek virtualizálásra:

- Vista alkalmazások.
- Futtatható állományok, mint az *.EXE, .BAT, .VBS* és *.SCR*. A további fájlrendszeri kivételek a *HKLM\System\CurrentControlSet\Services\Luafv\Parameters\ExcludedExtensionsAdd* kulcsban adhatóak meg.
- 64-bites alkalmazások és folyamatok.
- Azok az alkalmazások, amelyeknél gyárilag definiálva van, hogy nem virtualizáltan futtatandók (mint az összes Vista-komponens).
- Folyamatok és alkalmazások, amelyek rendszergazdai jogokkal futnak.
- Kernelmódú alkalmazások.
- Műveletek, amelyek nem interaktív bejelentkezésből származnak (pl.: fájlmegosztáson keresztüli elérés).
- Alkalmazások amelyek a regisztrációs adatbázisban a *Dont_Virtualize* jelzéssel vannak megjelölve.

Az utolsó ponthoz tartozó plusz információ: a *reg.exe* segítségével láthatjuk a három új *registry flag*-et a *HKLM\Software* kulcs alatt, ezek a következőek: *DONT_VIRTUALIZE, DONT_SILENT_FAIL, RECURSE_FLAG*

Az egyes alkalmazások virtualizációját a Task Managerből *(Feladatkezelő)* akár saját magunk is engedélyezhetjük (vagy tilthatjuk le). Ezt a műveletet ajánlott csak szükség esetén elvégezni, kiváltképp a Windows beépített folyamatainál, mert a téves konfiguráció akár a rendszer instabil működéséhez is vezethet.



3.20. ábra: *A feladatkezelőben a „közönséges" processzeket egyszerűen virtualizálhatjuk*

Fájl- és registryvirtualizáció
Ebben a screencastban több példát is hozunk az UAC „melléktermékeként" megjelent fájl- és registryvirtualizációra, először egy dedikált alkalmazás majd a cmd.exe segítségével.
Fájlnév: I-3-3c-Fajl-es-registry-virtualizacio.avi

Mandatory Integrity Control (MIC)

A következőkben bemutatott kerülő védelmi eljárás még egy, az 1970-es években született elgondoláson alapszik, megvalósítására azonban csak napjainkban került sor. Míg a fájlrendszer-jogosultságok könnyen kezelhető és hatékony védelmet nyújtanak az illetéktelen hozzáférésektől, a technológia rendelkezik némi korlátoltsággal. Hiába védjük másoktól a fájlokat, ha magát a tulajdonost is viszonylag könnyen rávehetjük, hogy lefuttasson egy-egy parancsot – természetesen adminisztrátori jogokkal. A MIC alapelgondolása a következő: a csökkentett megbízhatósági szinten dolgozó alanyok nem módosíthatnak magasabb szinten lévő objektumokat, a magasabb szinten létező objektumok pedig nem kényszeríthetők, hogy megbízzanak alacsonyabb szintről érkező utasításokban vagy adatokban. A kulcsszó itt a „megbízhatóság", a MIC pedig ezt az információáramlási szabályt valósítja meg a Windows Vistában.

Amikor bejelentkezünk, a Windows egy adott integritási azonosítót rendel a felhasználónkhoz. Ez az azonosító tartalmazza mindazt az információt, amiből a rendszer megállapítja, hogy mely területekhez van hozzáférésünk, és melyekhez nincs. Nem csak a felhasználók, de a védeni kívánt rendszerobjektumok, úgy mint fájlok, mappák, adatcsatornák, folyamatok (processzek), folyamatszálak (threadek), az ablakkezelő, registrykulcsok, szolgáltatások, nyomtatók, megosztások, ütemezett feladatok stb. is kapnak egy-egy saját szintazonosítót. Ezek az azonosítók a System Access Control Listben (SACL) tárolódnak.

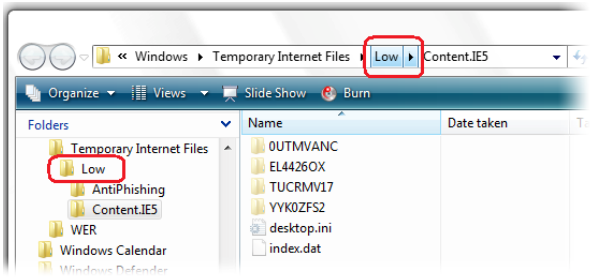
Amikor a felhasználó egy műveletet végez, a Windows még azelőtt, hogy a fájlrendszer-jogosultságokat vizsgálná, összehasonlítja a felhasználó integritásszintjét a műveletben részt vevő objektumokéval. Ha a felhasználó szintje a domináns – vagyis az objektuméval megegyező vagy magasabb – a Windows engedélyezi a feladat végrehajtását – feltéve, hogy fájlrendszerszinten is megvan hozzá a kellő engedélye. Ha a felhasználó alacsonyabb szintről próbál manipulálni egy objektumot, a Windows nem engedélyezi a hozzáférést, függetlenül attól, hogy magához a fájlhoz, registrykulcshoz, vagy egyéb komponenshez különben meglenne a hozzáférése. Láthatjuk tehát, hogy az integritásszintek minden esetben a fájlrendszer-jogosultságok, vagyis az ACL fölött állnak.

A Windows Vistában négy integritásszintet definiáltak a fejlesztők: Low *(alacsony)*, Medium *(közepes),* High *(magas)* és a System *(rendszer).* Az egyszerű felhasználók közepes, a (valódi) rendszergazda jogosultságúak pedig magas szinten tevékenykednek. A felhasználó által indított folyamatok vagy az általa létrehozott objektumok öröklik a felhasználó integritásszintjét, a rendszerszolgáltatások a „rendszer" szintre kapnak belépőt. Ha valamilyen okból kifolyólag egy objektum nem kap integritásszint-jelölést, az operációs rendszer automatikusan közepes szintre sorolja be, ezzel megakadályozva, hogy az alacsony szinten futó folyamatok hozzáférhessenek a nem jelölt ob-

jektumokhoz. Az operációs rendszer fájljai alapértelmezésként nem jelöltek, így közepes szinten tartózkodnak, valamint természetesen alkalmazódnak rájuk a megfelelő fájlrendszer-jogosultsági beállítások (ACL) is. Az egyes objektumok integritási szintjei a SACL-ekben tárolódnak és az ellenőrzésük minden esetben a DACL ellenőrzések előtt történik.

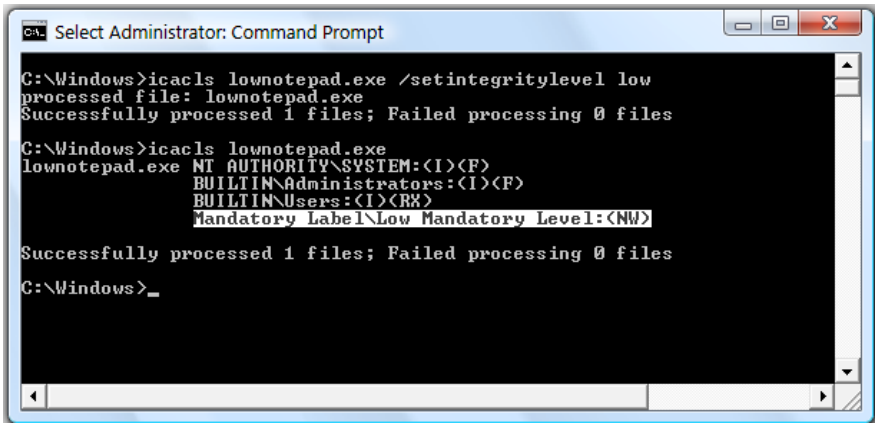
Szint	SID	Hex érték	Használati példák
Low	S-1-16-4096	1000	Védett módú Internet Explorer
Medium	S-1-16-8192	2000	Hitelesített felhasználók/ Nem elevált
High	S-1-16-12288	3000	Rendszergazdák/ Elevált jogok
System	S-1-16-16384	4000	Helyi rendszer

Hogy miért szükséges ez a bűvészkedés a jogosultsági szintekkel? Képzeljük el a következő helyzetet: kapunk egy e-mailt egy csatolt fájllal. Amikor lementjük a fájlt, az rögtön alacsony integritásszintre kerül, mivel az internetről (azaz egy nem megbízható helyről) érkezett. Ezért aztán bármi legyen is a fájl tartalma, amikor lefuttatjuk, semmi különös nem történhet, mivel a fentiek alapján egy alacsony szinten futó folyamat nem férhet hozzá a felhasználó magas, vagy nem jelölt, így közepes szinten lévő adataihoz.



Az Internet Explorer védett módja a megbízhatósági szintek köré épült, és – mivel a böngésző alapértelmezésként alacsony *(Low IL)* integritásszinten fut – biztosak lehetünk benne, hogy az Internet Exploreren keresztül hozzájárulásunk nélkül nem települhet többé a rendszerre semmilyen ártó kód. Ezen túlmenően, mivel a Windows munkaasztal közepes szintre van besorolva, a böngészőben esetlegesen lefutó ActiveX-vezérlő sem küldhet többé olyan megtévesztő üzeneteket az asztalra, miszerint vírustámadás áldozatai lettünk, és azonnali hatállyal töltsünk le egy bizonyos programot – ami valójában maga a vírus.

Az NTFS fájlrendszer-jogosultságokhoz hasonlóan – bizonyos korlátok között – az integritásszinteket is az *icacls* paranccsal kezelhetjük. Két korlátozás létezik: az objektumokat nem helyezhetjük át a System, illetve az Untrusted szintekre. Az integritásszintek változtatásához használjuk a */setintegritylevel* kapcsolót, azonban bánjunk óvatosan ezzel az eszközzel és csak szükség esetén módosítsuk ezt az objektumtulajdonságot!



3.21. ábra: *Sikeres integritási szint beállítás parancssorból*

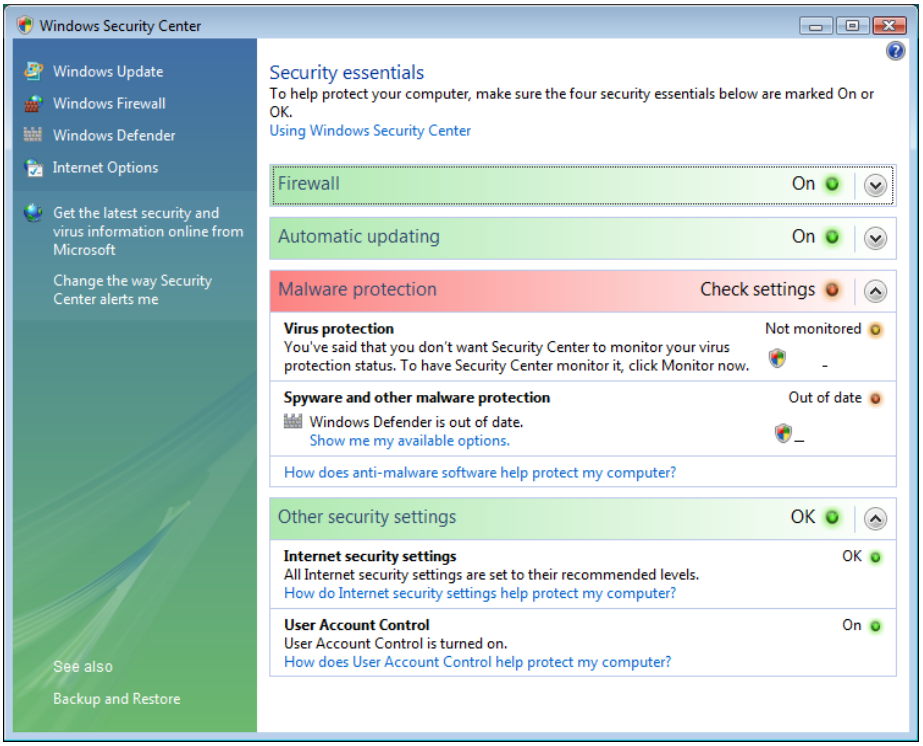
A biztonsági rendszer összetevői

A következő alfejezetben a Vista olyan a biztonságához kapcsolódó komponenseinek lehetőségeit és alkalmazási területeit foglaljuk össze, amelyekkel már sűrűbben találkozunk a felszínen is. Természetesen itt elsősorban az üzemeltetők jelentik a hatókört, akiknek akár a napi feladatai közé is tartozhat a Security Center jelzéseinek értelmezése, az Internet Explorer 7-es változatának precíz beállítása és új lehetőségeinek ismerete. De a Windows Defender, az EFS, a BitLocker vagy akár a Vista új tűzfalának mélyreható megismerését sem érdemes kihagyni – főképp, ha a feladataink közé tartozik az ügyfélszámítógépek biztonságos működtetése.

A Security Center

A Windows Vistába beépített Security Center *(Biztonsági központ)* sokban hasonlít a korábbi verzióhoz, azonban el is tér attól. A tűzfal, az Automatikus frissítések ügyfél és a vírusirtó állapotának állandó vizsgálata megmaradt, viszont bekerült a monitorozandó komponensek közé az immár integrált Windows Defender (lásd később) a frissítési opcióval együtt.

Az UAC működése szintén nyomon követhető a Security Centerben, valamint egy teljesen új szakasszal is bővültek a lehetőségeink, azaz az Internet Explorer legfontosabb biztonsági beállításait is ellenőrzi a rendszer, és jelzést is kapunk, ha ezek állapotában negatív változás következik be (a megfigyelt paraméterekről további részleteket olvashatunk kicsit később, a „Biztonsági beállítások automatikus felügyelete" szakaszban).



3.22. ábra: *A Windows Vista Security Center tartalma bővült*

A Windows XP és a Windows Vista Biztonsági központja *(Security Center)*
Ennek az előadásnak a témája a két operációs rendszer Biztonsági központjának bemutatása.
Fájlnév: I-3-4a-Security-Centers.avi

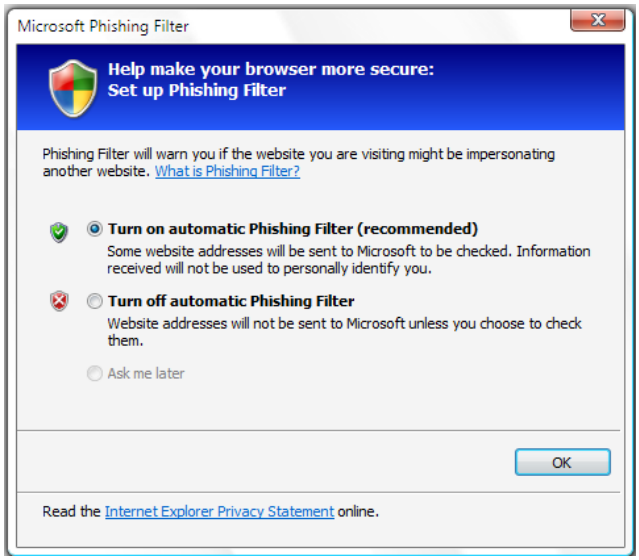
Az Internet Explorer 7 biztonsági újításai

A korábbi ügyfél operációs rendszerekben, és különösen a Windows XP Service Pack 2-ben már jelentős változások voltak tapasztalhatóak a Microsoft böngészőprogramjával kapcsolatban – elsősorban a biztonságosságot tekintve. Lehetővé vált pl. a felugró ablakok blokkolása, valamint módosult (lényegesen szigorúbb lett) az ActiveX vezérlők kezelése is, és megjelent a figyelemfelkeltő biztonsági sáv is.

A Windows Vistába már a böngésző következő, 7.0-s verziója került, mely jó pár régóta várt funkciót hozott. Először is lehetővé vált a füles/lapos navigálás, valamint egyéb olyan biztonsági megoldások is beépültek, mint például az opt-in (engedélyezendő) ActiveX-kezelés, a továbbfejlesztett bővítménykezelő, az adathalászat *(phishing)* elleni védelem, valamint a védett módú böngészés *(Protected Mode)*. A tanúsítványkezelés és a haladó beállítások területén is tapasztalhatunk pozitív változásokat.

Ugyan a Windows XP-re és a Windows Server 2003-ra is letölthető az Internet Explorer 7-es változata, de ezek mégsem egyeznek meg mindenben a Vistába integrált változattal. A különbségek az eltérő biztonsági háttérből adódnak: a Vistánál használt IE7 olyan lehetőségeket is képes alkalmazni, amelyek az UAC jelenlétének a következményei, pl. az ún. védett mód (lásd később).

Phishing filter



3.23. ábra: *Az IE7 első indításakor rögtön bekapcsolhatjuk az adathalászat-szűrőt*

Napjaink egyik legelterjedtebb online bűnözési formája, az úgynevezett adathalászat, a phishing. Ennek az a lényege, hogy például olyan pénzügyi szolgáltatásnak álcázott webhelyre csalják a felhasználót, mely külsőre szinte pontosan megegyezik egy-egy bank vagy pénzintézet honlapjával. Itt aztán a felhasználótól olyan személyes adatokat kérnek be, melyek felhasználásával hozzáférhetnek bankszámlájához és egyéb személyes értékeihez. A phishing elleni védelem központi szerepet kapott az Internet Explorer 7-ben, a böngésző első indításakor máris lehetőségünk van a szűrő bekapcsolására és a beállítások testreszabására. Az IE7 phishing filtere rendszeresen frissülő online adatbázison és egy intelligens szűrőn alapul, mely tipikus jellemzők után kutatva megvizsgálja a weblap eredetiségét és megbízhatóságát. Ha e vizsgálat során nem találja megfelelőnek az adott oldalt, akkor ezt szembetűnően jelzi a felhasználónak.

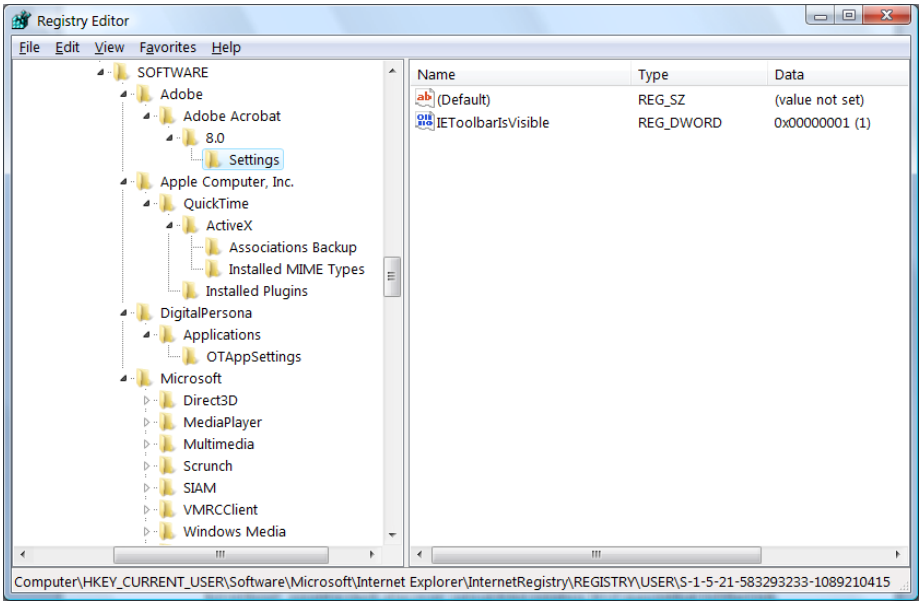
Védett mód

Az előző részben ismertetett User Account Control nemcsak a figyelmeztető ablakok küldésével próbálja kordában tartani a felhasználókat, de neki köszönhetjük, hogy az Internet Explorer 7 képes úgynevezett védett módban *(Protected mode)* futni – de csak a Vistán, az XP-re telepített IE7 nem ismeri ezt a fajta működést.

Ha a védett mód engedélyezve van, az IE7 nagyon alacsony integritási szinten *(Low IL)* dolgozik, amely számos biztonsági korlátot jelent a működésben. Ezek közül az egyik az, hogy a rendszer biztonsági alapbeállításainak megváltoztatása vagy egy emelt szintű jogosultság nélkül egy website nem képes semmilyen módon egy alkalmazást telepíteni a böngészőn keresztül. Ez azért van, mert az alacsony integritási szintnek köszönhetően a böngésző a fájlrendszerbe, illetve a registrybe nem írhat automatikusan. Mivel a különböző integritási szinten lévő processzek közötti kommunikáció szintén erősen limitálva van, a kényszerűen hasonlóan alacsony szinten működő ActiveX-vezérlők és az extra eszköztárak sem képesek hozzáférni semmilyen fontos rendszerelemhez.

Ezen kívül a Vista egy speciális virtuális mappát is előkészít az IE7 számára, az olyan fájlok tárolásához, amelyeket a böngésző menetközben egyébként a számára tiltott helyekre mentene el. Ez a mappa szokásos gyorsítótáron belül helyezkedik el *(Temporary Internet Files\Low)*, és ide és csak ide képes egy alacsony integritási szinttel rendelkező folyamat írni. Gyakorlatilag ez a korábban ismertetett fájl- és registryvirtualizáció elve alapján működik, csendben a háttérben, sikeresen megtévesztve bővítményeket, vagy a bármit, amely az IE7 alatt tevékenykedik.

A teljesség kedvéért említsük meg, hogy a rendszerleíró adatbázist érintő írási próbálkozások ugyanezzel a módszerrel, ugyanígy végzik, egy – szintén – elkülönített területen *(HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\REGISTRY\USER\{a_user_SIDje}\Software)*.



3.24. ábra: *A bővítmények „homokozója” a registry elkülönített részében*

De mi történik, ha az IE7 mégis ki akarja „olvasni” ezt az elkülönített, virtualizált tartalmat, azaz pl. egy rendszergazda szeretne egy ActiveX-vezérlőt telepíteni? Egy ún. broker processz beavatkozik, azaz megerősítést kér a folytatás előtt, és jön az ismerős UAC-prompt és a felhasználói interaktivitás.

A színfalak mögött a Vista további mappákat is létrehoz a védett módú működés kiszolgálása céljából, azaz a böngésző rendszeres használatával a következő, szintén csak alacsony integritási szinten lévő mappákat tölthetjük meg fájlokkal, a szokásos böngésző mappák helyett:

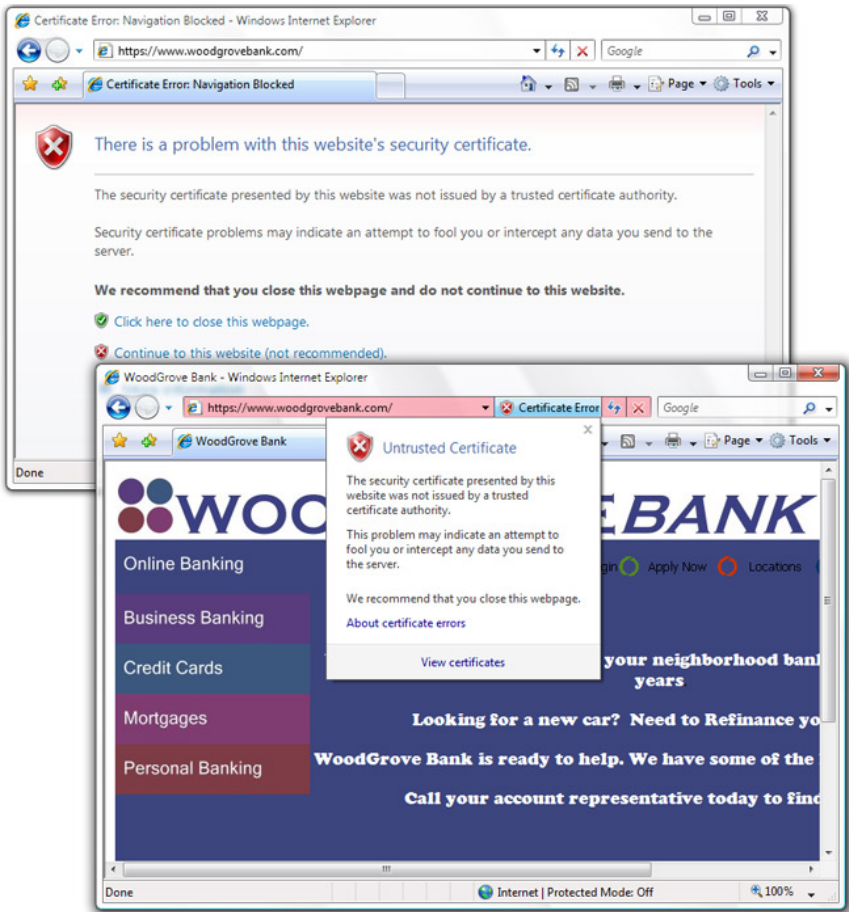
- **Temp**: %LocalAppData%\Temp\Low
- **Cookies**: %AppData%\Microsoft\Windows\Cookies\Low
- **History:** %LocalAppData%\Microsoft\Windows\History\Low

A védett mód alapértelmezés szerint be van kapcsolva az Internet, Helyi intranet *(Local intranet)* és Tiltott helyek *(Restricted sites)* zónákban (a Megbízható helyek *(Trusted sites)* zónában tehát nem), a bekapcsolt állapotot pedig egy, az állapotsorban látható ikon jelzi.

A védett mód alapértelmezésként aktív, kikapcsolása – hacsak nem abszolút megbízható helyen, például céges intraneten böngészünk – nem ajánlott, már csak azért sem, mert ekkor az IE automatikusan a közepes integritási szintre „kapaszkodik fel”.

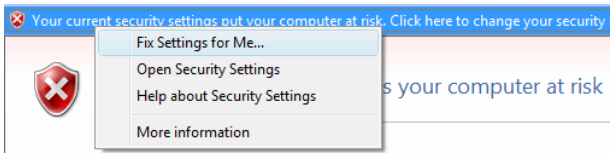
Tanúsítvány-ellenőrzés

Az érvénytelen tanúsítvánnyal rendelkező oldalak meglátogatásakor eddig is kaptunk figyelmeztetést, most azonban olyan hangsúlyos lett a biztonsági riasztás, hogy az a kezdő felhasználók figyelmét sem kerülheti el. A megbízható, erős titkosítást használó oldalak címe mellett egy lakat ikon jelzi a biztonságos kapcsolatot, a veszélyesnek minősített oldalak címsora pedig pirosra változik. Az érvénytelen, vagy lejárt érvényességi idővel rendelkező tanúsítványt használó weblapok továbbra is megtekinthetők, előtte azonban a felhasználónak nyugtáznia kell, hogy megértette a kockázati tényezőket és saját felelősségére lép be az oldalra.

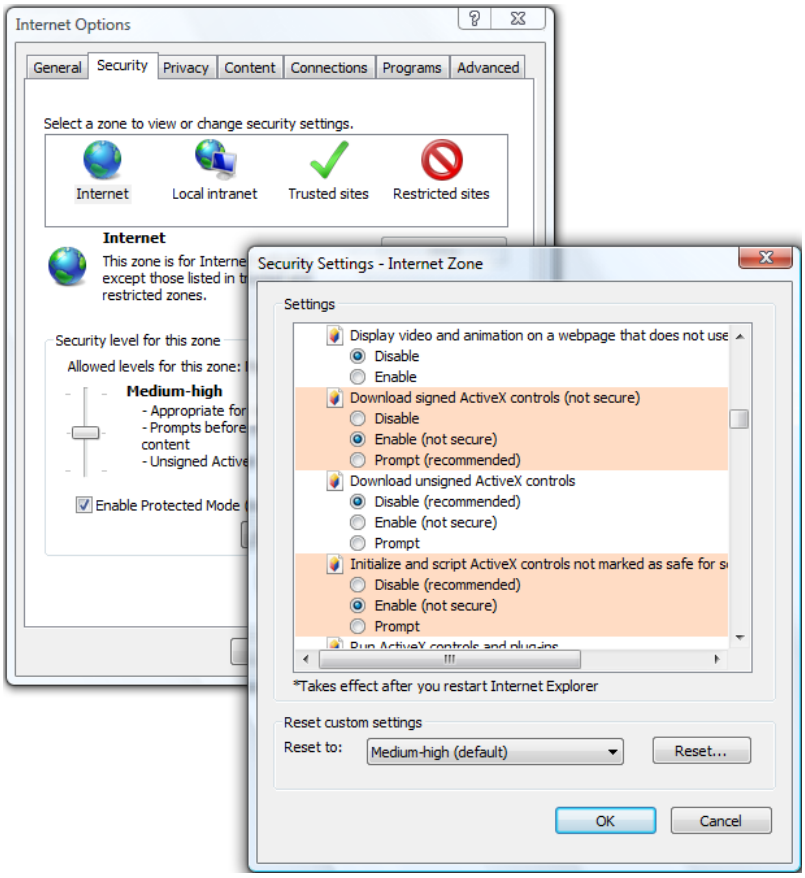


3.25. ábra: *A figyelmeztetés nyilvánvaló: ez a tanúsítvány nem megfelelő*

Biztonsági beállítások automatikus felügyelete



Az Internet Explorer 7 képes detektálni, ha az adott zónának megfelelő biztonsági beállítások eltérnek az alapértelmezett szinttől és veszélyesek lehetnek a böngészésre nézve. A biztonsági sávra kattintva lehetőségünk van a problémás beállítások automatikus korrigálását kérni, vagy a konfigurációs panelt megnyitva kézzel módosítani azokat.



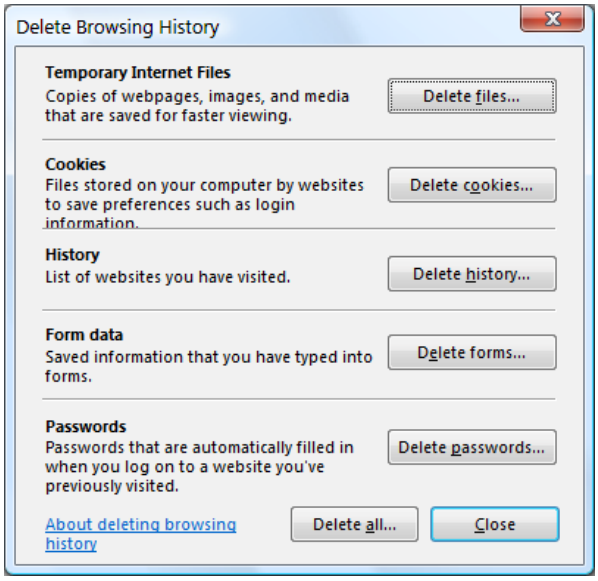
3.26. ábra: *A zóna biztonsági opciók között kiemelve látjuk az igazán fontosakat*

Ha a manuális módszer mellett döntünk, segítségünkre lehet, hogy az Internet Explorer piros színnel megjelöli számunkra a veszélyesnek ítélt beállításokat. A zónabeállítások között olyan újdonságokat találunk, mint a felbukkanó szkriptelt ablakok tiltása, a státuszsor weboldal általi frissítésének letiltása, valamint immár minden egyes ablaknak kötelező jelleggel látszik a cím- (URL) és állapotsora. Ezekre a korlátozásokra szintén az egyre terjedő adathalász-támadások kivédése miatt van szükség.

Haladó lehetőségek és beállítások — egyszerű problémamegoldás

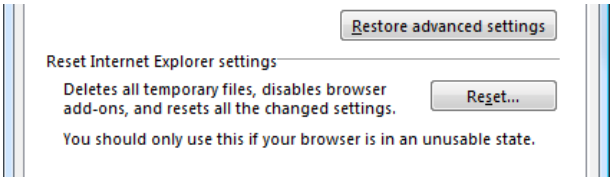
Ha tallózzuk a Start menüt, az *Accessories \ System Tools (Kellékek/Rendszereszközök)* programcsoportban rátalálhatunk egy speciális IE-változatra, amelyet Internet Explorer (No Add-ons) névvel láttak el. Ezzel az ikonnal egy teljesen csupasz, bővítmények és extra eszköztárak nélküli böngészőt indíthatunk el, azaz az esetleg, már jó alaposan beépült rosszindulatú vagy hibás működésű bővítmények használata kikerülhető. Ezt a problémamegoldáshoz nagyon hasznos üzemmódot egyébként elérhetjük a parancssorból is, a következő paranccsal: *iexplore -extoff*.

A biztonság fokozója az a speciális, az Internet Options\General *(Internet-beállítások/Általános)* fülről elérhető panel is, amelyben egy menetben törölhetjük az IE gyorsítótárát, a komplett előzménylistát, a sütiket, a különböző űrlapokba beírt és eltárolt adatokat, valamint az internetezés során itt-ott megadott jelszavakat.



3.27. ábra: *Érzékeny adatok egyszerű törlése*

Végül, de nem utolsósorban említsünk meg még két szintén haladó opciót, amelyek az Internet Options\ Advanced *(Internetbeállítások/Speciális)* fülön találhatóak, a panel alján a kiemelt opciók között Az egyikkel (Restore advanced settings – *Speciális beállítások visszaállítása)* könnyedén visszaállítható az összes haladó beállítás, amely szép számban, ugyanezen a panelen találhatóak. A másikkal viszont az egész Internet Explorert totális alaphelyzetbe hozhatjuk (Reset Internet Explorer Settings – *Alaphelyzet),* amely bizonyos esetekben igencsak hasznos és gyors megoldásnak bizonyulhat.



3.28. ábra: *Az IE7 biztonsági opcióinak alaphelyzetbe állítása egyszerű*

Az Internet Explorer 7.0 biztonsággal kapcsolatos újdonságai
Ebben az előadásban online példákkal mutatjuk be az itt felsorolt újdonságokat és változásokat az Internet Explorer 7-tel kapcsolatban.
Fájlnév: I-3-4b-IE7-biztonsag.avi

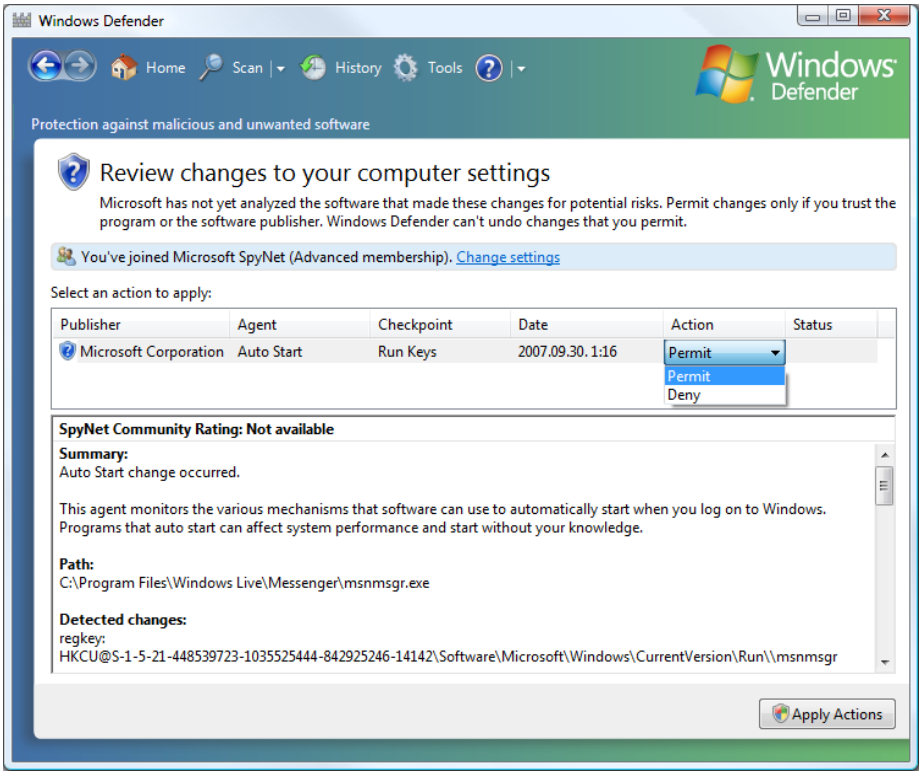
A Windows Defender

A Microsoft eredetileg a Windows XP-hez kezdte fejleszteni „Microsoft Anti-Spyware" néven kémprogram és trójai-figyelő alkalmazását, melynek végleges verziója a Windows Defender nevet kapta, és végül a Windows Vistába is be lett építve.

A szolgáltatásként futó Defender alapértelmezésként engedélyezve van, és az automatikus, ütemezett gyorskeresés is be van kapcsolva. Az alkalmazás kártevő-adatbázisa az internetről a Windows Update szolgáltatás segítségével folyamatosan frissül, de a definíciós fájlok igény szerint akár manuálisan is letölthetők és telepíthetők.

A Windows Defender XP-re telepíthető változata a következő webcímről tölthető le: http://www.microsoft.com/windowsdefender.
A legfrissebb szignatúra fájlok pedig a következő Microsoft tudásbáziscikken keresztül érhetők el: http://support.microsoft.com/?kbid=923159)

A Windows Defender az idő nagy részében a háttérben, a felhasználó megzavarása nélkül fut, jelenlétére csak akkor figyelhetünk fel, ha valamilyen beavatkozás szükséges – ekkor a tálca értesítési területéről egy buboréküzenetet jelenít meg, melyben ismerteti a teendőket.



3.29. ábra: *Nemcsak véd a kémprogramok ellen, hanem a rendszerindítást is befolyásolhatja a Windows Defender*

Az ismert kártevők lefülelésén kívül a Defender valóban átfogó védelmet nyújt a Windows rendszer egészének, így képes a következő eseményeket is detektálni:

- automatikusan induló programok listájának módosulása;
- rendszerkonfiguráció változása;
- Internet Explorer bővítmények telepítése;
- Internet Explorer biztonsági beállítások módosulása;
- szolgáltatások és eszközmeghajtók telepítése, valamint azok konfigurációjának változása;

- alkalmazás-regisztráció (Registry módosulása);
- Windows-bővítmények telepítése.

A Windows Defender része a Software Explorer, mellyel megtekinthetjük a rendszerrel automatikusan induló és az éppen futó alkalmazások biztonsági besorolását, valamint letilthatjuk a nem kívánt startup-programokat. Ha hozzá akarunk járulni a Windows Defender fejlesztéséhez, saját vizsgálat közben született eredményeinket is közzé tehetjük, ha csatlakozunk a Microsoft SpyNet programhoz. A belépés kétszintű, Basic, illetve Advanced tagságot is beállíthatunk. Míg a Basic esetén a Defender csak alapvető információkat küld a Microsoftnak a gépünkön esetlegesen észlelt spyware-ekről, az Advanced tagságot választva minden beállításunkról értesíthetjük a fejlesztőket, például a még be nem sorolt, de általunk biztonságosnak ítélt alkalmazások lenyomatait is feltölti a program – ezzel segítve az adatbázis tökéletesítését.

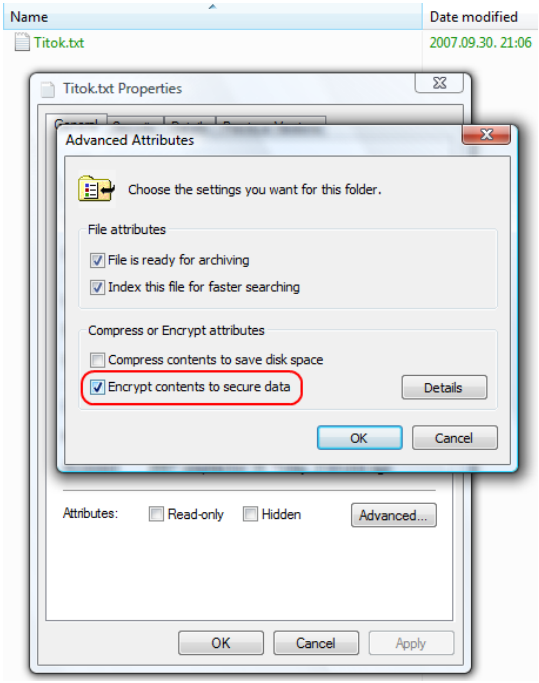
A titkosított fájlrendszer: az EFS

A Windows 2000 óta elérhető titkosított fájlrendszer (EFS = Encrypting File System) az NTFS-fájlrendszer egyik alapszolgáltatása. Segítségével transzparens módon titkosíthatjuk fájljainkat, így azokat a tulajdonos felhasználó a saját profiljába bejelentkezve a szokásos módon elérheti, de a háttértároló tartalma más számítógépbe helyezve – vagy más számítógépről hálózaton keresztül tallózva nem hozzáférhető.

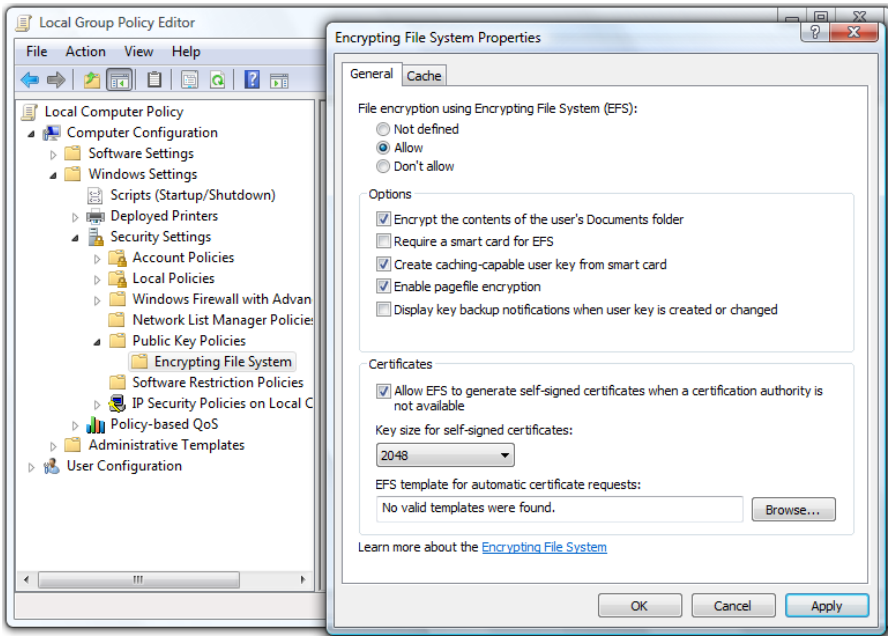
Az EFS-titkosítás érvényesítéséhez egy-egy mappára vagy fájlra mindössze meg kell nyitnunk az objektum tulajdonságlapját, majd az *Advanced* gombra kattintva bejelölnünk az *Encrypt contents to secure data* négyzetet. A titkosított állományok színe a Windows Explorerben alapértelmezésként zöldre változik.

Az egyes fájlokon, vagy teljes mappákon túl a Windows Vista már a lapozófájl titkosítását is lehetővé teszi. Erre azért lehet szükség, mert a lapozófájlban még a rendszer leállítása után is maradhatnak bizalmas adatok, melyek külső eszközökkel kinyerhetők.

Az EFS-sel titkosított adatok visszafejtésére jelenleg nincs lehetőség, hacsak nem rendelkezünk a titkosításhoz használt tanúsítvánnyal. Ezt a tanúsítványt – a titkosítást végző felhasználó profiljába bejelentkezve – a tanúsítványtárból bármikor kiexportálhatjuk, EFS használata esetén pedig erősen ajánlott biztonsági másolatot is tartani belőle arra az esetre, ha az operációs rendszer nem indítható.

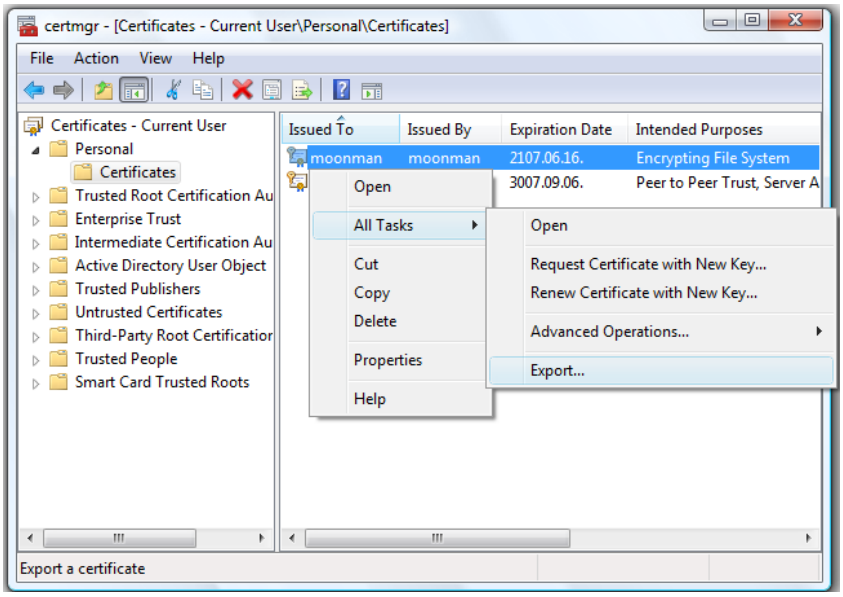


3.30. ábra: *A titkosítás bekapcsolása*



3.31. ábra: *Az EFS házirend-beállítások mennyisége alaposan megnőtt*

Az EFS-tanúsítványt a Certificate Managerből exportálhatjuk ki, melyet a *certmgr.msc* paranccsal indíthatunk. A Personal *(Személyes)* tanúsítványok között jelöljük ki azt, amelynek használati cél mezőjében *(Intended Purposes)* az Encrypting File System bejegyzést találjuk, majd kattintsunk jobb gombbal a tanúsítványra, és az *All Tasks/Export (Összes feladat/Exportálás)* paranccsal mentsük le a fájlt. Ahhoz, hogy egy másik számítógépen, vagy ugyanazon, de esetlegesen újratelepített rendszer esetében hozzáférjünk titkosított adatainkhoz, az imént kimentett tanúsítványfájl importálására van szükség (melyet szintén a Certificate Managerrel végezhetünk el).



3.32. ábra: *Az EFS-tanúsítvány exportálása*

A csoportházirendből igen részletesen konfigurálhatjuk az EFS működését. Lehetőségünk van az EFS teljes tiltására, de beállíthatjuk a felhasználók *Dokumentumok* mappáinak, vagy akár az imént említett lapozófájl automatikus titkosítását, valamint megkövetelhetjük USB SmartCard használatát is.

A Windows Defender és a titkosított fájlrendszer *(Encrypted File System — EFS)*
Ebben a demóban együtt mutatjuk be a Windows Defender kémprogram kereső alkalmazás részleteit, illetve a fájlok/mappák titkosításáért felelős EFS-szolgáltatás megváltozott lehetőségeit.
Fájlnév: I-3-4c-Defender-EFS.avi

BitLocker: a lemezek titkosítása

A felmérések szerint a legtöbb kényes vállalati és személyes információ elveszett vagy ellopott számítógépekről, főként notebookokról jut illetéktelen kezekbe. Éppen ezért egyre inkább elvárás, hogy adataink még a számítógép kikapcsolt állapotában is védve legyenek. A Windows Vista ezt is lehetővé teszi a BitLocker meghajtótitkosítás segítségével. A BitLocker egy vadonatúj technológia, mely a merevlemez tartalmát még a gép szétszerelése és a lemezhez való közvetlen hozzáférés esetén is olvashatatlan adathalmazzá változtatja. Természetesen – mivel az operációs rendszer ilyenkor nem fut – ehhez külső segítségre van szüksége, nevesül a TPM, azaz Trusted Platform Module chipre, vagy egy USB-kulcsra.

A BitLocker két fő funkcióval védi adatainkat: a lemez tartalmának teljes titkosításával (128- vagy 256-bites AES algoritmussal) és a bootfolyamat előtt a kritikus rendszerfájlok integritásának ellenőrzésével. Az operációs rendszer még akkor sem indítható el, ha illetéktelenek valamilyen külső eszközzel esetleg módosítják a betöltést végző komponenseket, így próbálván kiiktatni a titkosítást. A BitLocker a Vista eredeti kiadásában a teljes fájlrendszert – beleértve a lapozó- és hibernációs fájlt is – titkosítja, de csak a rendszermeghajtóra alkalmazható. Ez az állapot várhatóan a Windows Vista első javítócsomagjában változni fog, és az említett korlát végleg megszűnik, azaz a BitLocker titkosítás valamennyi lemezre és partícióra kiterjeszthetővé válik.

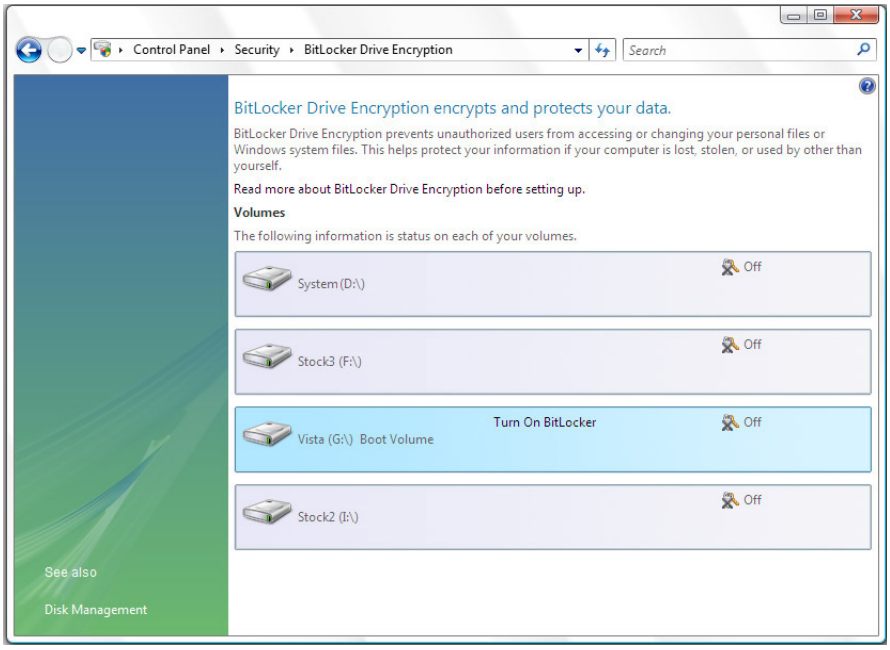
A BitLocker működéséhez az alábbi feltételek szükségesek:

- A BitLocker használatához speciális módon kell particionálni a merevlemezt: a rendszerköteten kívül szükség van egy legalább 1,5 GB méretű, aktív, NTFS fájlrendszert használó partícióra is, melyen a rendszerindító fájlok kapnak helyet – ez a kötet nem kerül titkosításra.
- A számítógép BIOS-ának támogatnia kell az USB-szabványú eszközökről való olvasást és írást még az operációs rendszer betöltődése előtti fázisban.
- Legalább TPM 1.2-es verziójú integrált titkosító chip az alaplapon, vagy egy USB-kulcs.
- Trusted Computing Group (TCG)-szabványt támogató BIOS (TPM használata esetén).

A BitLocker háromféle módon alkalmazható, a következőkben – növekvő biztonsági sorrendben – bemutatjuk a titkosítási eljárás lehetséges konfigurációit.

- **Transzparens mód (TPM chip használata)** – A felhasználónak semmilyen plusz teendője nincs, ha a rendszerindító fájlok érintetlenségéről a TPM modul megbizonyosodott, elindul az operációs rendszer és a felhasználó a szokásos módon bejelentkezhet.
- **USB-kulcs használata** – A felhasználónak még a számítógép indítása előtt csatlakoztatnia kell a titkosítókulcsot tartalmazó USB-eszközt a számítógéphez. Ebben az esetben szükséges, hogy a számítógép még az operációs rendszer betöltése előtt képes legyen kezelni az USB-eszközöket.
- **TPM chip és felhasználószintű hitelesítés együttes használata** – A legbiztonságosabb konfiguráció, ha a TPM modulon kívül a felhasználó birtokában lévő PIN-kód is szükséges az indításhoz. A BitLocker multifaktoros hitelesítéséhez a Windows Vista kétféle módszert támogat: a boot-folyamat előtt a PIN-kód bekérése a felhasználótól, vagy a kiegészítő azonosító USB-kulcsról történő beolvasása.

Mivel a BitLocker technológia elsősorban a vállalati felhasználókat célozza, a meghajtótitkosítást csak a Windows Vista Enterprise és Ultimate változatai támogatják. Ha rendelkezésre áll a megfelelő konfiguráció, a szolgáltatást a *Control Panel/Security/BitLocker Drive Encryption* menüpont alatt kapcsolhatjuk be.



3.33. ábra: *A BitLockert csak a rendszerpartíción használhatjuk (egyelőre)*

A haladó tűzfal és az IPSec-kapcsolatok

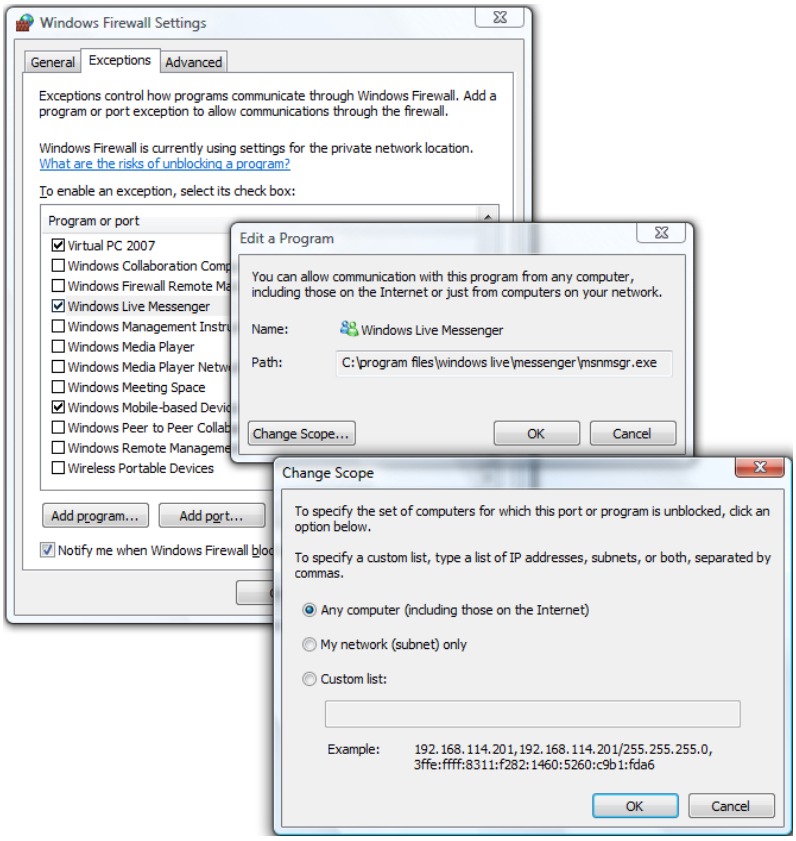
A számítógépes tűzfalak feladata a hálózati interfészeken keresztül folyó forgalom szűrése és – szükség szerint – tiltása. Ezeket a feladatokat különféle szabályok szerint végzik, melyek vagy alapértelmezésként kerülnek beállításra, vagy a felhasználó később határozza meg azokat. A Windows ügyfél operációs rendszerek az XP óta beépített tűzfallal rendelkeznek, mely igazán az XP Service Pack 2-ben vált „nagykorúvá". A Windows Vista viszont egy teljesen új tűzfalat tartalmaz, melynek két arcával is találkozhatunk: az egyszerű, XP-ből már ismerős felülettel és egy rendkívül részletes beállítási lehetőségeket nyújtó, saját MMC-konzollal.

A tűzfal egyszerű felülete a vezérlőpultból egyetlen kattintással elérhető, mindössze a *Security* kategória alatt az *Allow a program through Windows Firewall* hivatkozást kell választanunk. Mint láthatjuk, a kezelőfelület semmit sem változott az XPSP2 óta, a lap első fülén ki-, illetve bekapcsolhatjuk a szolgáltatást (alapértelmezésként be van kapcsolva), valamint egy gombnyomással letilthatjuk a második fülön beállítható kivételszabályokat. Erre akkor lehet szükség, ha valamilyen nem megbízhatónak minősített hálózatra, például egy nyilvános WiFi-hálózatra csatlakozunk.

A második fülön kivételeket képezhetünk saját alkalmazásaink számára, melyeknek a tűzfalon keresztül, saját porton át kell kommunikálniuk a külvilággal. Itt már találhatunk néhány gyárilag konfigurált kivételt olyan Windows-rendszerszolgáltatások számára, mint például a hálózati felderítés, fájl- és nyomtatómegosztás, vagy a távsegítség. Amikor egy program úgynevezett listening portot nyit magának, vagyis bejövő adatokat kíván fogadni, a Windows tűzfal egy kérdést intéz a felhasználó felé, ahol eldönthetjük, hogy engedélyezzük-e a kivételszabály létrehozását. A kérdéssel minden program esetében és minden hálózati profilban csak az első alkalommal találkozunk, a szabály bekonfigurálása után a tűzfal nem kérdez többet.

Kivételszabályt kézzel is megadhatunk, ekkor lehetőségünk van portszám (és hálózati protokoll), illetve alkalmazás szerint létrehozni a bejegyzést. A beállított kivételhez ezek után már csak hatókört kell társítanunk – ez jelentheti csak az alhálózaton, vagy akár minden irányból, így az internet felől történő kapcsolat-fogadását, de megadhatunk egyéni címtartományt is.

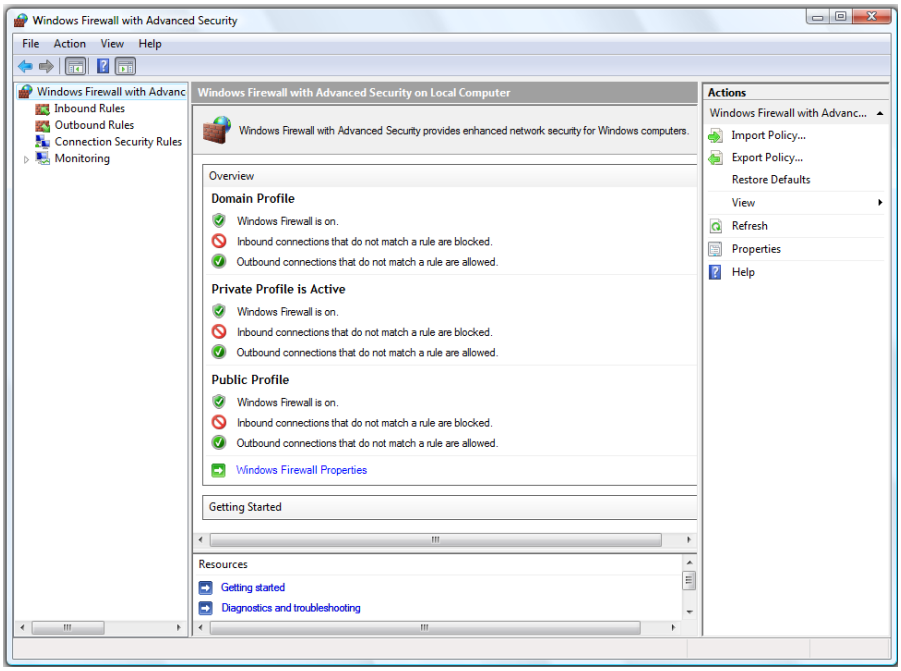
Ha ennél részletesebb beállításokra van szükségünk, a Windows Firewall with Advanced Security *(Fokozott biztonságú Windows tűzfal)* konzolhoz kell fordulnunk, melyet a felügyeleti eszközök között találhatunk. A kezdőlapon egy gyors áttekintést kapunk a tűzfal állapotáról, hálózati profilonként olvashatjuk le a szolgáltatás jellemzőit: fut-e a tűzfal, illetve mely szabályrendszerek szerint vannak tiltva, illetve engedélyezve a kapcsolatok. Alapértelmezésként a tűzfal minden profilban aktív, illetve minden olyan bejövő kapcsolat, mely nem kötődik szabályhoz, tiltás alatt áll.



3.34. ábra: *Az új tűzfal hagyományosan ismerős arca…*

Mivel a Windows Vista alkalmas különféle hálózati szolgáltatások nyújtására is (például web- és FTP-helyek publikálására), illetve egy kártevő program is működtetheti pl. SMTP-kiszolgálóként az operációs rendszerünket, alapvetően szükséges a tűzfal részéről a forgalom kétirányú szűrése. Az új tűzfal ennek megfelelően immár két irányban véd, igaz a kifelé irányuló kapcsolatok szűrése alapértelmezésként ki van kapcsolva, mert a tapasztalatlan otthoni felhasználók számára ez általában szükségtelen és problémákat okozhat – azonban bármikor bekapcsolhatjuk.

A bal oldali sáv legfelső bejegyzésére (*Windows Firewall with Advanced Security – Fokozott biztonságú Windows tűzfal)* jobbkattintva és a tulajdonságlapot megnyitva elérhetjük a tűzfal általános beállításait, itt konfigurálhatjuk be a főlapon is látható paramétereket, valamint a blokkolt kapcsolatok esetén felbukkanó értesítéseket. Több fület is láthatunk, mivel a három hálózati profilnak megfelelően külön-külön határozhatjuk meg a tűzfal működését, egy külön lapon pedig az integrált IPSec-szolgáltatás alapértelmezett beállításait találhatjuk.

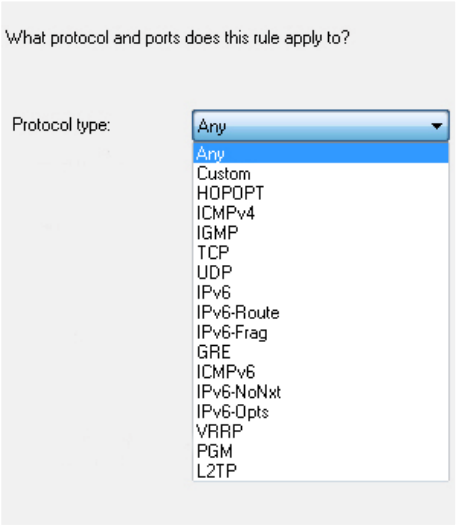


3.35. ábra: *...és a teljesen új MMC konzol, a haladó opciókkal*

A konzol fastruktúrájában találhatók a szabályrendszerek tárolói, illetve az egyéb kapcsolatbiztonsági beállítások, valamint a tűzfal felügyeleti eszközei. Az Inbound Rules *(Bejövő szabályok)* bejegyzésre kattintva előtűnnek a befelé irányuló kapcsolatokra érvényes szabályok. Számos előre definiált bejegyzéssel találkozhatunk itt, ezek közül csak néhány aktív, ezeket a sor előtti zöld ikon jelzi. Egy-egy szabályt kettős kattintással szerkeszthetünk, de a gyári beállításokat érdemes érintetlenül hagyni. Saját szabályt is létrehozhatunk, erre az Action *(Művelet)* menü alatti New Rule... *(Új szabály...)* varázslót használhatjuk, mely végigvezet egy szabály beállításának lépésein.

Mint a tűzfal egyszerűsített vezérlőpultján, itt is lehetőség van program és port szerint is felállítani a szabályt. Pluszként azonban előre definiált szolgáltatásokat (távoli asztal, fájl- és nyomtatómegosztás, hálózati felderítés stb.) is bekonfigurálhatunk – ezekhez előre és eltérő körülményekre legyártott szabályok léteznek – és teljesen egyéni szabály létrehozását is kérhetjük, ahol minden paramétert kézzel kell megadnunk.

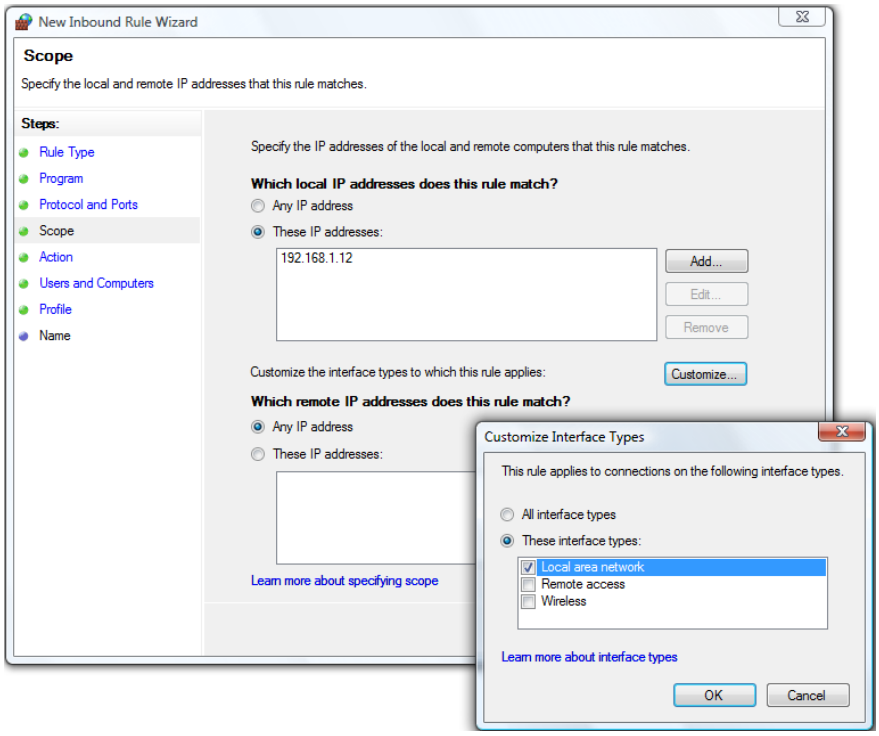
A szabály hatókörét egyes programokra korlátozhatjuk, de egy listából kiválaszthatunk Windows-szolgáltatásokat is. Ha protokoll és port szerint szűrünk, megadhatjuk a protokoll típusát, (illetve számát), a kapcsolathoz használt helyi és távoli portok számát. Ugyanígy a helyi, illetve távoli IP-címeket, sőt akár a hálózati interfészt is megszabhatjuk, melyek a kapcsolatban részt vehetnek, majd azt kell meghatároznunk, hogy a szabály engedélyezze vagy blokkolja az imént beállított paraméterek szerinti kapcsolatokat. Ebben a lépésben beállíthatjuk, hogy a kapcsolat csak akkor legyen engedélyezett, ha az titkosított, tehát biztonságos.



Következő lépésként azokat a hálózati profilokat kell kiválasztanunk, melyekben a tűzfalszabály él, végül egy nevet és egy rövid leírást (opcionális) kell csatolnunk a szabályhoz. Ugyanezzel a varázslóval dolgozunk, amikor kimenő forgalom szabályozását állítjuk be az Outbound Rules *(Kimenő szabályok)* szekcióban.

A Windows tűzfal – mivel MMC konzolból vezérelhető – távoli számítógépről felcsatlakozva is kezelhető, valamint a *netsh* parancssori eszközzel is lekérdezhetjük és megváltoztathatjuk a beállításokat. A tűzfal haladó beállításainak parancssorból történő kezeléséhez használjuk a *netsh advfirewall* utasításcsoportot.

A már említett IPSec olyan nyílt szabványokból álló keretrendszer, amely kriptográfiai biztonsági szolgáltatások segítségével teszi lehetővé a titkosított kommunikációt az IP-protokollt használó hálózatokon. Az IPSec-protokoll két legfontosabb célja, hogy megvédje az IP-csomagok tartalmát, és hogy védelmet nyújtson hálózati támadásokkal szemben a megbízható kommunikáció kikényszerítésével. Az IPSec a titkosításon alapuló védelmi szolgáltatások, a biztonsági protokollok és a dinamikus kulcskezelés alkalmazásával mindkét célnak megfelel. E biztos háttér szolgáltatja azt a hatékonyságot és rugalmasságot, amely a szóló és site-to-site VPN-hálózatok számítógépei, tartományok, és pl. webhelyek közötti biztonságos kommunikációt lehetővé teszi. Sőt, az IPSec a megadott forgalomtípusok fogadásának vagy továbbításának blokkolására is használható.

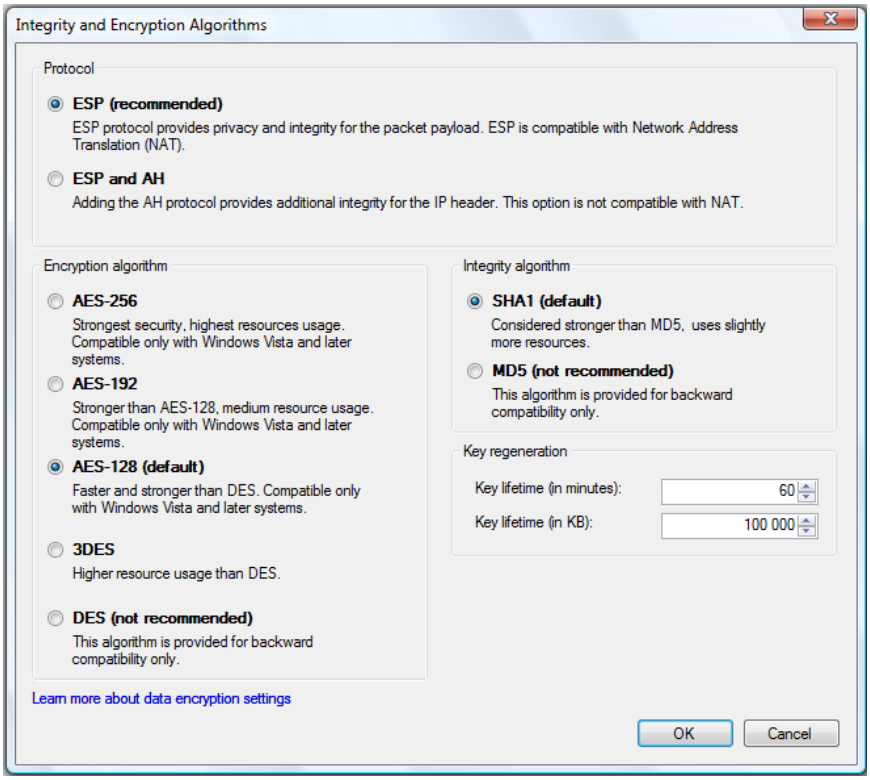


3.36. ábra: *A szabályok akár a hálózati interfész típusától is függhetnek*

Az IPSec-protokoll biztonsági szolgáltatásainak beállításához eddig kizárólag a különböző házirendek voltak használatosak. Az IPSec-házirendek igény szerint alakíthatók, így egy adott számítógépre, alkalmazásra, tartományra vagy az akár az egész vállalatra szabhatók.

A Windows Vistában az IPSec is új ruhába bújt, ezen túl Connection Security Rules *(Kapcsolatbiztonsági szabályok)* néven, a haladó tűzfal MMC-be integrálva is találkozhatunk vele (a csoportházirendből továbbra is definiálhatók IPSec házirendek). De nem csak a ruha új, most már valóban egyszerűvé vált a használat is, azaz nem szükséges elmerülnünk a kriptográfia mélységeibe, ahhoz, hogy bekapcsoljuk két tetszőleges végpont közt az IPSec-et. A haladó beállítások nagyon szépen el vannak rejtve, az alapbeállításokkal viszont eleve biztonságosan, pár kattintással készíthetünk azonnal működő hálózati forgalomtitkosítást.

Kapcsolatbiztonsági szabályokat a hagyományos tűzfalszabályokhoz hasonlóan varázsló segítségével állíthatunk elő, a lehetőségek tárháza bőséges, választhatunk izolációt, kiszolgáló-kiszolgáló kapcsolat beállítását, hitelesítés-mentesítést állíthatunk be, valamint biztonságos átjárót *(tunnel)* hozhatunk létre. Rendelkezésünkre állnak új algoritmusok is, a titkosításhoz AES-128/192/256, a kulcscseréhez ECDH-P 256/384 titkosítást is használhatunk.



3.37. ábra: *Az IPSec titkosítási beállításai*

Az IPSec parancssorból is kezelhető, ehhez a már ismert *netsh* eszközt alkalmazhatjuk. A netsh IPSec kontextusába való belépéshez használjuk a *netsh -c ipsec* parancsot.

A tűzfal MMC-konzol Monitoring *(Figyelés)* tárolóban megtekinthetjük az aktuálisan aktív és működő szabályokat, tűzfal- és kapcsolatbiztonság szerint külön csoportosítva. A Security Associations *(Biztonsági társítások)* bejegyzés alatt az aktív kapcsolatbiztonsági (IPSec) beállítások kerülnek listázásra.

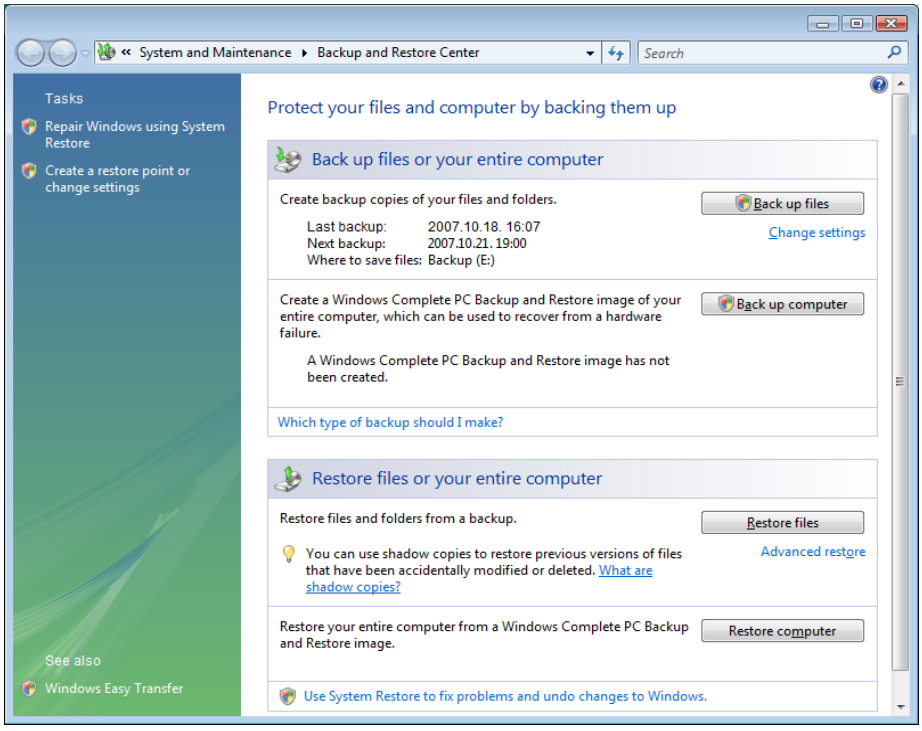
A „két" (valójában csak egy) Windows Vista tűzfal
Ebben az előadásban sor kerül a Windows Vistában integrált tűzfal mindkét arcának bemutatására, a haladó lehetőségeket részletesen kielemezve.
Fájlnév: I-3-4d-Windows-Firewall.avi

Mentés és visszaállítás

A korábbi Windows-verziókkal ellentétben a Vista mentésével és visszaállításával kapcsolatos feladatokat már nem az NTBackup-program, hanem a hangzatos nevű Backup and Restore Center *(A biztonsági mentés és visszaállítás központja), illetve* az innen elindítható Backup Status and Configuration *(Biztonsági mentés állapota és konfigurációja, sdclt.exe)* felületéről végezhetjük el.

Az NTBackup-program használatával, a kiszolgálók mentésének és visszaállításának kérdéseivel a hatodik fejezetben részletesen fogunk foglalkozni, most csak a Vista speciális lehetőségeivel ismerkedünk meg.

Itt adhatjuk meg az egyes fájlok és mappák, automatikus mentésével, illetve a teljes számítógép disk image *(lemezkép)* alapú mentésével kapcsolatos beállításokat, és innen kezdeményezhetjük az adatok visszaállítását is.



3.38. ábra: *Backup and Restore Center*

A Vista négy különböző lehetőséget nyújt a biztonsági mentések készítésére, ezek mindegyike más módon, és másféle adatok mentésére használható előnyösen. A következőkben áttekintjük az egyes mentési típusokat, és megvizsgáljuk azt is, hogy melyik típus milyen adatok mentésére használható legjobban.

- **Restore points** *(Visszaállítási pontok)* – a rendszerfájlok és a rendszerkonfiguráció mentésére használható, segítségével az operációs rendszer egy korábbi állapotára térhetünk vissza (a felhasználók adataira a visszaállítás nem vonatkozik).
- **Previous Versions** *(Előző verziók)* – a szolgáltatás elsősorban a felhasználók fájljainak mentésére és visszaállítására használható, a mentések automatikusan történnek, a visszaállítási műveleteket pedig maguk a felhasználók kezdeményezhetik. (A szolgáltatás az árnyékmásolatokon alapul, amelynek részletes ismertetése a negyedik fejezetben található.)
- **Create backup copies of yout files and folders** *(Fájlok és mappák biztonsági mentése)* – elsősorban a felhasználók fájljainak mentésére használható automatikus (időzített), illetve kézi indítással.
- **Complete PC backup** *(A teljes számítógép mentése)* – a teljes számítógép lemezkép alapú mentése, ami tartalmazza valamennyi kötet valamennyi adatát, vagyis az összes rendszerfájlt és -beállítást, illetve a felhasználók fájljait is.

A biztonsági másolatok tárolása

A biztonsági mentések típusainak megfelelően alapvetően két különböző módszer áll rendelkezésre a mentéskor keletkező állományok tárolására. A System Restore *(Rendszer-visszaállítás)* és az árnyékmásolatok szolgáltatáshoz kapcsolódó adatok minden esetben a szolgáltatás által védett kötet rejtett részére kerülnek, vagyis például a merevlemez meghibásodása esetén várhatóan nem lesznek elérhetők.

Ezzel ellentétben a fájlokról készített mentések, illetve a teljes számítógép lemezkép alapú mentését tároló fájlok csak önálló tárolóeszközre helyezhetők. A biztonsági mentések a következő adathordozókon tárolhatók:

- Merevlemezek (belső vagy külső).
- Írható DVD- és CD-lemezek. (A program szükség esetén kérni fogja további üres lemezek behelyezését is.)
- Hálózati megosztás (csak fájlokról készített mentés esetén).

A System Restore-szolgáltatás

A System Restore *(Rendszer-visszaállítás)* szolgáltatás segítségével restore pointokat *(visszaállítási pontok)* hozhatunk létre, amelyek lehetővé teszik a rendszer helyreállítását sikertelen frissítések, szoftver- vagy hardvertelepítés, illetve más változtatások után. A következőkben áttekintjük a visszaállítási pontokkal kapcsolatos tudnivalókat és beállítási lehetőségeket.

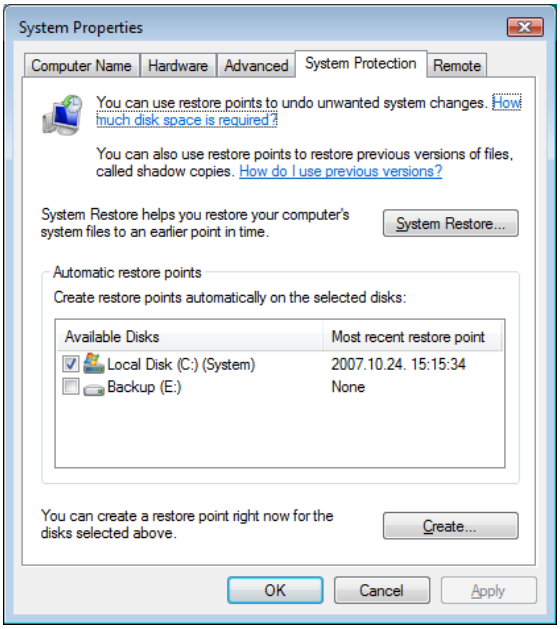
A visszaállítási pont tulajdonképpen a számítógép egy adott kötetének (pontosabban a köteten lévő rendszer- és programfájloknak, illetve a regisztrációs adatbázisnak) lemezre mentett pillanatfelvétele, amelynek segítségével visszaállítható a pillanatfelvétel időpontjának rendszerkonfigurációja. A System Restore-szolgáltatás alapértelmezés szerint napi ütemezéssel automatikusan készíti el a helyreállítási pontokat. A System Restore az adatok mentését kötetenként végzi, vagyis a szolgáltatás az egyes kötetekre engedélyezhető, illetve tiltható. Alapértelmezés szerint a Vista maximálisan az adott kötet területének 15%-át használja a visszaállítási pontok tárolására (a minimálisan szükséges terület 300 MB), és a szolgáltatás a rendszert tartalmazó kötet esetében engedélyezve van.

A *System Restore*-szolgáltatás által mentett adatok az adott kötet *System Volume Information* nevű mappájában tárolódnak. Minden egyes visszaállítási pont külön almappába kerül, amelynek neve tartalmaz egy 32 karakter hosszú egyedi azonosítót (GUID). NTFS-köteteken a mappa nem érhető el a felhasználók számára (még a rendszergazdáknak sem); alapértelmezés szerint egyedül a *System* fiók kap jogot a mappa elérésre. Ha szeretnénk tudni, hogy mennyi helyet foglalnak a *System Restore* által mentett adatok, egy rendszergazda jogosultsággal futó parancssorban adjuk ki a következő parancsot: *vssadmin list shadowstorage*.

Fontos megjegyezni, hogy a System Restore a személyes adatokat (például a felhasználói profil tartalmát) nem menti, így ezeket az esetleges visszaállítás sem fogja érinteni, viszont mivel az árnyékmásolatok (lásd később) készítését is a System Restore engedélyezésével kapcsolhatjuk be, mégis érdemes lehet a szolgáltatást a felhasználói adatokat tartalmazó kötetekre is engedélyezni.

A napi ütemezés mellett természetesen „kézzel” is készíthetünk visszaállítási pontokat (az ábrán lévő Create *(Létrehozás)* gomb megnyomásával), illetve a Vista bizonyos események bekövetkeztekor automatikusan is készít további visszaállítási pontokat. A visszaállítási pont készítését kiváltó események a következők (csökkentett módú rendszerindítás esetén nem készülnek visszaállítási pontok):

- **Program telepítése** – megfelelő telepítőprogram esetén a telepítést megelőzően visszaállítási pont készül. A visszaállítási pont segítségével probléma esetén helyreállíthatjuk a számítógép telepítést megelőző állapotát.



3.39. ábra: *Alapértelmezés szerint a System Restore csak a rendszert tartalmazó kötet változásait figyeli*

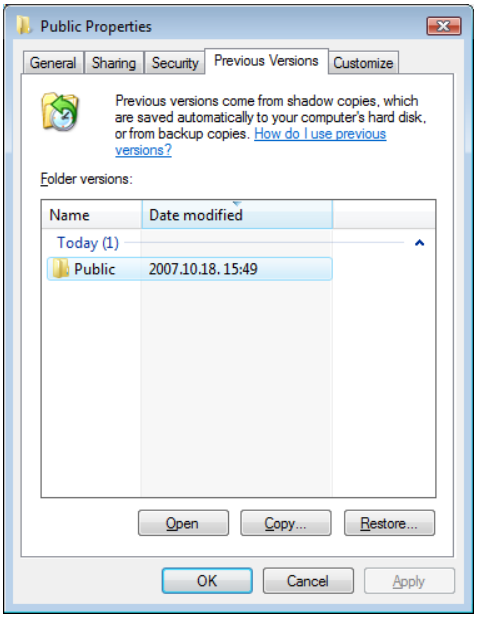
- **Frissítések telepítése** – az automatikus frissítések telepítése előtt is készül visszaállítási pont.
- **Visszaállítási művelet** – visszaállítási pont készül minden visszaállítási pontra történő visszatérés előtt is, így könnyen visszavonhatjuk az elhibázott műveletek hatását.
- **Aláírás nélküli eszközmeghajtó telepítése** – visszaállítási pont készül az aláíratlan, illetve nem minősített eszközmeghajtók telepítése előtt. (A minősített meghajtók korábbi állapotának visszaállítása a Device Manager *(Eszközkezelő)* Driver Rollback *(Az eszközmeghajtó visszaállítása)* műveletével lehetséges.)
- **Mentésből való visszaállítás** – visszaállítási pont készül, ha a Vista beépített mentőszoftverének segítségével fájlokat állítunk vissza.

Problémát okozhat, ha a Windows Vista-rendszer mellett Windows XP is telepítve van a számítógépen. Ebben az esetben a Windows XP indításakor a Vista által mentett valamennyi visszaállítási pont (az árnyékmásolatokkal együtt) megsemmisül. A jelenségnek oka az, hogy mivel a Windows XP nem ismeri a Vista által létrehozott visszaállítási pontok formátumát, azt feltételezi, hogy azok sérültek, így egyszerűen törli őket, majd létrehozza a saját visszaállítási pontjait.

A Previous Versions-szolgáltatás

A Previous Versions *(Előző verziók)* szolgáltatás a sérült, illetve véletlenül módosított vagy törölt fájlok egyszerű, a felhasználók által kezelhető visszaállítási lehetőségét biztosítja. Egy fájl vagy mappa előző verziója származhat a Vista beépített mentőszoftverével létrehozott mentési fájlból, vagy árnyékmásolatból, amelyek a visszaállítási pontok részeként alapértelmezés szerint naponta egyszer kerülnek mentésre (csak változás esetén).

Az árnyékmásolat-szolgáltatás a Windows Server 2003 esetében is létezik, erről részletes leírás található a negyedik fejezetben. A Windows Server 2003 esetén azonban az előző verziók csak az árnyékmásolattal védett kötet megosztott mappáinak elérésekor állnak rendelkezésre. A Vista újdonsága, hogy az árnyékmásolatok, és így a fájlok és mappák előző verziói helyi kötetek esetében is elérhetők és használhatók.



3.40. ábra: *Az árnyékmásolat szolgáltatás helyi meghajtókra is használható a Vistában*

Az árnyékmásolatokat a rendszer a visszaállítási pont részeként, az ott megadott paramétereknek megfelelően menti. Ha a System Restore szolgáltatás engedélyezve van (a szolgáltatás alapértelmezés szerint csak a rendszert tartalmazó kötetet védi), akkor a kötet megváltozott fájljairól naponta egy árnyékmásolat készül (természetesen a nem módosított fájlokról nem). Ha több kötetet is szeretnénk védeni az árnyékmásolatok segítségével, azokon is engedélyeznünk kell a System Restore-szolgáltatást.

Az árnyékmásolatok használatával kapcsolatban mindenképpen figyelembe kell vennünk az alábbi szempontokat:

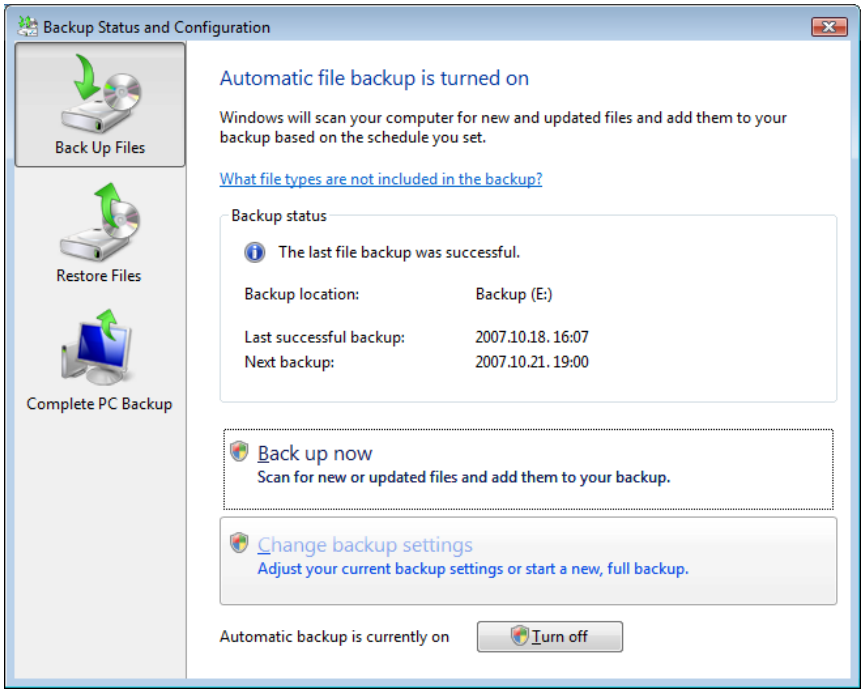
- Az árnyékmásolatok élettartama korlátozott. Alapértelmezés szerint a kötet 15%-a áll rendelkezésre, erre a célra, ha ezt elérjük, a további árnyékmásolatok elkezdik felülírni a legrégebben készült példányokat.
- Árnyékmásolat csak a fájlok, illetve mappák megváltoztatásakor készülnek. Ha egy adott fájl már hosszú idő óta változatlan, akkor elképzelhető, hogy egyáltalán nem lesznek árnyékmásolatai (bár ebben az esetben nincs is szükség rájuk).
- Amint már említettük, ha a számítógépen más operációs rendszert (Windows XP-t) indítunk el, akkor valamennyi árnyékmásolat és a visszaállítási pontok is törlődni fognak.

A rendelkezésre álló előző verziók megtekintéséhez kattintsunk a fájlra, illetve mappára az egér jobb gombjával, és válasszuk a Restore Previous Versions *(Korábbi verziók visszaállítása)* menüpontot.

Az előző verziók *(Previous Versions)* használata
Ebben a demóban bemutatjuk a Vistába immár alapértelmezésben integrált Previous Versions szolgáltatás igencsak kellemes előnyeit.
Fájlnév: I-3-5a-Previous-Versions.avi

Fájlok és mappák mentése

A fájlalapú mentés segítségégével a felhasználók személyes fájljainak mentését végezhetjük el, ez a módszer programok, illetve beállítások mentésére nem használható. A mentési fájlból önálló fájlokat és mappákat is visszaállíthatunk, de például a merevlemez meghibásodása esetén először fel kell telepítenünk az operációs rendszert és valamennyi programot. A mentés a beállított ütemezés szerint történik, de az időzítésen kívül csak a mentési helyet és a mentendő fájlok típusát határozhatjuk meg.



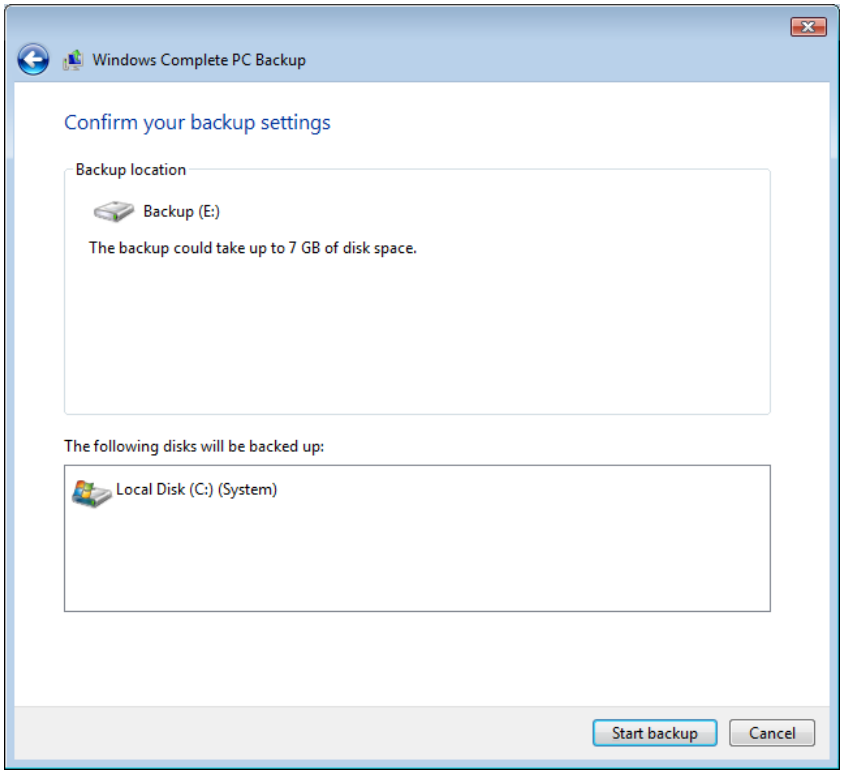
3.41. ábra: *A Vista beépített mentőszoftvere automatikusan menti a felhasználók fájljait*

Complete PC Backup

A teljes számítógép mentése azt jelenti, hogy a számítógép kijelölt köteteiről (a rendszerkötetről mindenképpen) lemezkép *(disk image)* alapú másolatot készítünk. A lemezkép tartalmazza az adott kötet valamennyi adatát, a rendszerfájlokat és beállításokat, valamint a felhasználók fájljait is. A mentési fájl (vagyis a lemezkép) mérete nagyjából meg fog egyezni az összes elmentett adat eredeti méretével.

A lemezképek formátuma a Virtual PC (és a Virtual Server) által is használt *.vhd* (virtual hard disk) formátum, vagyis azok akár egy virtuális gép alá is becsatolhatók.

Mielőtt a mentést elvégeznénk, célszerű megkeresni és kijavítani a kötet esetleges hibáit (*chkdsk*), és töredezettségmentesíteni a kötetet. Ha a mentést második merevlemezre szeretnénk elvégezni, NTFS fájlrendszerrel kell megformáznunk azt (tömörített kötetre nem helyezhetjük a mentési fájlt).



3.42. ábra: *A rendszerkötet lemezkép alapú mentése második merevlemezre*

A teljes számítógép mentése csak teljes kötetekre vonatkozhat, egyedi fájlok vagy mappák kiválasztására nincs lehetőség, így aztán a mentés elvégzése is meglehetősen egyszerű: csak a célhelyet kell megadnunk és ki kell választanunk a mentendő köteteket.

A számítógép visszaállítását elvégezhetjük a Backup and Restore Center felületéről, de nem induló rendszer esetén ez az út természetesen nem járható. Ebben az esetben a visszaállításhoz a Vista telepítőlemezéről kell elindítanunk a számítógépet, de a szokásos telepítés helyett válasszuk a Repair Your Computer *(Számítógép javítása)* hivatkozást, majd a Windows Complete PC Restore *(Windows Complete PC Visszaállítás)* opciót.

Mentés és visszaállítás
Ez a részletes előadás a Vista fájlokat és mappákat érintő mentőeszközével, illetve a speciális komplett lemezkötet mentés szolgáltatással foglalkozik.
Fájlnév: I-3-5b-Mentes-visszallitas.avi

II. RÉSZ

A kiszolgáló

A második részben a jelenleg aktuális hálózati kiszolgáló operációs rendszer, a Windows Server 2003 R2 képességeit ismertetjük, szintén három fejezetben.

Kiszolgáló a hálózatban — Windows Server 2003 R2 185. oldal

A könyv negyedik fejezete egy általános bevezetésnek tekinthető a Windows kiszolgálók alkalmazásához. A telepítés témakörétől az alap fájl- és nyomtatószolgáltatásokon keresztül egészen a hálózati szolgáltatásokig jutunk el. A fejezet utolsó harmadában kapott helyet a Windows Software Update Services (WSUS) részletes ismertetése is.

Tartományi környezet 275. oldal

Az ötödik fejezetben megpróbáltunk egy általános, de azért alapos és mély áttekintést nyújtani a Windows hálózatok legfontosabb alkotóeleméről, a címtárszolgáltatásról. Részletesen taglaljuk a címtár szerkezetét, objektumait, mentését, és az olyan kapcsolódó szolgáltatásokat, mint például a DNS névfeloldás. Ezek mellett a Csoportházirendről és a telephelyekről is szót ejtünk.

Hibakeresés és -elhárítás 339. oldal

A könyv befejező fejezete igazi unikumnak számít. A hibakeresés kapcsán ismertetjük a Windows operációs rendszerek alapszintű működését, a rendszerindítástól kezdve, a Recovery Console-on keresztül egészen a „kék halálig”. A fejezet további részeiben pedig a Windows hálózatokban előforduló problémák megoldásához használható, beépített illetve külső eszközökről esik szó.

NEGYEDIK FEJEZET

Kiszolgáló a hálózatban — Windows Server 2003 R2

A fejezet tartalma:

A Windows Server 2003 használatával számos új, jól használható szolgáltatás, és természetesen számos megoldandó feladat jelenik meg a hálózat és a rendszergazda életében. Bár az ügyfélgépek felügyelete közben megszerzett ismeretek jelentős része a kiszolgálók üzemeltetéséhez is jól felhasználható, rengeteg új kihívással is szembe kell néznünk: a kiszolgáló számítógép mind a hardver, mind pedig az operációs rendszer szintjén jelentős újdonságokat nyújt.

A következőkben megismerkedünk a kiszolgálók telepítésének, valamint az alapszolgáltatások beállításának és felügyeletének legfontosabb elemeivel. Az alábbi témaköröket fogjuk megtárgyalni:

- **Kiszolgáló alkalmazása: előnyök, alapismeretek** – áttekintjük, hogy milyen előnyökkel jár, és milyen esetekben szükséges a kiszolgáló számítógépek alkalmazása.
- **Előkészületek és telepítés** – sorra vesszük azokat a szempontokat, amelyeket figyelembe kell vennünk a kiszolgáló operációs rendszer telepítése előtt, majd áttekintjük a telepítés menetét és a kész operációs rendszerben elvégzendő ellenőrző műveleteket.
- **A kiszolgálók alapfunkciói** – megismerkedünk a Windows kiszolgálók alapszolgáltatásaival, a fájlok tárolásának és megosztásának különféle módszereivel. Bemutatjuk a Windows Server 2003 R2 verziójában megjelenő, a fájl- és nyomtatómegosztással kapcsolatos legfontosabb újdonságokat.

- **Hálózati szolgáltatások** – a kiszolgálók valamennyi szolgáltatása a hálózaton keresztül érhető el, így számos funkció kapcsolódik a megfelelő hálózati működés, és az ügyfelek hálózati hozzáférésének biztosításához. Ebben a részben áttekintjük az IP-címek kiosztásának módszereit, a WINS-névszolgáltatással kapcsolatos legfontosabb tudnivalókat, és a hálózathoz, illetve az egyes számítógépekhez való távoli hozzáférés lehetőségeit. Ide tartozik természetesen a hálózatok névfeloldását biztosító, és az Active Directory címtár működéséhez feltétlenül szükséges DNS-szolgáltatás is, de ezzel a következő fejezetben fogunk részletesen foglalkozni.
- **Egyéb kiszolgálóoldali összetevők** – ebben a részben röviden ismertetünk néhány további szolgáltatást, majd megismerkedünk a Windows alkalmazáskiszolgáló platformjával és két erre épülő alkalmazással is.

Kiszolgáló alkalmazása: előnyök, alapismeretek

Mielőtt nekifognánk a kiszolgálók telepítésével és üzemeltetésével kapcsolatos tudnivalók tárgyalásának, mindenképpen tisztáznunk kell egy fontos kérdést, amely joggal merülhet fel egy kisebb, mondjuk négy-öt számítógépből álló hálózat esetében: kell nekünk egyáltalán kiszolgáló? Hiszen a számítógépekből kialakított egyenrangú hálózat (látszólag) mindent tud, amire egy kiszolgálót használnánk: létrehozhatunk megosztott mappákat és közösen használt nyomtatókat, definiálhatunk felhasználói fiókokat, hozzáférési jogosultságokat stb. Mindenünk megvan, minek ide még egy számítógép, amely nagy, drága, hangos, sokat kell vele foglalkozni és még egy Word se futhat rajta?

A kiszolgáló számítógép azonban még egy egészen kis hálózat esetében is igen fontos és hasznos lehet. Az ügyfél-kiszolgáló hálózat rengeteg előnyös tulajdonsággal rendelkezik, számos olyan szolgáltatást vehetünk igénybe, amelyek egyenrangú hálózat esetében nem elérhetők, illetve az ott meglévő szolgáltatások is jelentősen eltérő formában, sokkal hatékonyabban használhatók és felügyelhetők. A kiszolgálók a következő előnyöket biztosítják az egyenrangú számítógépekből álló hálózatokkal szemben:

- **Állandó, folyamatos üzem, folyamatos erőforrás-megosztás** – egy kiszolgáló számítógépet már a hardver szintjén arra terveztek, hogy képes legyen a folyamatos, megszakítás nélküli üzemre, hónapokon, vagy akár éveken keresztül. A megbízhatóbb, sok esetben redundáns

hardverelemekből felépített gépek sokkal ritkábban hibásodnak meg, illetve meghibásodás esetén is nagyon rövid idő alatt, sőt esetenként folyamatos üzem közben is elvégezhető a hiba elhárítása. A kiszolgálók tehát képesek arra, hogy erőforrásaikat folyamatosan, megszakítás nélkül ügyfeleik rendelkezésére bocsássák.

- **Nagyobb teljesítmény** – Természetesen a kiszolgáló általában jóval nagyobb teljesítményre képes, mint egy átlagos asztali gép, ráadásul az erőforrások használata a hálózatból érkező kérések minél hatékonyabb kiszolgálására van optimalizálva. Például fájlmegosztás esetén egy kiszolgáló számítógép jóval hatékonyabban képes feladatának ellátására sok beérkező kérés esetében is.

- **Jogosultságok központi kezelése** – ha az erőforrások megosztását a kiszolgáló végzi, akkor a hozzáférési jogosultságokat is a kiszolgáló kezeli, így azok beállítását és felügyeletét csak egy helyen kell elvégeznünk. További lehetőséget nyújt ezzel kapcsolatban, ha a kiszolgáló beüzemelésével kapcsolatban a címtárat, vagyis az Active Directoryt is telepítjük. A címtár képes arra, hogy a hálózat objektumait egységes, jól kezelhető formában tegye elérhetővé a felhasználók és a rendszergazdák számára, így a jogosultságok központi kezelése a hálózat valamennyi elemére vonatkozóan megvalósítható. Az Active Directory címtárszolgáltatás felépítésével, telepítésével és használatával a következő fejezetben részletesen is foglalkozni fogunk.

- **Központi felügyelet** – kiszolgáló (vagy kiszolgálók) használatával megvalósítható a teljes hálózat központi felügyelete (leginkább akkor, ha az Active Directory szolgáltatásait is igénybe vesszük). A központi felügyelet alapját képező csoportházirend segítségével a kiszolgálók és ügyfélgépek beállításait nem egyesével, hanem a kiszolgálón létrehozott beállítás-gyűjtemények használatával, központilag adhatjuk meg. Ez a megközelítés lehetővé teszi azt, hogy valamennyi számítógép és felhasználó biztosan megkapja a neki járó beállításokat – vagyis az ügyfélgépek teljesen egységesen, pontosan a rendszergazda által meghatározott módon működhetnek –, és jelentősen megkönnyíti a sok számítógépet, illetve felhasználót érintő változtatások kezelését is. A központi felügyelet részeként olyan célszoftvereket is használhatunk (például System Center Esentials 2007 (SCE), System Center Operations Manager 2007 (SCOM), Windows Server Update Services (WSUS), amelyek lehetővé teszik, hogy gyakorlatilag minden, a hálózatot, illetve a számítógépeket érintő felügyeleti műveletet központilag végezhessünk el, és a rendszer működését befolyásoló valamennyi jelentős eseményről már a bekövetkezésével egy időben (sőt sok esetben előre is) értesüljünk.

- **Alkalmazásplatform** – a Microsoft kiszolgáló operációs rendszerei stabil, megbízható alkalmazásplatformot nyújtanak különféle kiszolgáló termékek számára (legyen szó akár a Microsoft, akár külső gyártók, akár a vállalat saját fejlesztőinek termékeiről). Az infrastruktúrában rejlő lehetőségek kihasználásával az egészen bonyolult, összetett alkalmazások is viszonylag gyorsan és könnyen elkészíthetők.

A kiszolgáló feladatai

Hogy valóban szükség van-e kiszolgáló beszerzésére és üzembe állítására, az attól is függ, hogy milyen szolgáltatásokat igényel a hálózat és a felhasználók. Ezek közül bizonyos feladatokat az ügyfélgépek maguk is elláthatnak, de a fent felsorolt előnyök miatt, nagyobb igénybevétel, vagy kritikus fontosságú funkció esetén már mindenképpen érdemes megfontolni a kiszolgáló alkalmazását. A következőkben áttekintjük a tipikus kiszolgálói feladatokat, és szót ejtünk arról is, hogy milyen esetben lehet ezek egy részét ügyfélgépre bízni.

- **Fájl-, és nyomtatómegosztás** – a fájlok és nyomtatók megosztása a kiszolgáló számítógépek klasszikus funkciója. Ez a funkció látszólag azonos módon megvalósítható ügyfélgépeken is, azonban intenzívebb, biztonságos és folyamatos használatra ez a megoldás már nem alkalmas, ráadásul számos kiegészítő funkció csak kiszolgáló operációs rendszer esetén érhető el. Nagyjából azt mondhatjuk, hogy az ügyfélgépek által biztosított fájl- és nyomtatómegosztás az egyetlen szobányi cégméretig használható, már csak azért is, mert az ügyfelek megosztásaihoz egy időben maximum tíz felhasználó csatlakozhat. A kiszolgálók fájl- és nyomtatómegosztásai elvileg korlátlan számú felhasználó kiszolgálására képesek, intenzív használat esetén is biztosíthatják a megfelelő teljesítményt, a folyamatos hozzáférést és az adatbiztonságot, a kiegészítő szolgáltatások (árnyékmásolatok, elosztott fájlrendszer, mappa alapú kvótázás, fájlszűrés stb.) pedig sok felhasználó esetén is biztosítják a hatékony üzemeltetés feltételeit.
- **Hálózati szolgáltatások** – a hálózati szolgáltatások egy része (például az internetkapcsolat megosztása) elérhető ügyfélgépek esetében is, de erre is vonatkoznak a hálózat méretével és a számítógépek számával kapcsolatos korábban már említett korlátozások, a vállalati hálózatok számára legfontosabb szolgáltatások (DHCP, DNS, távoli elérés, útválasztás) pedig csak kiszolgáló operációs rendszereken érhetők el.

- **Biztonsági mentés** – a biztonsági mentést és helyreállítást végző NTBackup.exe alkalmazás természetesen elérhető az ügyfélrendszereken is, de ebben az esetben csak az ügyfél saját merevlemezén tárolt adatok mentését végezhetjük el segítségével. A központi (kiszolgálón történő) adattárolás (például a felhasználók dokumentumtároló mappáinak átirányításával) nagymértékben megkönnyíti a biztonsági mentéssel és visszaállítással kapcsolatos feladatok hatékony és biztonságos elvégzését, az elosztott fájlrendszer és a replikáció használatával pedig tovább fokozhatjuk a tárolt adatok biztonságát.
- **Levelezés és csoportmunka** – ha a vállalat saját kezébe kívánja venni a levelezés és csoportmunka kezelését (vagyis nem elégszik meg az internetszolgáltató által nyújtott lehetőségekkel, vagy a különféle ingyenes megoldásokkal), akkor Windows-platformon mindenképpen szükség van a kiszolgáló operációs rendszer beépített POP3 és SMTP-szolgáltatásra (vagy a kiszolgálóra telepíthető Exchange Serverre), illetve a Windows SharePoint Services-szolgáltatásra.
- **Web- és ftp-szolgáltatások** – a web- és ftp-szolgáltatásokat, illetve a webkiszolgálón alapuló hálózati alkalmazások hátterét az IIS (Internet Information Services) biztosítja. Az IIS ügyfélrendszereken is elérhető, de ebben az esetben több szempontból is korlátozott lehetőségekkel rendelkezik. Nyilvánosan elérhető web-, vagy ftp-hely üzemeltetésére például az ügyfél-IIS semmiképpen nem alkalmas, már csak azért sem, mert egy időben legfeljebb tíz felhasználó csatlakozhat hozzá. Egészen más a helyzet azonban a kiszolgálón futó IIS esetén, ez a változat már tökéletesen megfelelő nagy terheléssel működő, nyilvános web- vagy ftp-szolgáltatás biztonságos üzemeltetésére is.

Egy vagy több kiszolgáló kell?

A vállalatunk számára szükséges kiszolgálók számának meghatározásakor alapvetően három szempontot kell figyelembe vennünk:

- **Teljesítmény** – teljesítmény szempontjából a Windows-rendszerek igen jól méretezhetők, a Windows Server 2003 R2 Enterprise Edition 64-bites változata például 8 processzor, 2 TB memória és a jövőbeli álmok szintjén mozgó tárolókapacitás kezelésére képes. Természetesen az operációs rendszer mellett figyelembe kell vennünk az elérhető hardverkonfigurációk teljesítményét (és árát) is, mindenesetre ez a szempont még meglehetősen nagy teljesítményigény esetén sem indokolja feltétlenül több kiszolgáló használatát. Mindenképpen több kiszolgálóra van szükség azonban akkor, ha valamilyen hálózati szolgál-

tatás teljesítményét terheléselosztást végző fürt (Network Load Balancing, NLBS) használatával szeretnénk megnövelni. A hálózati terheléselosztást végző fürtök legfeljebb 32 darab Windows-kiszolgáló egyesítésével biztosítják a TCP- és UDP-alapú szolgáltatások és alkalmazások méretezhetőségét. A hálózati terheléselosztás segítségével például a web- és ftp-kiszolgálók, a távoli elérést biztosító VPN-kiszolgálók, és a terminálszolgáltatások teljesítményét növelhetjük.

- **Igényelt szolgáltatások** – egyáltalán nem mindegy, hogy a rendelkezésre álló teljesítményt milyen szolgáltatások megvalósítására fordítjuk, bizonyos esetekben a különféle funkciókat nem ajánlott (esetleg nem is lehetséges) egyetlen kiszolgálón elhelyezni. A vállalat SBS-kiszolgálója (Small Business Server) nem lehet például terminálkiszolgáló; ha erre a szolgáltatásra is szükségünk van, mindenképpen egy második kiszolgálót kell üzembe állítanunk. Bár elvileg lehetséges, de biztonsági jellegű problémákat okozhat az, ha a tűzfalszoftver (ISA Server) a belső hálózat által igényelt szolgáltatásokkal (tartományvezérlő, belső DNS-kiszolgáló, Exchange stb.) egy számítógépen osztozik, mivel ebben az esetben kényszerűen növelnünk kell a tűzfalat futtató számítógép támadható felületét (bár ez a kifelé néző interfészre természetesen nem vonatkozik). Megfelelő hardver esetén azonban ezek a problémák a különböző virtualizációs technológiák (például az ingyenesen használható Virtual Server 2005) segítségével is kezelhetőek.
- **Üzembiztonság (redundancia)** – a legtöbb esetben ez a szempont indítja el a kisvállalatokat a több kiszolgáló felé vezető úton. Bár a kiszolgálók a legtöbb esetben már a hardver szintjén is rendelkeznek bizonyos redundanciával (tápegység, RAID lemezvezérlők stb.), a teljes hálózat üzemképessége olyan fokon függ a kiszolgálók által biztosított szolgáltatásoktól (például az Active Directorytól), hogy nem érdemes kockáztatni, ha kritikus fontosságú a hálózat folyamatos működése (és hol nem az?), akkor például tartományvezérlőből minimálisan kettőre van szükség. A kiszolgálófürtök alkalmazása szintén az üzembiztonság fokozását szolgálja, amihez természetesen ugyancsak több kiszolgálóra van szükség (maximálisan nyolc csomópontot használhatunk). A Microsoft Cluster Service (MSCS) segítségével feladatátvételi fürtöket *(Fail-Over Cluster)* valósíthatunk meg, azaz, ha a fürt valamelyik csomópontja kiesik, az azon futó szolgáltatásokat egy másik csomópont veszi át. Kiszolgálófürt esetén a közös szolgáltatások adatai egyetlen példányban, megosztott elérésű lemezeken tárolódnak.

Előkészületek és telepítés

A következőkben megismerkedünk a Windows-kiszolgálók különféle változataival, áttekintjük, hogy milyen szempontokat kell figyelembe vennünk a kiszolgáló telepítése előtt, és mely kérdésekre kell választ találnunk, mielőtt a telepítőlemezt a meghajtóba helyezzük. Tulajdonképpen ez a telepítés nehezebb része; a későbbi esetleges problémák nagy része a tervezésre, (illetve annak hiányára) vezethető vissza. Megfelelő előkészítés után a telepítőprogram futtatása tulajdonképpen már semmiféle problémát nem okozhat.

A Windows Server 2003 különféle változatai

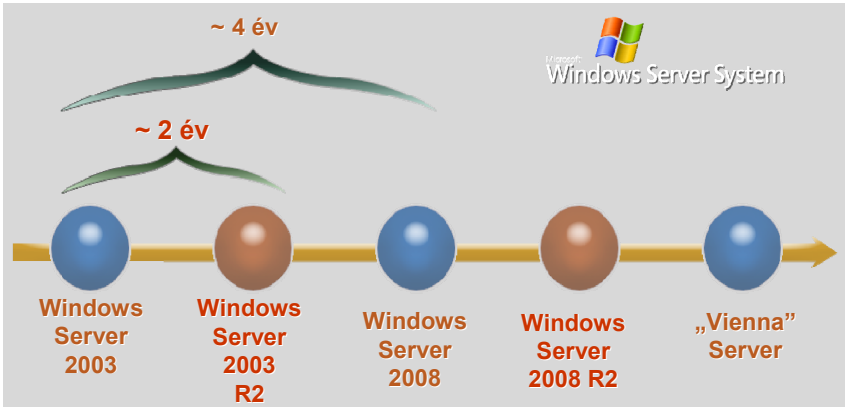
A tervezés egyik fontos lépése az operációs rendszer vállalatunk számára megfelelő változatának kiválasztása. A vállalatok eltérő igényeinek figyelembe vételével a Windows Server 2003 számos különféle változatban is elérhető, amelyek részben az elérhető szolgáltatások körében, részben pedig a skálázhatóságban különböznek egymástól. A következőkben áttekintjük az egyes változatok legfontosabb tulajdonságait:

- **Windows Server 2003 Datacenter Edition R2** – Ez a változat biztosítja a legmagasabb szintű méretezhetőséget és rendelkezésre állást, kritikus üzleti megoldásokhoz, nagy mennyiségű „real-time" tranzakcióhoz, szerverkonszolidációhoz használható. A Datacenter Edition 32-bites és 64-bites változatban is létezik. A 32-bites változatban minimum 8, maximum 32 processzor és 128 GB RAM használható, a 64-bites változat pedig maximálisan 2 TB memória és 64 processzor kezelésére képes. A Datacenter Edition persze nem kapható akármelyik boltban (sőt önmagában sehol sem), a Microsoft ezt a változatot csak speciális, többnyire igen nagy teljesítményű, testreszabott hardverkonfiguráció részeként értékesíti.
- **Windows Server 2003 Enterprise Edition R2** – Közepes és nagyvállalati környezetben képes a hálózati infrastruktúrához tartozó valamennyi fontos szolgáltatás biztosítására, kiválóan használható vállalati alkalmazások, és elektronikus kereskedelmi rendszerek háttereként. A 32-bites változat 64 GB, a 64-bites pedig 2 TB RAM kezelésére képes, és mindkét változat 1…8 processzoron használható.

- **Windows Server 2003 Standard Edition R2** – Kisvállalati és telephelyi környezetben képes az alapvető hálózati és alkalmazásszolgáltatások biztosítására. A Standard változat maximum 4 processzor használatát támogatja, és 4 GB a használható RAM felső határa.
- **Windows Server Web Edition** – Dedikált webkiszolgáló, feladata weboldalak, webalkalmazások és webszolgáltatások hátterének biztosítása. A kiszolgáló kifejezetten webes alkalmazásokhoz van optimalizálva, tartalmazza az ehhez szükséges alapvető felügyeleti és biztonsági funkciókat. Egy- és kétprocesszoros gépekre telepíthető, és 2 GB RAM kezelésére képes (egyéb korlátozásokkal is találkozhatunk használatakor).
- **Windows Small Business Server 2003 (SBS) Standard Edition R2** – Komplett kiszolgálócsomag kisvállalatok részére. A csomag az önálló komponensekhez képest jelentősen kedvezőbb áron kapható, de használata bizonyos korlátozásokkal jár. Az SBS szolgáltatásait legfeljebb 75 felhasználó veheti igénybe, és a licencfeltételek szerint a csomagot alkotó valamennyi kiszolgáló-alkalmazásnak egyetlen gépen kell futnia. További korlátozás, hogy az SBS-tartomány nem integrálható más tartományokkal (viszont az SBS-tartományban több kiszolgáló, sőt tartományvezérlő is használható). A standard változat a következő komponenseket tartalmazza:
  - Microsoft Windows Server 2003.
  - Microsoft Exchange Server 2003 SP2, Standard Edition – csoportmunka, internetes levelezés.
  - Microsoft Office Outlook 2003 – levelezőprogram az SBS-ügyfélgépekre.
  - Health Monitor 2.1 – a kiszolgáló és az alkalmazások teljesítményének, paramétereinek ellenőrzése, naplózása.
  - Remote Web Workplace *(Távoli webes munkahely)* – a legfontosabb szolgáltatások interneten keresztül történő elérése.
  - Windows Server Update Services (WSUS) – a frissítőcsomagok központi letöltése és elosztása.
- **Windows Small Business Server 2003 Premium Edition** – A Premium Edition minden korlátozása megegyezik a Standard változatéval, de dobozában a fentieken kívül a következő komponenseket is megtalálhatjuk:

- Microsoft Internet Security and Acceleration Server 2004 – tűzfal és proxykiszolgáló
- Microsoft SQL Server 2005, Workgroup Edition – adatbázis kiszolgáló

Valamennyi változatból már csak az R2 kiadás kapható, ez a megelőzőhöz képest 21 új komponenst tartalmaz, amelyek közül a legfontosabbakkal a továbbiakban meg is fogunk ismerkedni.



4.1. ábra: *A Windows Server fejlesztési ciklusa*

A fenti ábrán látható a Microsoft kiszolgáló operációs rendszereinek tervezett fejlesztési ciklusa. A nagyjából négyévente megjelenő új fővonalbeli verziók között félúton szerepel egy-egy köztes változat, amelyben alapvető technológiai változás nélkül jelenik meg jó néhány új szolgáltatás. Ennek a vonalnak az első képviselője a Windows Server 2003 R2, ami az SP1-re alapul, és telepítésekor szabadon válogathatunk a megjelent új komponensek közül.

A telepítés előkészületei

A kiszolgáló telepítésének megkezdése előtt (különösen, ha egy kisvállalat első kiszolgálójáról van szó) rengeteg körülményt kell figyelembe vennünk, hogy jó döntéseket hozhassunk, és a beüzemelt számítógép beválthassa a hozzá fűzött reményeket. Nagyon fontos, hogy minden lényeges körülményt tisztázzunk előre, vagyis még a telepítés megkezdése előtt. Alapos tervezéssel egy rugalmas és átlátható, könnyen kezelhető és a cég későbbi, akár nem tervezett igényeinek is megfelelő rendszert hozhatunk létre. A következőkben felsoroljuk azokat az alapvető szempontokat, amelyek az előkészítés során figyelmet érdemelnek.

Hardverigény (eredetileg ajánlott)

Az alábbi táblázatban a Windows Server 2003 elméleti jellegű hardverigényét láthatjuk, a valós igények meghatározása azonban nem minden esetben egyszerű feladat. A szükséges hardver erősen függ a körülményektől, minél több szolgáltatást futtatunk, minél több felhasználót kell kiszolgálnunk, annál izmosabb hardverre lesz szükség.

Komponens	Minimális követelmény
Processzor	P-III 550 MHz
RAM	256 MB
Merevlemez	2,9 GB szabad terület a rendszerpartíción
Optikai meghajtó	CD-ROM vagy DVD-ROM meghajtó
Képernyő	VGA, vagy a konzolátirányítást támogató hardver
Egyebek	Hálózati csatoló

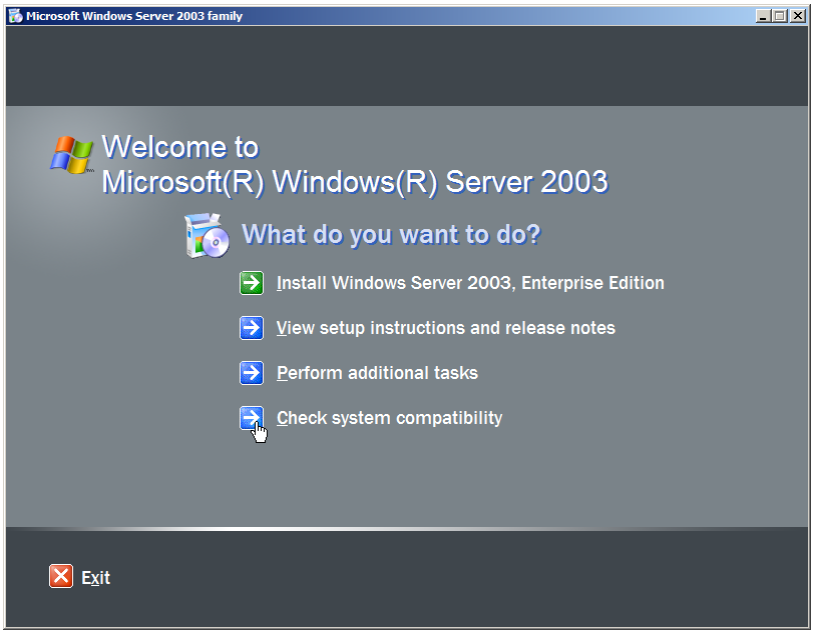
Általánosságban a következő szempontok megfontolását javasoljuk:

- **Több processzor** – a processzorok számának növelésével általában jelentős teljesítménynövekedés érhető el, mivel ebben az esetben az erre felkészített programok több processzor egyidejű használatával párhuzamosíthatják működésüket, illetve az egyes alkalmazások is több processzoridőt kaphatnak.
- **RAM** – Gyakran a fizikai memória bővítése a legfőbb teljesítményjavító tényező.
- **Hardver RAID** – Több gyors lemezmeghajtó külön lemezvezérlőkkel való használata jelentős mértékben gyorsíthatja az I/O-feldolgozást és lerövidítheti az írási/olvasási időt. A különféle RAID-megoldások használata a sebességen kívül az adatbiztonságot és megbízhatóságot is jelentősen növelheti.
- **Több lapozófájl** – Ha a lapozófájlt több fizikai lemezre osztjuk szét, valamelyest gyorsulhat a virtuális memóriához való hozzáférés.

Előzetes hibafelderítés

A minimális hardverkövetelmények betartásán kívül némi figyelmet kell fordítanunk hardvereszközeink, illetve alkalmazásaink kompatibilitására is. A hardvereszközök előzetes vizsgálatára a Hardware Compatibility List *(Windows-hardverkompatibilitási lista)* weboldalt *(http://www.microsoft.com/hcl)*, illetve a telepítőlemezen található *hcl.txt* fájlt is használhatjuk. Természetesen, még a kompatibilis eszközök esetében is gondoskodnunk kell a legfrissebb meghajtóprogramok beszerzéséről, illetve esetleg a számítógép BIOS-ának frissítéséről is.

Ha a számítógépen már van valamiféle Windows operációs rendszer, akkor alkalmazásaink és a meghajtóprogramok kompatibilitás-vizsgálatát a telepítőprogram nyitóképernyőjéről indítható kompatibilitás-vizsgáló program segítségével is elvégezhetjük. A program segítségével automatikus vizsgálatot indíthatunk, amelynek eredményeként listát kapunk a problémás alkalmazásokról, illetve meghajtóprogramokról.



4.2. ábra: *A negyedik menüponttal indítható a telepítés előtti kompatibilitás-vizsgálat*

A programot elindíthatjuk a telepítőprogram futtatása nélkül is, ha a telepítőlemez \i386 mappájában kiadjuk a *winnt32 /checkupgradeonly* parancsot.

Aktív internetkapcsolat esetén a telepítés, vagy a kompatibilitás-vizsgálat közben is frissíthetjük a rendszerben található meghajtóprogramokat, sőt a telepítőprogram által használt rendszerállományokat is.

Az operációs rendszer nyelvi verziója

Bár látszólag jelentéktelen, de a későbbiekre való tekintettel mégis megfontolásra érdemes a kiszolgáló operációs rendszer nyelvi verziójának kiválasztása. A magyar nyelvű rendszer talán kényelmesebbnek tűnhet, különösen a kezdő rendszergazdák számára, de ha bármilyen hibaüzenetre kell rákeresnünk az interneten, akkor az angol változat begépelésével valószínűleg nagyságrendekkel több releváns találatot kapunk. Persze bőven elég egyetlen jó találat is, de sajnos magyarul az esetek jelentős részében ennyire sem számíthatunk. További előnye az angol verzió használatának, hogy ebben az esetben hetekkel, esetleg hónapokkal korábban jutunk hozzá a különféle javítócsomagokhoz és szoftverfrissítésekhez.

Milyen környezetbe kerül az új kiszolgáló?

Figyelembe kell vennünk, hogy pontosan milyen a környezet, amivel már rendelkezünk, milyen körülményekhez kell alkalmazkodnunk, esetleg mi az, amit éppen a kiszolgáló telepítésével szeretnénk megváltoztatni. Ugyancsak tekintettel kell lennünk a hálózatunkban használt többi kiszolgáló komponensre, és a különféle speciális alkalmazásokra. Könnyen megtörténhet, hogy a jelenleg használt verziót nem támogatja az új operációs rendszer, de ha már elérhető a frissített változat, akkor erősen ajánlott ezt még a telepítés előtt tisztázni, és megtenni a szükséges intézkedéseket. Ugyanez vonatkozhat különféle egzotikus hardvereszközökre; elképzelhető az is, hogy a régóta meglévő eszköz már egyáltalán nem használható.

Fontos kérdés a kiszolgáló beállításainak megadásakor, hogy milyen ügyfélrendszerek fogják igénybe venni annak szolgáltatásait. Ha régebbi ügyfélrendszerek használatára kényszerülünk, a velük való együttműködés befolyásolhatja a használható biztonsági paraméterek körét, illetve támogatásuk speciális szolgáltatások használatát is szükségessé teheti (például WINS). Természetesen figyelembe kell vennünk a kiszolgálóhoz és az ügyfélrendszerekhez kapcsolódó licenceket, be kell szereznünk a szükséges példányokat.

Ha már meglévő számítógépen frissítjük az operációs rendszert (akár Windows NT 4.0 Server rendszerről is frissíthetünk), fel kell készülnünk arra az eshetőségre is, hogy valami miatt nem sikerül az új kiszolgáló telepítése (hardver inkompatibilitás, esetleg egy kritikus fontosságú szoftver, amely az új rendszeren nem működik megfelelően), és ezért vissza kell állítanunk a korábbi kiszolgálót. Hogy ezt megtehessük, a frissítés előtt mindenképpen készítsünk az NTBACKUP-program segítségével rendszerállapot- *(System State)* mentést (kényesebb esetben teljes mentésre is szükség lehet) a régi rendszerről.

Ha korábban is volt már kiszolgálónk, újra kell gondolnunk a kiszolgálószerepek elosztását, és fontos lehet a kiszolgálók frissítésének sorrendje is.

Lemezparticionálás és fájlrendszer

Még a telepítés megkezdése előtt tervezzük meg a létrehozandó partíciók méretét és a használandó fájlrendszert. Kiszolgálónk teljesítményét jelentősen megnövelheti, ha az operációs rendszert és az adatokat külön lemezmeghajtón (vagy legalább külön partíción) tároljuk. Több lemezegység használatával az időigényes írási/olvasási műveletek párhuzamosan hajthatóak végre. Szintén teljesítménynövelő hatású, és az adatok elvesztésének esélyét is csökkenti, ha a több lemezt tartalmazó kiszolgálók esetében hibatűrő köteteket hozunk létre (tükrözött és RAID-5 kötetek) dinamikus lemezekkel. Szoftveres RAID-5 kötetek létrehozhatók az operációs rendszer Lemezkezelés eszközével, de választhatunk hardveres megoldást is.

A rendszert tartalmazó partíció mérete természetesen erősen függ a használandó szolgáltatások mennyiségétől, de ezen nem nagyon érdemes takarékoskodni. 10 GB-nál kisebb rendszerpartíciót csak komoly kényszerítő eszközök hatásának engedve hozzunk létre, de a 15-20 GB sem túlzás, ha azt szeretnénk, hogy ne kelljen zavarba jönnünk egy-egy kiegészítő komponens, vagy javítócsomag telepítésekor, elférjen a lapozófájl stb. Szintén célszerű előre átgondolni azt, hogy fogunk-e használni olyan komponenst, amelyhez önálló partícióra van szükség. Ilyen lehet például (nagyon sok várható objektum esetén) a címtár, vagy például a WSUS-kiszolgáló.

A rendszer számára kiválasztott partíció formázását mindenképpen NTFS fájlrendszer használatával végezzük el, sőt erősen ajánlott az összes többi partíciót is ilyen módon formázni. Az NTFS fájlrendszer használata számos előnnyel jár, ezek közül csak a legfontosabbakat soroljuk fel:

- Az NTFS maximális partíció- vagy kötetmérete jóval nagyobb a FAT rendszerénél, ráadásul a kötet- vagy a partícióméretek növekedésével az NTFS fájlrendszer teljesítménye nem csökken, ellentétben a FAT-tal.
- Az NTFS által biztosított jogosultsági rendszer a megosztások használatakor is előnyös, mivel segítségével nemcsak mappák, hanem egyedi fájlok szintjén is szabályozható a hozzáférés.
- A fájltitkosítás szolgáltatás nagymértékben növelheti az adatok biztonságát.
- NTFS fájlrendszer esetén működik a lemezműveletek helyreállítási naplózása, amelynek segítségével a fájlrendszer képes az adatok áramszünet, vagy más rendszerproblémák utáni helyreállítására, így nem kell erős izgalmi állapotban újraindítanunk a kiszolgálót egy váratlan leállás után.
- Az alkalmazások által létrehozott nagyon nagyméretű, de átmenetileg csak kevés adatot tároló fájlok esetében az NTFS fájlrendszer csak a fájl azon része számára foglal le lemezterületet, ahová már adatok íródtak.

Hálózati paraméterek

Gondolkodjuk el előre (és lehetőleg írjuk is fel az eredményt) a különféle hálózati paramétereken. Mi legyen például a számítógép, vagy a tartomány neve? Mivel a TCP/IP-protokollkészlet kötelező elem a Windows Server 2003 esetén is, nem árt, ha előre tisztázzuk, hogy mely hálózati interfész milyen módszerrel fog IP-címet kapni. Ha statikus beállítást használunk (ez a különböző kiszolgáló komponensek miatt sok esetben kötelező), akkor mi legyen az IP-cím, az alapértelmezett átjáró (ha szükséges egyáltalán), mi a DNS- vagy WINS kiszolgáló(k) címe a választott névfeloldás típusától függően stb. Feltétlenül célszerű előre tisztázni a fentieket, mivel gépünk már a telepítés közben (de legkésőbb az első bejelentkezéskor) használni fogja ezeket az adatokat, így sok múlhat a megadott értékeken.

Tartomány vagy munkacsoport?

A kiszolgáló telepítésének előkészületei közben joggal merül fel a kérdés, hogy érdemes-e belevágni az Active Directoryra épülő tartományi rendszer kiépítésébe, vagy jobban járunk az egyszerűbben beüzemelhető munkacsoportos környezet használatával. A válasz tulajdonképpen nagyon egyszerű, a bonyolultabb tartományi rendszer kiépítésébe fektetett munka, és az elérhető haszon összehasonlításából könnyen levezethető.

Talán meglepő lesz az állítás, de a határvonal valahol öt(!) ügyfélszámítógép környékén van. Ennél kevesebb gép esetén, bár kiszolgálóra már szükség lehet, de az Active Directory-rendszer beüzemelésével és felügyeletével (és még inkább a megtanulásával) kapcsolatos tennivalók elvégzése helyett valószínűleg jobban járunk a munkacsoportos környezet kialakításával. Nagyjából tíz számítógépig a befektetés és a haszon többé-kevésbé megegyezik, vagyis a bevezetéskor elvégzett munkát már kompenzálják a későbbi előnyök. Tíz gép fölött egyértelműen az Active Directory javára billen a mérleg, munkacsoportos környezetben a jó színvonalú üzemeltetés már aránytalanul több munkával jár, sőt néhány újabb ügyfélgéppel később egyszerűen lehetetlenné válik. Bizonyos esetekben a gépek számától függetlenül sincs mérlegelési lehetőségünk: ha például Exchange Serverre van szükség, akkor mindenképpen tartományi környezetet kell kialakítanunk.

Az Active Directory-rendszer kialakításával és üzemeltetésével a következő fejezetben fogunk részletesen foglalkozni.

Az operációs rendszer telepítése

A telepítőprogram elindítására két lehetőségünk van: bootolhatunk közvetlenül a telepítőlemezről, illetve már telepített Windows rendszer esetén futtathatjuk a Setup.exe programot a CD gyökérmappájából. Ha a CD-lemezről indítjuk a számítógépet, és valamiféle speciális tárolóeszközt használnánk (ismeretlen SCSI vagy RAID lemezvezérlő stb.), a gép elindulása némi izgalommal járhat, mivel összesen kettő másodpercünk van arra, hogy F6-ot nyomjunk, és hajlékonylemezről beadjuk a megfelelő eszközmeghajtó fájlt.

Ha ezen túljutottunk, a telepítőprogram futása közben már nincs sok teendőnk, sorban meg kell adnunk a korábban összegyűjtött adatokat, és ki kell várnunk az a nagyjából 30-40 percet, amíg a folyamat lezajlik. Ebben a szakaszban már igen kicsi rá az esély, hogy bármilyen izgalmas esemény történjen, de ha esetleg megáll a telepítőprogram, akkor sem kell kétségbe esni. Ha biztosan nem csak a türelmetlenség miatt estünk tévedésbe, akkor nyugodtan indítsuk újra a gépet, a telepítő onnan fogja folytatni, ahol abbahagyta.

Nagyobb a baj, ha ez azt jelenti, hogy ugyanott újra meg is áll (esetleg „kék halált" hal), ekkor biztosan valami komolyabb (várhatóan hardverrel kapcsolatos) problémába sikerült belefutnunk. Írjuk fel pontosan a hibaüzenetet, és nézzünk utána a jelenségnek a Microsoft Knowledge Base-ben *(Tudásbázis)* a *http://support.microsoft.com* címen.

Ha a telepítő lefutott

A telepítő sikeres lefutása esetén azonban még nem vagyunk készen: ellenőriznünk kell a hardver és szoftvereszközök megfelelő működését. Teszteljünk mindent! Kezdjük a Device Managerrel *(Eszközkezelő),* bizonyosodjunk meg róla, hogy a Windows valóban helyesen felismerte és telepítette a számítógépben lévő hardvereszközök meghajtóprogramjait, különös tekintettel a hálózati csatolókra.

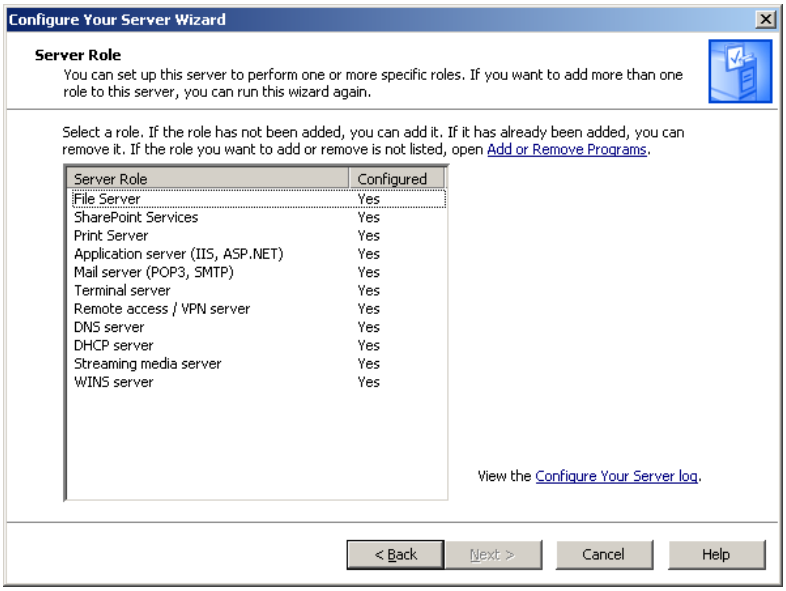
Nézzük át az Event Viewer *(Eseménynapló)* különféle bejegyzéseit! Ha már ebben a szakaszban sorozatos hibákat találunk, akkor annak mindenképpen utána kell nézni.

Ha frissített kiszolgálóról van szó, akkor próbáljuk meg elindítani valamennyi örökölt alkalmazást, amit az új gépen is használni szeretnénk!

Vizsgáljuk meg részletesen a hálózati kapcsolatot! Elérhető minden, aminek elérhetőnek kell lenni? Van névfeloldás (ha kellene lennie)? Az ügyfelekről elérhető a kiszolgáló? A hálózaton kívülről elérhető minden, aminek elérhetőnek kell lennie? Esetleg olyasmi is elérhető, ami inkább nem kéne?

Ha minden rendben van, akkor a kiszolgáló telepítésének első részével készen vagyunk. Azért csak az első résszel, mert amit kaptunk, az még csak egy üres váz, a továbbiakban ki kell választanunk, és fel kell telepítenünk azokat a szolgáltatásokat, amelyekre a vállalatnak és a felhasználóknak (és persze a rendszergazdának) szüksége van.

A 4.3. ábrán látható lista azokat a szolgáltatásokat tartalmazza, amelyekre a Windows Server 2003 R2 változata külső erők bevonása nélkül képes. A következőkben minden „Yes” megjelölésű (vagyis valamennyi) szolgáltatással meg fogunk ismerkedni, bár néhány esetben (IIS, Sharepoint stb.) csak a legfontosabb funkciók leírására szorítkozunk. Az egyes szolgáltatások telepítését innen, vagyis a Configure Your Server Wizard *(Kiszolgáló konfigurálása varázsló)* felületéről, illetve az Add or Remove Programs *(Programok telepítése/törlése)* modulból is elvégezhetjük.



4.3. ábra: *A Windows 2003 R2 szolgáltatásai*

A Windows Server 2003 különféle szolgáltatásainak felügyeletére szinte minden esetben az ügyfél operációs rendszernél már megismert Microsoft Management Console (MMC) technológián alapuló felügyeleti konzolok szolgálnak. Valamennyi konzol esetében lehetőség van távoli kiszolgálók elérésére is, vagyis akár egyetlen konzol segítségével felügyelhetjük a vállalat összes kiszolgálóját.

A kiszolgálóhoz tartozó felügyeleti konzolokat telepíthetjük bármelyik ügyfélgépre is, így a rendszergazda saját gépéről is megadhatja a kiszolgálók beállításait. A konzolok telepítéséhez az ügyfélgépen el kell indítanunk a Windows Server telepítőlemezén, az i386 mappában található *adminpak.msi* nevű fájlt. A telepítés után az új konzolokat a Start menü Administrative Tools *(Felügyeleti eszközök)* csoportjában fogjuk megtalálni.

A kiszolgálók alapszolgáltatásai

Ebben a szakaszban megismerkedünk a kiszolgáló számítógépek klasszikus funkcióival: a fájlok és nyomtatók megosztásával. Elsőként áttekintjük a lemezkezeléshez kapcsolódó fogalmakat, megismerkedünk az alap- és dinamikus lemezekkel, a tükrözött, csíkozott, és RAID-5 kötetekkel, a GUID partíciós táblával, az NTFS-tömörítéssel és a hagyományos lemezkvótákkal.

Ezután következnek a fájlok tárolásához, kezeléséhez kapcsolódó kiegészítő szolgáltatások: a Removeable Storage *(Cserélhető tároló)*, a Remote Storage *(Távtároló)* és a Storage Area Network *(Tárolóhálózatok)*.

Szót ejtünk a fájlok megosztásához kapcsolódó alapszolgáltatásokról, a Shadow Copies-ról *(Árnyékmásolat)* és a Distributed File System-ről *(Elosztott fájlrendszer)*. Végül következhetnek az R2 verzióban megjelenő újdonságok: a File Server Resource Manager, FSRM *(Fájlkiszolgálói erőforrás-kezelő)*, és a Print Management Console, PMC *(Nyomtatáskezelő)*.

Fájlkiszolgáló szolgáltatások

Mielőtt hozzálátnánk a fájlkiszolgálók alapszolgáltatásaink ismertetéséhez, feltétlenül tisztáznunk kell, hogy az ügyfélgépeken elérhető megosztott mappák szolgáltatásai közel sem azonosak a kiszolgáló által megvalósítható fájlmegosztással. A fájlkiszolgáló egyrészt a szolgáltatások és felügyeleti lehetőségek szintjén is jelentős többlettel rendelkezik, másrészt a kiszolgáló számítógép jellemzően nagy CPU-teljesítménnyel, sok memóriával, lemezterülettel és hálózati sávszélességgel rendelkezik, vagyis képes sok egyidejű kérés kiszolgálását is megfelelő sebességgel elvégezni.

A fájlkiszolgálók alapszolgáltatásai
Ebben a screencastban áttekintjük a fájlkiszolgálók kezeléséhez kapcsolódó legfontosabb eszközök használatát.
Fájlnév: II-1-1a-fajlszerver-alapok.avi

Ahogyan már korábban említettük, a kiszolgálók esetében természetesen nem érvényes az ügyfél operációs rendszerek fájlmegosztással kapcsolatos korlátozása (maximálisan tíz egyidejű kapcsolat), a kapcsolatok számát csak az ügyfél licencek száma és a kiszolgáló számítógép teljesítménye korlátozza.

Basic Disks *(Alaplemezek)*

A Windows terminológia szerinti alaplemez a hagyományos particionálást és formázást lehetővé tevő lemezmeghajtó-sémát jelenti. Az alaplemezeken elsődleges és kiterjesztett partíciókat, illetve a kiterjesztett partíción belül logikai meghajtókat hozhatunk létre. A partíciókat és logikai meghajtókat kötetnek *(volume)*, illetve alapkötetnek *(basic volume)* nevezzük.

A lemezmeghajtón létrehozható partíciók száma a lemez partíciótípusától függ. A hagyományos, vagyis fő rendszertöltő rekordot *(Master Boot Record, MBR)* használó lemezeken a partíciós tábla maximálisan négy bejegyzést tartalmazhat, vagyis legfeljebb négy elsődleges partíciót, vagy három elsődleges és egy kiterjesztett partíciót lehet rajtuk létrehozni. A logikai meghajtók nyilvántartása már nem a partíciós táblában található, így ezek száma nem korlátozott. A 64-bites rendszereken elérhető GUID partíciós tábla esetén a fenti korlátozások nem érvényesek (lásd később).

NTFS fájlrendszer használata esetén az elsődleges partíciók és logikai meghajtók területe létrehozásuk után is megnövelhető, vagyis a partíció kibővíthető az adott lemezen rendelkezésre álló szabad területtel.

A Windows Server 2003 termékcsaládba tartozó rendszerek nem támogatják a Windows NT 4.0 különféle többlemezes kötettípusait (tükrözött kötetek, különféle csíkkészletek) ilyen struktúrák csak dinamikus lemezek használatával hozhatók létre.

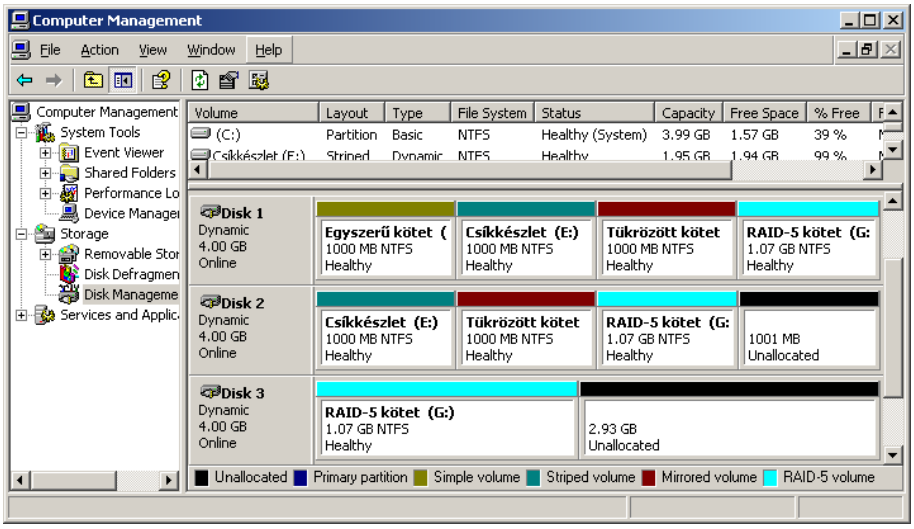
Dinamikus lemezek *(Dynamic Disks)*

A dinamikus lemezek használatával számos olyan szolgáltatást vehetünk igénybe, amelyek az alaplemezek esetében nem érhetők el, a dinamikus lemezeken például több lemezre kiterjedő (átnyúló vagy csíkozott) köteteket, illetve hibatűrő (tükrözött és RAID-5) köteteket is létrehozhatunk. A dinamikus lemezeken elméletben lemezcsoportonként akár 2000 dinamikus kötet is létrehozható, bár az ajánlott maximális kötetszám 32.

A dinamikus lemezeken létrehozható kötetek öt típusba sorolhatók:

- **Egyszerű kötet** *(Simple volume)* – az egyszerű kötetek egyetlen dinamikus lemezen helyezkednek el. Állhatnak a lemez egy meghatározott területéből, illetve a lemez több különálló területét is összekapcsolhatjuk egyetlen dinamikus kötetté. Ha a kötet nem rendszer- vagy rendszerindító kötet, akkor az egyszerű kötet a lemezen belül tetszés szerint bővíthető. Lehetőség van másik lemezre kiterjedő bővítésre is, ám ebben az esetben a bővítéssel együtt az egyszerű kötet átnyúló kötetté alakul. Az egyszerű kötetek nem hibatűrők.

- **Átnyúló kötet** *(Spanned volume)* – az átnyúló kötetek kettő, vagy több fizikai lemezre (dinamikus lemez) terjednek ki. Az átnyúló kötetek mérete tetszés szerint bővíthető bármelyik fizikai lemezen lévő üres terület terhére. Az átnyúló kötetek nem hibatűrők és nem is tükrözhetők.
- **Csíkozott kötet** *(Striped volume)* – a csíkozott kötetek az adatokat két vagy több fizikai lemezen (több fizikai lemez használatával növekszik a teljesítmény) lévő csíkokban tárolják. A több lemezvezérlő és merevlemez miatt az olvasási és írási műveletek ebben az esetben rendkívül jól párhuzamosíthatók, így a Windows operációs rendszerekben használható kötetek közül ez nyújtja a legnagyobb teljesítményt, bár hibatűrést nem biztosít. Ha egy csíkozott kötet valamelyik lemeze meghibásodik, akkor az egész kötet adatai elvesznek. A csíkozott kötetek nem tükrözhetők és nem is bővíthetők.



4.4. ábra: *Különféle dinamikus kötetek a Disk Management (Lemezkezelés) konzolban*

- **Tükrözött kötet** *(Mirrored volume)* – a tükrözött kötetek két fizikai lemezt használnak, ilyen kötet esetén valamennyi adatunk egyszerűen két példányban tárolódik. Ha az egyik tükröt tartalmazó fizikai lemez meghibásodik, és a rajta lévő adatok elérhetetlenné válnak, a másik lemezen található tükörkép használatával a rendszer továbbra is működőképes marad. A tükrözött kötetek bővítése nem lehetséges.
- **RAID-5 kötet** *(Redundant Array of Inexpensive Disks, olcsó merevlemezek redundáns tömbje)* – RAID-5 kötet esetén a tárolt hasznos adat és a helyreállításhoz szükséges paritásadatok három, vagy több fizikai lemezen elosztva tárolódnak. Ha valamelyik fizikai lemez meghibásodik, a

rajta tárolt adatok a másik két lemez adatai és a paritásadatok alapján, egy új merevlemezen helyreállíthatók. A RAID-5 kötetek nem tükrözhetők és nem bővíthetők. A RAID-5 kötetek adatolvasási műveletek esetében jelentősen gyorsabbak például a tükrözött köteteknél, de írás közben a paritásadatok számítása lassítja a műveleteket. Az egyik lemez meghibásodása esetén azonban az olvasási teljesítmény is jelentősen csökkenhet, hiszen ekkor az adatok egy részét a paritásadatok segítségével az olvasási művelet közben kell generálni. A Windows Server 2003 termékcsalád által kínált szoftveres RAID-megoldás esetében a paritásadatok létrehozása és a sérült adatok helyreállítása szoftveresen történik, vagyis a művelet a számítógép processzorát terheli.

Hardveres RAID-megoldások

Hardveres RAID esetén a redundáns adatok létrehozását és a sérült adatok javítását egy önálló, intelligens lemezvezérlő végzi. A hardveres megoldások legfőbb előnye, hogy teljes mértékben mentesítik az operációs rendszert a lemezkezelés feladataitól, sőt az operációs rendszer egyáltalán nem is tud a valós, fizikai lemezkonfigurációról, a Lemezkezelőben általában csak egy közönséges alaplemezt találunk. Az operációs rendszer szintjén megjelenő fizikai lemez tulajdonképpen már csak a RAID-vezérlő által létrehozott logikai lemez, a valóságos fizikai elrendezést a vezérlőkártya eltakarja az operációs rendszer elől. Ebben az esetben a Lemezkezelőben egyáltalán nem célszerű még dinamikus lemezek létrehozása sem, a lemezekkel kapcsolatos valamennyi beállítást a vezérlőkártya szoftveres beállítófelületén kell megadnunk. Hardveres RAID-megoldások olyan rendszerekben is használhatók, amelyek szoftveresen nem támogatják ezek használatát (például Windows XP).

A hardveres RAID-eszközök általában saját BIOS-vezérlőprogrammal, és önálló konfigurációs programmal rendelkeznek. A logikai lemezek létrehozását és a különféle beállítások megadását (csíkozás, tükrözés, RAID-5 stb.) ezekkel a programokkal végezhetjük el.

A hardveres RAID-megoldás további nagy előnye, hogy a tömb valamelyik merevlemezének meghibásodása esetén a csere akár a számítógép leállítása nélkül is elvégezhető *(Hot Swap),* így a különféle karbantartási műveletek nem okoznak kiesést.

Ha a Windowst RAID-vezérlővel felszerelt számítógépre telepítjük, speciális eszközmeghajtó-illesztőprogramra lehet szükség ahhoz, hogy az operációs rendszer elérje a számítógépben lévő lemezeket. A meghajtóprogramot a Windows telepítésének elején, az F6 billentyű megnyomása után telepíthetjük, méghozzá kizárólag hajlékonylemezről. Bizonyos RAID-vezérlők illesztőprogramját a Windows beépítetten tartalmazza, ha ilyet használunk, akkor a fenti probléma nem jelentkezik.

GPT-lemezek

A GPT (GUID Partition Table, *globálisan egyedi azonosítók partíciós táblája)* az EFI (Extensible Firmware Interface, b*ővíthető belső vezérlőprogram-felület)* csatoló által az Itanium-alapú számítógépeken használt lemezparticionálási séma. A GPT számos előnyös tulajdonsággal rendelkezik az MBR-en alapuló particionálással szemben, az ilyen lemezeken például lemezenként akár 128 partíciót is létrehozhatunk, és ezek mindegyike akár 18 exabájt (azaz 18 millió GB) méretű is lehet. A jobb hibatűrés érdekében a partíciós tábla két példányban tárolódik, de – az MBR-particionálású lemezektől eltérően – nem particionálatlan vagy rejtett szektorokban, hanem magukban a partíciókban.

A GPT-lemezek a Windows valamennyi 64-bites változatában használhatók. A GPT-lemezek a Lemezkezelés programban is az MBR-lemezektől jól megkülönböztethető módon, GPT-lemezekként jelennek meg.

NTFS-tömörítés *(NTFS Compression)*

Az NTFS-tömörítés a szokásos tömörítéséi eljárásokkal (zip, rar stb.) szemben teljesen transzparens megoldást biztosít, a tömörített fájlok és mappák kezelése semmiben nem különbözik a szokásostól. Az NTFS-tömörítés segítségével fájlokat, mappákat, és teljes NTFS-meghajtók is tömöríthetők, az ilyen elemeket a könnyebb azonosítás miatt a többitől különböző színnel is megjeleníthetjük. Az NTFS-tömörítés természetesen kissé csökkenti a fájlműveletek sebességét, mivel a fájlok megnyitásakor azokat ki kell tömöríteni, bezáráskor pedig automatikusan újra tömörített állapotba kerülnek.

Az NTFS-eljárással tömörített fájlok és mappák csak addig maradnak tömörítettek, amíg azokat NTFS-meghajtón tároljuk.

A Cserélhető tároló *(Removeable Storage)*

Cserélhető tároló eszköz egy Microsoft Management Console (MMC) beépülő modulként megvalósított kezelőfelületből, egy API-val rendelkező Windows-szolgáltatásból és egy adatbázisból áll. A Cserélhető tároló az adathordozókkal kapcsolatos szolgáltatásokat nyújt az adatkezelő programok számára, és megkönnyíti a különféle adathordozók (szalagok és optikai lemezek) rendszerezését, valamint az ezeket tartalmazó hardveres tárak (például CD-tárak, szalagos meghajtók) kezelését. A Cserélhető tároló segítségével címkéket rendelhetünk az adathordozókhoz, katalogizálhatjuk őket, és nyomon követhetjük használatukat.

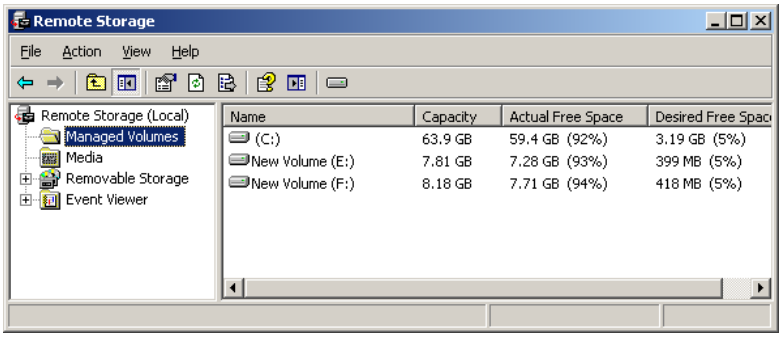
A Cserélhető tároló modul együttműködik az adatkezelő programokkal, például az NTBackup-programmal. Az adatkezelő programok végzik a különböző adathordozókon ténylegesen tárolt adatok kezelését, a Cserélhető tároló pedig lehetővé teszi, hogy ugyanazokat a tároló-erőforrásokat több program megosztva használja.

A Cserélhető tároló a felügyelete alatt álló összes adathordozót adathordozó-készletekbe rendezi. A Cserélhető tároló MMC segítségével az adathordozók áthelyezhetők egyik adathordozó-készletből a másikba, így biztosíthatjuk, hogy az egyes alkalmazások által igényelt adattároló-kapacitás rendelkezésre álljon.

A Távtároló *(Remote Storage)*

A Távtároló a kiszolgáló számítógép lemezterületének jobb kihasználását teszi lehetővé különféle cserélhető adathordozók felhasználásával. A Távtároló szolgáltatás a felügyeletére bízott NTFS-köteteken található ritkán használt fájlokat automatikusan cserélhető adathordozóra másolja, és szükség esetén elő is keresi onnan.

A távtároló szolgáltatás tehát két adattárolási szintet használ. A felső szint, a helyi tároló, a távtároló szolgáltatást futtató számítógépen található NTFS-kötetek közül tartalmazza azokat, amelyekre engedélyeztük a szolgáltatást. Az alsó szint, a távtároló, a kiszolgálóhoz csatlakoztatott automatizált adathordozótáron, szalagos meghajtón vagy lemezmeghajtón található.



4.5. ábra: *A Távtároló felügyeleti konzolja. Külön kell telepíteni!*

Amikor egy adott köteten engedélyezzük a távtároló használatát, meg kell adnunk, hogy a kötet területének hány százalékát szeretnénk szabadon tartani, és azt is, hogy a szolgáltatás hány napnál régebben használt fájlokat kezdjen el a megadott külső tárolóeszközre másolni (megadhatunk egy alsó méretkorlátot is, mivel a nagyon kis fájlokkal nem érdemes foglalkozni, több velük a baj, mint amennyit az elérhető helymegtakarítás ér). Amíg a köteten van elegendő szabad hely, addig a régen használt (és már lemásolt) fájlok megmaradnak az eredeti helyükön is, vagyis ha mégis szükség lenne rájuk, akkor gyorsan elérhetők. Ha viszont a szabad terület a megadott érték alá csökken, akkor a szolgáltatás elkezdi törölni a kötetről azokat a fájlokat, amelyeket már átmásolt a külső tárolóeszközre. A helyileg tárolt adatokat tehát a szolgáltatás csak akkor törli, ha valóban szükség van az általuk elfoglalt területre, viszont a mappalistákban látszólag megmaradnak a törölt fájlok is.

A távtároló által kezelt fájlok minden esetben a szokásos módon kereshetők, és nyithatók meg. Ha a fájl már nincs a merevlemezen, a távtároló szolgáltatás automatikusan előkeresi azt a külső tárolóból és visszaírja az eredeti helyére.

Alapértelmezés szerint a távtároló szolgáltatás nem települ az operációs rendszerrel együtt, de kiválasztható a telepítendő komponensek között, illetve a Control Panel *(Vezérlőpult)* Add or Remove Programs *(Programok telepítése és törlése)* elemének segítségével bármikor telepíthető.

Tárolóhálózatok támogatása

A tárolóhálózatok (*Storage Area Network, SAN)*, a tényleges tárolási kapacitást biztosító lemezmeghajtó-alrendszerekből, a köztük lévő speciális hálózatból, és a számítógépek kapcsolódását lehetővé tevő elemekből állnak. A merevlemezeket tartalmazó alrendszerek között igen gyors hálózati kapcsolat van, a kiszolgálók számára pedig elméletben a teljes tárolókapacitás egyetlen darabban elérhető. Jól megtervezett hálózat esetén a sebesség és a jó kapacitás-kihasználás mellett előny lehet a megnövekedett biztonság is, mivel a tárolóhálózat egyes elemei akár földrajzilag is elkülöníthetőek egymástól, így megfelelő redundancia esetén előre nem látható katasztrófa bekövetkeztekor is garantálhatja az adatok biztonságát.

A kiszolgálók és a tárolóeszközök közötti kapcsolat általában az SCSI vagy a Fibre Channel *(szálcsatorna)* interfészeken alapul, de mindkettőnek létezik TCP/IP-felületet használó változata is. Az iSCSI csatolófelület segítségével az SCSI-parancsok TCP/IP-hálózaton vihetők át, így lehetővé válik a nagy kiterjedésű SAN-hálózatok létrehozása. A tárolóhálózat kiépítése általában viszonylag nagy költséggel jár, de a hagyományos megoldásokhoz képest rugalmasabban használható, nagyobb kihasználtsággal üzemelhet és jobban bővíthető.

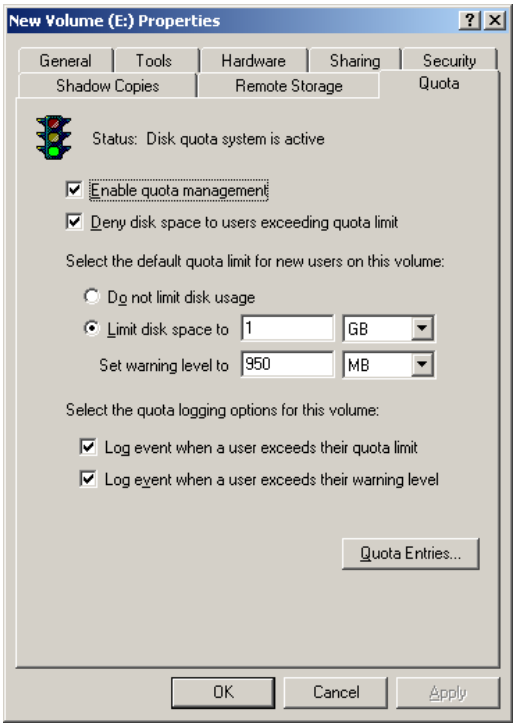
A SAN saját lemezvezérlővel rendelkezik, ami eltakarja a lemezek fizikai paramétereit, így azok a kiszolgálók számára logikai egységekként *(Logical Unit Number, LUN)* érhetők el. A logikai egységek tulajdonképpen a tárolási alrendszerek egyes részeire mutató hivatkozások. Egy logikai egység állhat egy teljes lemezből, egy lemezrészből, egy teljes lemeztömbből vagy a lemeztömb egy részéből. A Tárolóhálózati tárkezelő *(Storage Manager for SANs)* a tárolóhálózat szálcsatornás és iSCSI rendszerű lemezmeghajtó-alrendszereihez tartozó logikai egységek létrehozására és kezelésére szolgál.

Lemezkvóták *(Disk Quota)*

A lemezkvóták segítségével nyomon követhetjük és korlátozhatjuk a felhasználók által elfoglalt lemezterületet. A kvótákat kötetenként (csak NTFS fájlrendszer esetén) engedélyezhetjük az adott kötet tulajdonságlapján.

A következő leírás a „hagyományos”, R2 előtti kvótarendszerre vonatkozik. Az R2-ben megjelent mappa alapú kvótázás (amelyet később szintén bemutatunk) lényegesen jobban és rugalmasabban használható. Az R2-ben megmaradt azonban a „régi” kvótarendszer is.

Miután egy köteten engedélyezzük a kvótahasználatot, a rendszer folyamatosan nyomon követi az elfoglalt terület nagyságát, és a beállított határértékek elérésekor naplózza az eseményt, illetve a beállításoktól függően az adott felhasználó számára megakadályozza a további helyfoglalást.

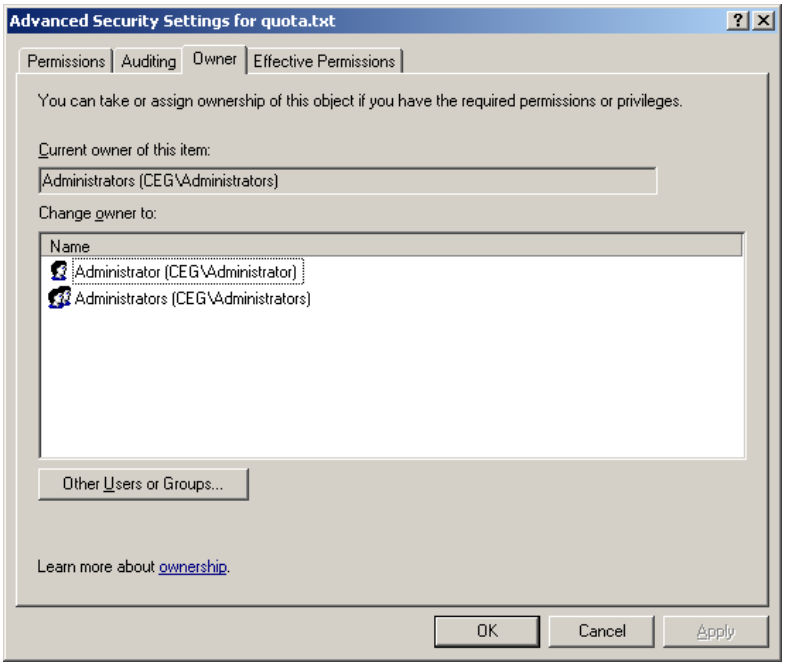


4.6. ábra: *A kvótahasználat engedélyezése és beállításai*

A lemezkvóták engedélyezésekor két értéket adhatunk meg: a lemezhasználat felső korlátját, és a kvótához tartozó figyelmeztetési szintet. Ha például a felhasználó korlátját 1 GB-ra, a figyelmeztetési szintet pedig 950 MB-ra állítjuk, akkor a korlát elérése előtt figyelmeztető üzenet kerül az Eseménynaplóba, bár sajnos, maga a felhasználó erről nem kap semmiféle tájékoztatást. Az adott kötet tulajdonságlapjának megjelenítésekor viszont a felhasználók a kvótának megfelelően módosított értékeket láthatják a Kapacitás, Foglalt terület és Szabad terület mezőkben, vagyis az 1 GB kvótával korlátozott felhasználó a kötet teljes méretét 1 GB-nak látja, annak valódi méretétől függetlenül. A 4.6. ábrán

látható beállítólapon megadott értékek minden felhasználóra egységesen vonatkoznak, de a Quota Entries *(Kvótabejegyzések)* gomb megnyomásával megjeleníthető listában már egyedileg módosíthatjuk a felhasználókra vonatkozó határértékeket, és ellenőrizhetjük az aktuális területfoglalást.

Megadhatjuk azt is, hogy a felhasználók túlléphessék a beállított kvótát. Ennek akkor van értelme, ha nem akarjuk ugyan korlátozni a lemezhasználatot, de szeretnénk folyamatosan figyelemmel kísérni az egyes felhasználók által elfoglalt területet.



4.7. ábra: *Minden fájl a tulajdonos kvótáját terheli, de a rendszergazdának többnyire nincs félnivalója☺*

Fontos hangsúlyozni, hogy a korlátozás az egy adott felhasználó által a kvótával védett köteten tárolt fájlok összesített méretére vonatkozik, függetlenül attól, hogy a fájlok melyik mappában vannak. A fájl annak a felhasználónak a kvótáját terheli, aki a fájl tulajdonosa, vagyis aki létrehozta azt a köteten (például átmozgatta oda egy másik kötetről). Egy fájl tulajdonosát a fájlhoz tartozó tulajdonságlap Biztonság *(Security)* lapján, a Speciális *(Advanced)* gomb megnyomásával jeleníthetjük meg.

Az NTFS-tömörítés használatával a felhasználók nem kerülhetik el kvótájuk túllépését, mivel a tömörített fájlokat a rendszer a tömörítetlen méretük alapján számítja be az összesítésbe.

Árnyékmásolatok *(Shadow Copies)*

Az árnyékmásolatokkal kapcsolatos beállítási lehetőségek
Ebben a screencastban engedélyezzük és beállítjuk az árnyékmásolatok szolgáltatást a kiszolgálón, illetve bemutatjuk az ügyféloldali nézetet is, vagyis visszaállítunk segítségével néhány törölt fájlt.
Fájlnév: II-1-1b-arnyekmasolatok.avi

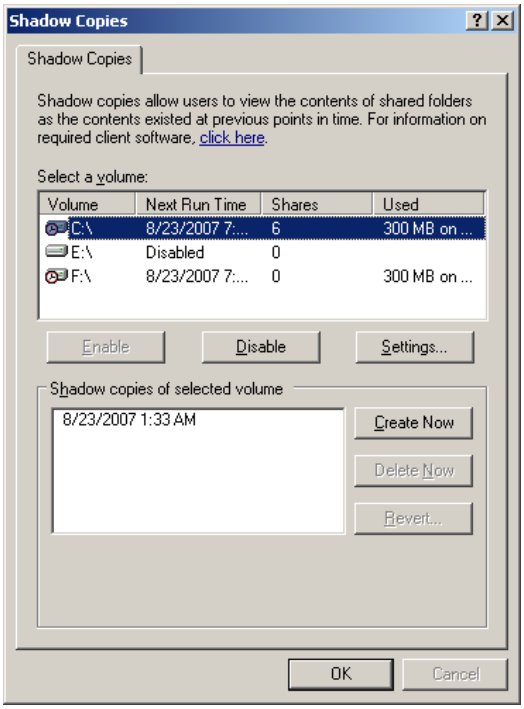
A megosztott mappák árnyékmásolatai a megosztott erőforrásokon (például fájlkiszolgálón) tárolt fájlok esetében a felhasználók által kezelhető, egyszerű visszaállítási lehetőséget biztosítanak. A szolgáltatás segítségével a megosztott fájlok múltbeli állapotait jeleníthetjük meg, illetve állíthatjuk vissza. A korábbi változatok elérésének lehetősége a következő esetekben lehet hasznos:

- **Véletlenül törölt fájlok visszaállítása** – A törölt fájlok korábbi változatai megnyithatók és újra elmenthetők.
- **Véletlenül felülírt fájl helyreállítása** – A véletlenül felülírt fájlok korábbi változatai az árnyékmásolatok között még megtalálhatók.
- **Fájlok különböző változatainak összehasonlítása** – A túlszerkesztett fájlok korábbi változatai közül a felhasználók kiválaszthatják azt az állapotot, amikor a fájl még megfelelő volt.

Miután engedélyezzük egy köteten az árnyékmásolatok készítését, meg kell adnunk, hogy a rendszer mekkora területen tárolhatja a fájlok korábbi változatait. Ha ezután töröljük, vagy módosítjuk, és elmentjük a kötet valamelyik fájlját, a törlés, illetve mentés tényleges elvégzése előtt a régebbi változat az árnyékmásolatok számára lefoglalt területre kerül.

Az árnyékmásolatok beállításai között meg kell adnunk egy ütemezést (alapértelmezés szerint reggel 7 és déli 12 óra), de ez nem a tényleges másolást jelenti, hanem csak azt, hogy a megadott időpontoknál régebbi fájlok és mappák minősülnek korábbi változatnak. Vagyis például reggel 7 és 12 között akárhányszor is mentünk el újra egy fájlt, nem készül minden esetben újabb árnyékmásolat. Az alapértelmezett időzítés tehát azt határozza meg, hogy naponta legfeljebb két előző változatunk keletkezhet (persze ennyi is csak akkor, ha a fájl valóban módosult a megadott időpontok között). Minden egyes árnyékmásolat készlet a beütemezett időpontok között megváltozott fájlok előző változatát tartalmazza. A szolgáltatás maximálisan 64 darab ilyen készlet tárolására képes, ha túllépjük ezt a számot, akkor a legrégebbi másolatok törlődnek.

Ha gyakrabban van szükségünk az árnyékmásolatok elkészítésére, akkor beállíthatunk például óránkénti időzítést is, de ebben az esetben sokkal hamarabb el fogjuk érni a maximális 64 fájlmásolatot, vagyis a régebbi változatok rövidebb idő után kezdenek törlődni.



4.8. ábra: *Az árnyékmásolatok engedélyezése és tiltása*

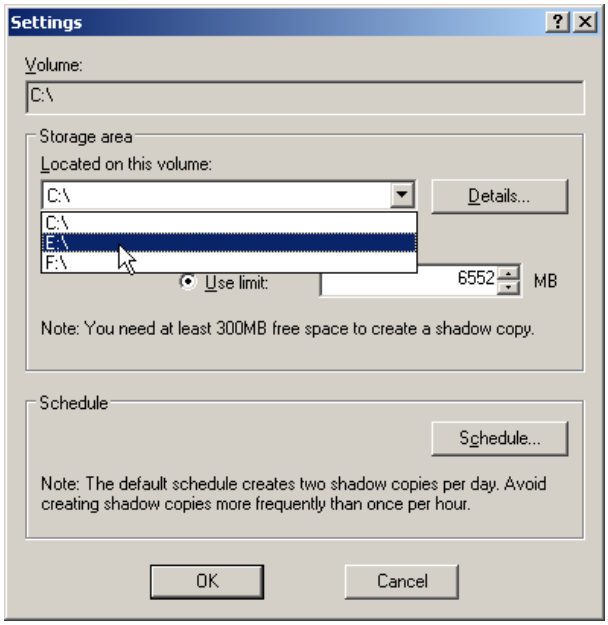
Eszközmeghajtók frissítésekor az árnyékmásolatok szolgáltatás menti a meghajtó előző állapotát, ez teszi lehetővé, hogy az eszközmeghajtók kezelésénél vissza tudjunk térni egy korábbi változatra *(Driver Rollback)*. Biztonsági mentések készítésekor az árnyékmásolatok segítségével menthetjük el a megnyitott fájlokat – legalábbis azok korábbi verzióját.

Az árnyékmásolat szolgáltatás kiszolgáló oldali beállításait a lemezmeghajtó Tulajdonságok *(Properties)* paneljének Árnyékmásolatok *(Shadow Copies)* lapja segítségével adhatjuk meg, illetve ugyanez a beállítólap elérhető a Számítógép-kezelés *(Computer management)* konzolból is.

Az árnyékmásolat készítése csak teljes kötetekre engedélyezhető és tiltható, azaz nem lehet csak a kötet bizonyos megosztott mappáinak és fájljainak másolását beállítani. Ennek megfelelően a beállítólapon elsőként ki kell választanunk azt a kötetet, amelyre a további műveletek vonatkozni fognak.

A kiválasztott kötetre engedélyezhetjük, illetve tilthatjuk az árnyékmásolatok létrehozását, a Készítés most *(Create Now)* gombra kattintva pedig nem készítünk másolatokat, csak azt állítjuk be, hogy mostantól a változásokról (ha vannak változások) újra készüljön egy árnyékmásolat-példány. Lehetőség van a már meglévő másolatok törlésére is.

A Beállítások *(Settings)* gombra kattintva megadhatjuk a kiválasztott kötetre vonatkozó méretkorlátozásokat, és átállíthatjuk az alapértelmezett ütemezést.



4.9. ábra: *A C:\ kötet árnyékmásolatának beállításai*

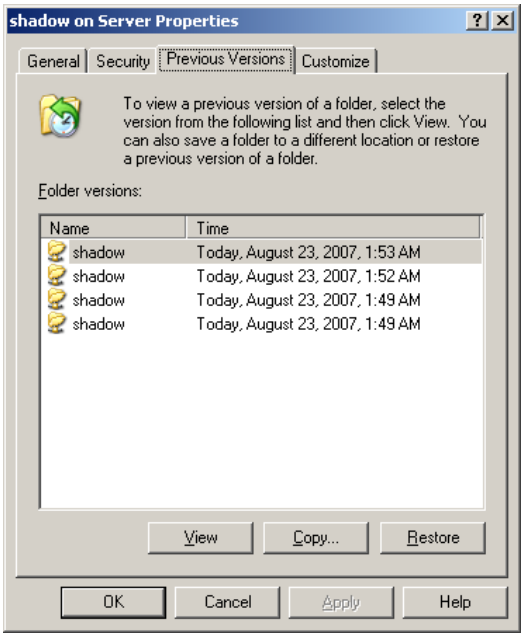
Komolyabb használat esetén mindenképpen érdemes tárolóterületként olyan önálló kötetet (még jobb, ha az külön fizikai meghajtón is van) megadni, amelyről nem készül árnyékmásolat, így jelentősen nagyobb teljesítmény érhető el. Ezt a beállítást azonban csak addig tehetjük meg, amíg nincsenek engedélyezve a kötet árnyékmásolatai, a korábban létrehozott árnyékmásolatok áthelyezésére nincsen lehetőség.

Ha meglévő fájl régebbi változatát állítjuk vissza, annak hozzáférési engedélyei nem változnak, meg fognak egyezni az eredeti fájllal. Ha törölt fájlt állítunk vissza, az arra vonatkozó engedélyek a mappa alapértelmezett engedélyei lesznek.

Természetesen az árnyékmásolatok szolgáltatás használata nem helyettesítheti, de jól kiegészítheti a rendszeres biztonsági mentéseket.

Régebbi ügyfélrendszerek esetén az árnyékmásolat szolgáltatás használatához szükség van a megfelelő ügyfélszoftver telepítésére is, de a Windows XP és Windows Vista rendszerekben a szoftver gyárilag benne van. Ha mégis szükség lenne az ügyfélprogramra, a telepítőt a kiszolgáló *%SYSTEMROOT%\system32\clients\twclient* mappájában találhatjuk meg.

Az árnyékmásolatok ügyféloldali nézetét a megosztott mappához tartozó Tulajdonságok *(Properties)* panel Előző verziók *(Previous Versions)* lapján érhetik el a felhasználók.



4.10. ábra: *Az árnyékmásolatok ügyféloldali nézete*

Itt a megjelenő dátum és idő alapján kiválasztható a mappa elérhető árnyékmásolatai közül a megfelelő, amellyel a következő műveletek végezhetők el:

- **View** *(Megtekintés)* – a másolat egy külön ablakban nyílik meg, így megtekinthető annak tartalma, és összehasonlítható a jelenlegi állapottal.
- **Copy** *(Másolás)* – a másolat kimenthető a kiválasztott mappába, így megmarad a jelenlegi változat is.
- **Restore** *(Visszaállítás)* – a gomb megnyomása után a kiválasztott másolat felülírja a mappa jelenlegi változatát.

Az elosztott fájlrendszer *(Distributed File System, DFS)*

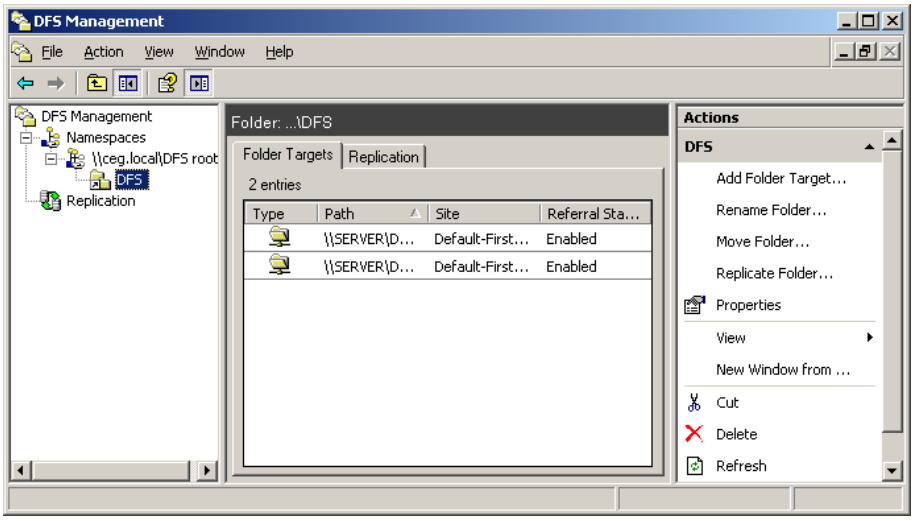
A DFS tulajdonképpen egy virtuális könyvtárfa, amely a különböző fájlkiszolgálókon található megosztásokat egyetlen névtérbe rendezi, vagyis a felhasználók egyetlen pontból kiindulva, összefüggő fájlrendszerként érhetik el a DFS-be felvett valamennyi megosztott mappát. A DFS alkalmazásával a kiszolgálókon tárolt fájlok úgy jeleníthetők meg a felhasználóknak, mintha azok a hálózat egyazon helyén lennének, a fájlok eléréséhez tehát nincsen szükség azok valódi helyének ismeretére.

További igen előnyös tulajdonság, hogy egy megosztott mappa fizikai helyének módosításakor a felhasználói élmény érintetlen marad, vagyis a felhasználók ugyanúgy érhetik el a mappát, mint azelőtt, hiszen annak elérési útja a DFS-névtéren belül nem változik. A rendszergazda által meghatározott logikai neveket a DFS-szolgáltatás fordítja el a fizikai megosztások neveire, a virtuális névtér stabil és állandó.

Az elosztott fájlrendszer szolgáltatás jelentős változáson ment keresztül az R2 verzióban, többek között megújult a felügyeleti felület is. Az új konzolt az Administrative Tools *(Felügyeleti eszközök)* csoportban találjuk DFS Management *(Elosztott fájlrendszer kezelése)* néven. A konzol segítségével hozhatjuk létre a DFS-névtereket, amelyek a virtuális és fizikai mappák összerendelését tartalmazzák. A névterek hierarchiáját mappák létrehozásával alakíthatjuk ki. Minden DFS-mappához valódi, fizikai mappapéldányok tartoznak (egy virtuális DFS-mappához több, akár különböző kiszolgálón elhelyezkedő fizikai mappát is hozzárendelhetünk), az ügyfelek a DFS-mappákból álló névtérben tallózva, a háttérben, titokban megkapják a szükséges átirányítást a megfelelő fizikai mappa eléréséhez. Az ügyfelek számára prioritásokat is meghatározhatunk, vagyis megadhatjuk, hogy egy adott virtuális mappát melyik fizikai mappapéldány szolgáljon ki elsősorban. Ha az előnyben részesített kiszolgáló éppen nem érhető el, akkor az ügyfél természetesen a többi mappapéldányt is használhatja, de a hiba elhárítása után újra vissza fog találni a neki kiosztott kiszolgálóhoz. A fizikai mappák tartalmának szinkronizálásáról a DFS replikációs szolgáltatása gondoskodik (lásd később).

Minden DFS-mappához tehát a hálózat különböző helyein lévő fizikai mappák tartozhatnak, vagyis a gyakran használt, nagy adatforgalmat bonyolító mappákat párhuzamosan több kiszolgáló is kezelheti, így a terhelés elosztásával nagyobb teljesítményt érhetünk el.

Az elosztott fájlrendszer a fizikai mappákhoz tartozó szabványos NTFS- és fájlmegosztási engedélyeket használja, így a már meglévő biztonsági csoportok és felhasználói fiókok segítségével a szokásos módon szabályozhatjuk a hozzáférési jogokat.



4.11. ábra: *Tartományi névtér a DFS-konzolban*

Az elosztott fájlrendszer alapvetően két üzemmódban működhet:

- **Különálló névtér** *(Stand-Alone Namespace)* – ebben az esetben a DFS-névtér szerkezetére vonatkozó minden adatot maga a kiszolgáló tárol. Különálló névtér esetén az egyes DFS-mappák hivatkozásai a kiszolgáló nevével kezdődnek, vagyis az elosztott fájlrendszer például a következő módon érhető el: *SERVER**DFS*. Különálló névtér esetén maga a névtér nem hibatűrő, így a névteret tároló kiszolgáló nem érhető el, akkor a teljes DFS-fa hozzáférhetetlenné válik.
- **Tartományi névtér** *(Domain-based Namespace)* – ebben az esetben az elosztott fájlrendszer topológiai adatait az Active Directory tárolja, vagyis azok minden tartományvezérlőn megtalálhatók. A DFS névtér elérése nem egy konkrét számítógépre, hanem a tartomány nevére való hivatkozással lehetséges, vagyis a következő módon: \\ceg.local\DFS. Mivel az adatok több tartományvezérlőn is megtalálhatók, ez a megoldás a névtér szintjén is hibatűrést biztosít.

Az elosztott fájlrendszer használata a következő esetekben jelenthet jó megoldást:

- Ha várhatóan új fájlkiszolgálók telepítésére, vagy a meglévők cseréjére lesz szükség.
- Ha a felhasználók sok megosztott mappához szeretnének hozzáférni.

- Ha a nagy forgalmú megosztott mappák miatt terhelésmegosztásra van szükség.
- Ha folyamatos (hibatűrő) hozzáférést kell biztosítanunk a megosztott mappákhoz.
- Ha a távoli telephelyek és a központban lévő kiszolgálók között biztonságos és nagyon kis sávszélességet igénylő fájlreplikációra van szükség.

Az elosztott fájlrendszer replikációja

Az elosztott fájlrendszer replikációja *(Distributed File System Replication, DFS-R)* gondoskodik arról, hogy a fizikai mappák tartalma a több helyen történő módosítás ellenére is megfelelő módon szinkronban maradjon. A DFS-R multimaster *(több főkiszolgálós)* replikációs modellt használ, vagyis valamennyi mappapéldány módosítható, az adatok átviteléhez pedig rendkívül alacsony sávszélesség is elegendő lehet. Az adatok átvitele az általunk megadott időközönként történik meg, nem a fájlok megváltozása váltja ki azt. A replikáció ütemezésekor minimálisan 15 perc, maximálisan pedig 7 nap frissítési időközt adhatunk meg, és meghatározhatjuk a szolgáltatás által igénybe vehető sávszélességet is (minimum 16 kbit/sec). A replikációban részvevő mappákat nem kell feltétlenül megosztani, vagyis nem kell feltétlenül részt venniük a DFS-szolgáltatásban sem (hiszen a DFS-névtérbe csak megosztott mappákat csatolhatunk be). A DFS-R-szolgáltatás tehát kiválóan felhasználható (DFS nélkül is) tetszőleges mappák sávszélesség-takarékos replikációjára, például egy távoli telephely fájlkiszolgálója és a központban lévő, biztonsági mentéseket végző kiszolgáló között. A globális replikációs beállításokat az Active Directory tárolja.

Az adatok átviteléhez a DFS-R a Remote Differential Compression *(távoli különbségi tömörítés, RDC)* technológiát használja. Az RDC minden fájlt változó nagyságú (a tartalomtól függően) részekre, úgynevezett chunkokra darabol, majd minden egyes darabkához MD4 hasht, vagyis gyakorlatilag egy egyedi ujjlenyomatot készít. Ha a fájl egy adott része megváltozik, akkor természetesen megváltozik az adott töredékhez tartozó ujjlenyomat is, az RDC pedig ez alapján azonosítja a fájlokon belüli változásokat. A replikáció során a töredékekhez tartozó ujjlenyomatok összehasonlításával az RDC meghatározza, hogy melyik darabok különböznek egy adott fájlon belül, és a hálózaton csak a megváltozott (a teljes fájlhoz képest általában minimális méretű) töredékeket mozgatja, a megváltozott fájl pedig a helyben már meglévő változatlan, és a hálózaton érkező frissített darabokból áll össze.

Ez tehát azt jelenti, hogy a replikáció nem a teljes fájlok, hanem a viszonylag kisméretű chunkok szintjén történik, vagyis az RDC tulajdonképpen nem a fájlokat, hanem csak a változást replikálja. Sőt az RDC még arra is képes, hogy ha több fájlon belül vannak azonos töredékek (például egy kissé módosított és más néven elmentett fájl esetén), akkor a változatlan töredékeket a teljesen új fájlok létrehozásához is felhasználja. A nagy fájlok módosításai (például egy Outlook postafiókfájl *(pst)* esetén) általában csak néhány töredéket érintenek, vagyis ilyen módon igen jelentős sávszélesség megtakarítás érhető el.

A Microsoft mérései szerint például egy 3,5 MB-os PowerPoint-bemutató egyik címsorának megváltoztatása utáni replikáció a teljes fájl másolásával járó 3,5 MB forgalom helyett mindössze 16 kB hálózati forgalmat eredményezett. A DFS-R tartományvezérlők esetén nem váltja ki a fájlreplikációs szolgáltatást *(File Replication Service, FRS)*, hanem vele párhuzamosan működik.

A fájlkiszolgáló újdonságai: az FSRM

A fájlok központi tárolása alapvető igény minden számítógépes rendszerrel szemben. Az adatok mennyiségének (és fontosságának) növekedésével a rendszergazdáknak egyre összetettebb tárolási struktúrát kell áttekinteniük, ráadásul a viszonylag drága, és többnyire szűkös központi tárolási kapacitással való hatékony gazdálkodáshoz folyamatosan figyelemmel kell(ene) kísérniük a felhasználók által tárolt fájlok mennyiségét, sőt lehetőleg azt is, hogy minden állomány esetében indokolt-e a központi tárolás.

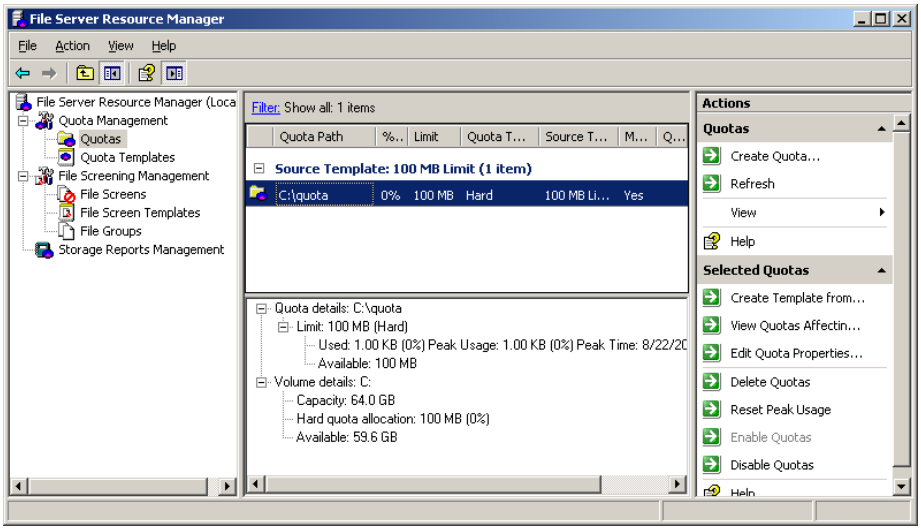
A Windows Server 2003 R2 változatában megtalálható File Server Resource Manager *(Fájlkiszolgálói erőforrás-kezelő)* olyan eszközkészletet ad a rendszergazdák kezébe, amelynek segítségével a központilag tárolt adatok mennyiségét és típusát is szoros ellenőrzés alatt tarthatják. Az új szolgáltatások három témához kapcsolódnak:

- **Quota Management** *(Kvótakezelés)* – a korábbi kvótarendszert kiegészítő, szemléletében teljesen új kvótarendszer.
- **File Screening Management** *(Fájlszűréskezelés)* – az egyes mappákban tárolható fájltípusokat (a fájlok neve, illetve kiterjesztése alapján) korlátozó szabályokat adhatunk meg.
- **Storage Reports Management** *(Tárolási jelentések kezelése)* – részletes jelentéseket kaphatunk az állományokról, a lemezhasználatról, a foglaltságról stb.

A fájlkiszolgálói erőforrás-kezelő használata
Ebben a screencastben kipróbáljuk a fájlkiszolgálói erőforrás-kezelő segítségével beállítható új szolgáltatásokat: általunk készített sablonok alapján beállítjuk a felhasználók mappáira vonatkozó kvótát, korlátozzuk a tárolható fájlok körét és részletes jelentéseket készítünk a fájlkiszolgáló állapotáról.
Fájlnév: II-1-1c-FSRM.avi

Kvótakezelés

A Windows Server 2003 R2 verziójának egyik újdonsága a mappa alapú kvótázás lehetősége. Az új kvótarendszerrel az egyes mappák méretét korlátozhatjuk a benne lévő fájlok tulajdonosától függetlenül.

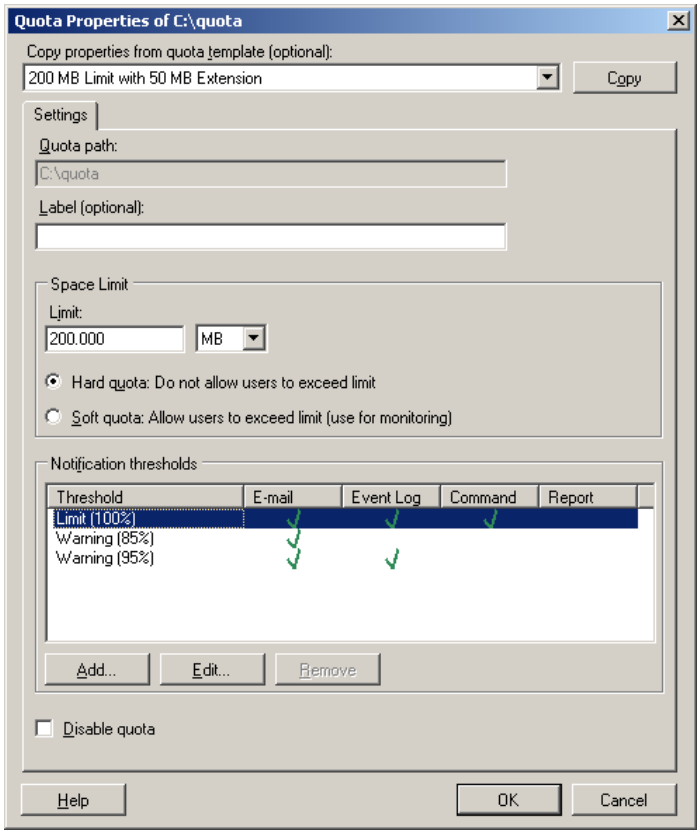


4.12. ábra: *A lemezhasználat korlátozása az egyes mappák által elfoglalható területre vonatkozik*

A tárterület limitálása tehát ebben az esetben nem kötetenként és felhasználónként, hanem az egyes mappák szintjén történik. Minden mappához hozzárendelhetünk egy limitet, ami a mappába helyezhető fájlok (és almappák) összesített méretének felső korlátja lesz.

A határértékeknek két típusát adhatjuk meg: a szigorú *(Hard)* kvóta tényleges korlátozást jelent, míg az enyhe *(Soft)* határérték az elfoglalható terület tényleges limitálása nélkül aktiválja a határértékhez rendelt eseményeket, vagyis a területhasználat megfigyelésére alkalmas.

A kvótarendszer szorosan együttműködik az NTFS fájlrendszerrel, így természetesen csak NTFS-köteteken használható.



4.13. ábra: *A kvóta tulajdonságainak beállítása (célszerű a „sablonos” megoldást választani)*

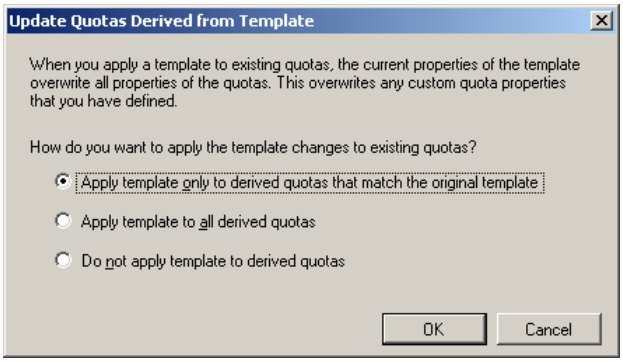
Hard kvóta esetén a határérték elérésekor az I/O-műveletek szintjén akadályozza meg a további helyfoglalást, vagyis a kvóta túllépése a legkisebb mértékben sem lehetséges. A kvóta nem a fájlok logikai méretét, hanem minden esetben az adott mappán belüli tényleges lemezfoglalást veszi alapul, vagyis a különféle speciális állományok (tömörített fájlok, hard linkek, felcsatolt mappák) beszámítása is ennek alapján történik.

Minden egyes határérték esetén, a határérték százalékaként adhatjuk meg azokat a foglaltsági szinteket, amelyek elérésekor a beállítható tevékenységek valamelyikét el szeretnénk végezni. Az eseményekhez kapcsolható tevékenységek a következők lehetnek:

- E-mail küldése a rendszergazdának, illetve az eseményt kiváltó felhasználóknak. A felhasználók esetében a rendszergazda adhatja meg az elküldendő levél szövegét is.
- Eseménynapló bejegyzés készítése.

- Megadott program, illetve szkript futtatása. Ilyen módon érhetjük el például azt, hogy a határérték elérésekor a kvóta megemelkedjen; a dirquota.exe parancssori segédprogramot kell elindítanunk a megfelelő paraméterezéssel.
- Tárolási jelentés *(Storage Report)* generálása (lásd később).

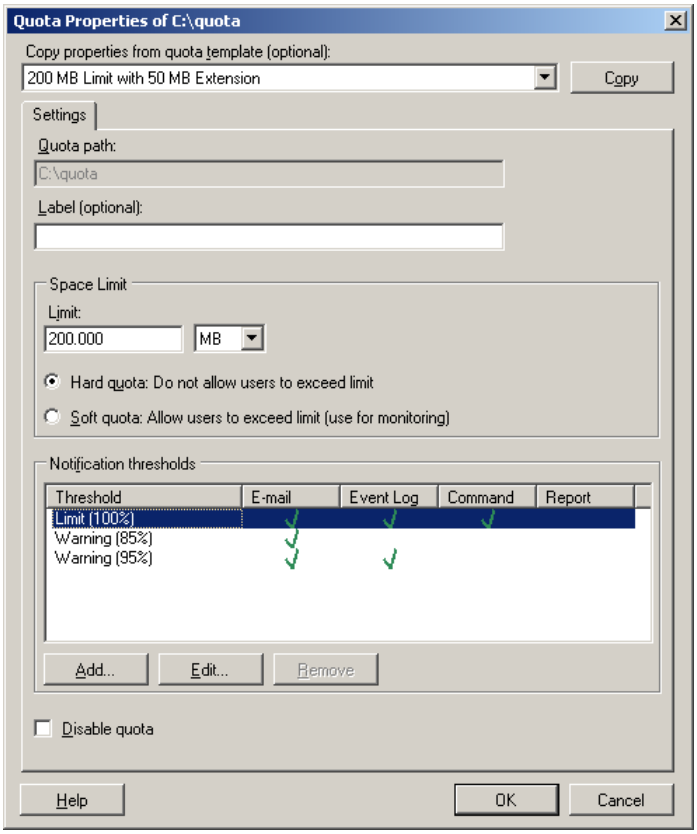
Valamennyi beállítást sablonként is elmenthetjük, hogy később, illetve másik mappa esetén már csak egyetlen mozdulat legyen a megfelelő beállításcsoport alkalmazása. Természetesen kapunk előre elkészített mintákat is, ezeket kissé módosítva (esetleg ezután új névvel elmentve) könnyen előállíthatjuk az igényeinknek megfelelő sablont, ami jelentősen megkönnyíti és meggyorsítja a beállítások megadását. Lehetőség van a sablonok exportálására és másik gépen való importálására is.



4.14. ábra: *A kvótákat eredeti sablonjuk módosításával is megváltoztathatjuk*

A „sablonos” módszer használata azért is ajánlott, mert a sablon módosításakor lehetőségünk van arra, hogy ezt a módosítást utólag érvényesítsük a sablon alapján létrehozott kvótákra is. Módosíthatjuk csak azokat a kvótákat, amelyek teljesen megfelelnek az eredeti sablonnak (vagyis amelyikben nincsenek egyedi módosítások), de hozzáigazíthatjuk az összes kvótát sablonjának változásaihoz. Ha így döntünk, akkor a sablonban megadott beállításokkal felülírhatunk minden egyedileg megadott kvótatulajdonságot (nem csak azokat, amelyeket a sablonban módosítottunk).

A mappák korlátját rugalmas (vagyis határérték eléréséhez rendelt parancs által ideiglenesen megnövelt) korlátként is megadhatjuk, így az érintett felhasználók e-mailben értesítést kaphatnak a túllépésről, és azonnal nekiláthatnak a szükségtelen fájlok törlésének.



4.15. ábra: *A határérték elérésekor lefutó parancs akár a kvótát is megnövelheti, vagyis adhat még egy kis haladékot*

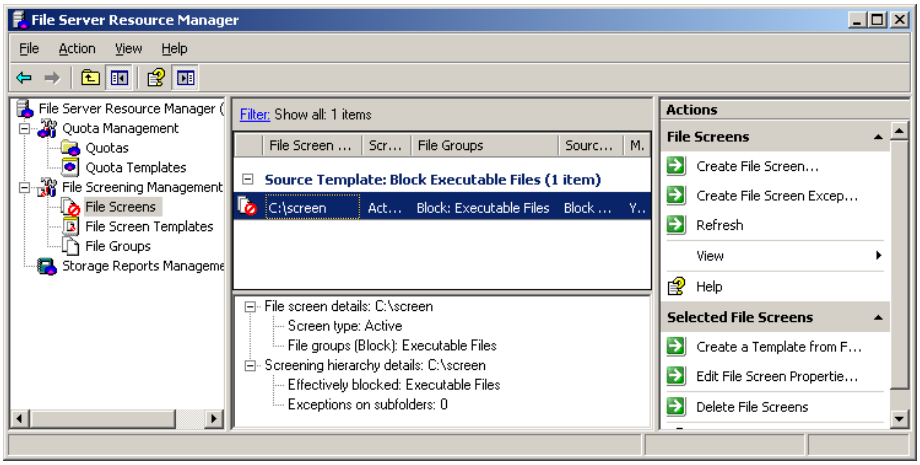
Beállíthatjuk azt is, hogy a rendszer ne korlátozza ugyan egy mappa méretét, de küldjön értesítést egy megadott e-mail címre, ha a méret elér egy meghatározott értéket. Nem célszerű például a különféle szolgáltatásokhoz tartozó ideiglenes mappák méretét korlátozni (mert esetleg egy csendes hétvégén emiatt leállhat az adott szolgáltatás), de fontos lehet, hogy a rendszergazda azonnal tudomást szerezzen róla, ha a mappa mérete a szokásos és elfogadható érték fölé emelkedik.

Az új kvótarendszer természetesen nemcsak a régi helyett, hanem mellette is használható, akár ugyanarra a tárterületre is érvényesülhet mindkét korlátozási szemlélet.

Fájlok szűrése *(File Screening)*

A fájlszűrés segítségével kötet, illetve mappaszinten korlátozhatjuk a tárolható fájlok típusát, vagyis meghatározhatjuk, hogy egy mappában a megadott típusú (például végrehajtható fájlok, vagy mozgóképek) fájlokat ne tárolhassák a felhasználók. A tiltott fájltípusokat az adott mappában sem létrehozni, sem odamásolni (vagy mozgatni) nem lehet. A tiltólista ellenőrzése a fájlműveleteket megelőzően történik, vagyis azok a fájlok, amelyek már a tiltás bevezetésekor is a mappában voltak, természetesen továbbra is ott maradhatnak.

A fájlok típusának meghatározása a fájl kiterjesztése, (illetve a fájlnévben tetszőleges helyen megtalálható minta) alapján történik, tehát az átnevezett, vagy például zippelt állományok másolását a szűrő nem akadályozza meg.



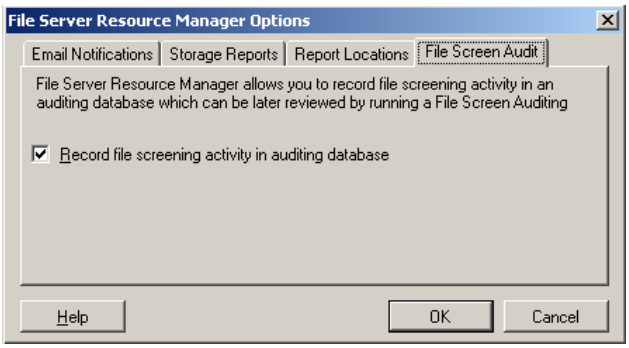
4.16. ábra: *A mappában tilos bármiféle végrehajtható fájl tárolása*

A tiltást fájlcsoportok alapján adhatjuk meg, a végrehajtható fájl kategóriába például számos kiterjesztés tartozik *(exe, com, bat, cmd, vbs* stb.), de valamennyi fájlcsoport szerkeszthető is, vagyis magunk határozhatjuk meg, hogy egy fájltípushoz milyen konkrét fájlnévminták tartozzanak. Természetesen, a meglévőkön kívül új típusokat is definiálhatunk, így tetszőleges kiterjesztéseket válogathatunk össze. Lehetőségünk van helyettesítő karakterek használatára is, vagyis például akár azt is beállíthatjuk, hogy egy mappában ne lehessen olyan fájlokat tárolni, amelyek nevének második betűje „a” (?a*). Persze egy ilyen korlátozás gyakorlati haszna legalábbis megkérdőjelezhető.

A korlátozások a kvótákhoz hasonlóan ebben az esetben is két különböző módon adhatók meg:

- Az **aktív szűrés** *(Active Screening)* valódi korlátozást jelent, a tiltott fájlok ebben az esetben nem kerülhetnek a kötetre, illetve mappába.
- A **passzív szűrés** *(Passive Screening)* a fájlok megfigyelésére szolgál, vagyis nem tiltja a fájlok létrehozását, de a megfigyelt fájlok megjelenése kiváltja a rendszergazda által meghatározott tevékenységek végrehajtását.

Természetesen a kvótákhoz hasonlóan a beállításcsoportokat itt is sablonok segítségével adhatjuk meg, és a különféle értesítések (Eseménynapló, e-mail, tárolási jelentések) és tevékenységek (szkript vagy program futtatása) is megegyeznek a kvótákkal kapcsolatban már megismert lehetőségekkel. Egyetlen lényeges különbség van: a fájlszűréssel kapcsolatos eseményeket a rendszer alapértelmezés szerint nem tárolja, vagyis ezek nem fognak szerepelni a megfelelő tárolási jelentésben sem. Az események tárolását az FSRM beállítólapján (jobb egérgomb -> Configure Options) kell engedélyeznünk.



4.17. ábra: *A fájlszűréssel kapcsolatos események tárolását külön kell engedélyezni*

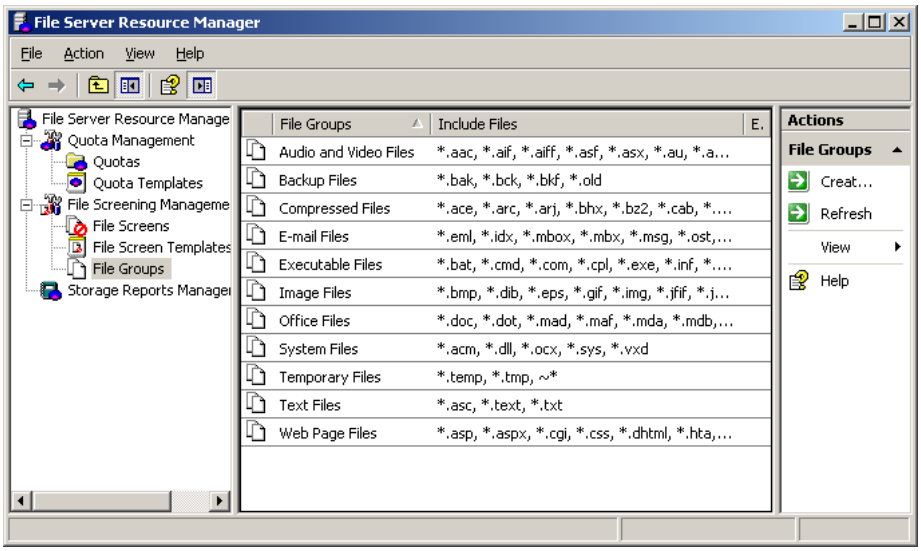
Az FSRM felületén számos alapértelmezett fájlszűrősablont találhatunk, amelyek segítségével megtilthatjuk a hang- és mozgóképfájlok, végrehajtható fájlok, képfájlok stb. tárolását.

A fájlszűrés természetesen szintén csak NTFS-köteteken használható, mivel a korlátozások megvalósítása csak a fájlrendszerrel szoros együttműködésben lehetséges. A korlátozások (akárcsak a hozzáférés-vezérlési listák) közvetlenül a fájlrendszerben tárolódnak.

A mappákra (vagy a kötetre) beállított korlátozások alapértelmezés szerint továbböröklődnek a hierarchia mentén. Ha ezt módosítani szeretnénk, akkor konkrétan meg kell adnunk azokat a fájltípusokat, amelyek tárolását a szülőmappára érvényes korlátozás ellenére is engedélyezni szeretnénk az adott almappában. Az engedélyezés a tiltáshoz hasonló módszerrel történik, a szülőmappán megadott tiltó *(Block)* típusú szabály mellett az almappára engedélyező *(Allow)* típusú szabályt kell létrehoznunk.

A fájlszűrés segítségével a rendszergazda biztosíthatja például, hogy a felhasználók a kiszolgálón tárolt, és rendszeresen szalagra mentett személyes mappáikat ne használhassák különféle mozifilmek és mp3 fájlok tárolására, így megakadályozhatja a tárterület és a mentési kapacitás szükségtelen igénybevételét.

Megadhatunk olyan szűrési beállításokat is, hogy a rendszer ne tiltsa le például a végrehajtható fájlok megosztott mappákba másolását, de az ilyen eseményekről a rendszergazda kapjon e-mail értesítést a másolást végző felhasználó és a megfigyelt fájl adataival.



4.18. ábra: *Alapértelmezett fájlcsoportok. Minden fájlcsoporthoz a fájlnévben szereplő tetszőleges mintákat adhatunk meg*

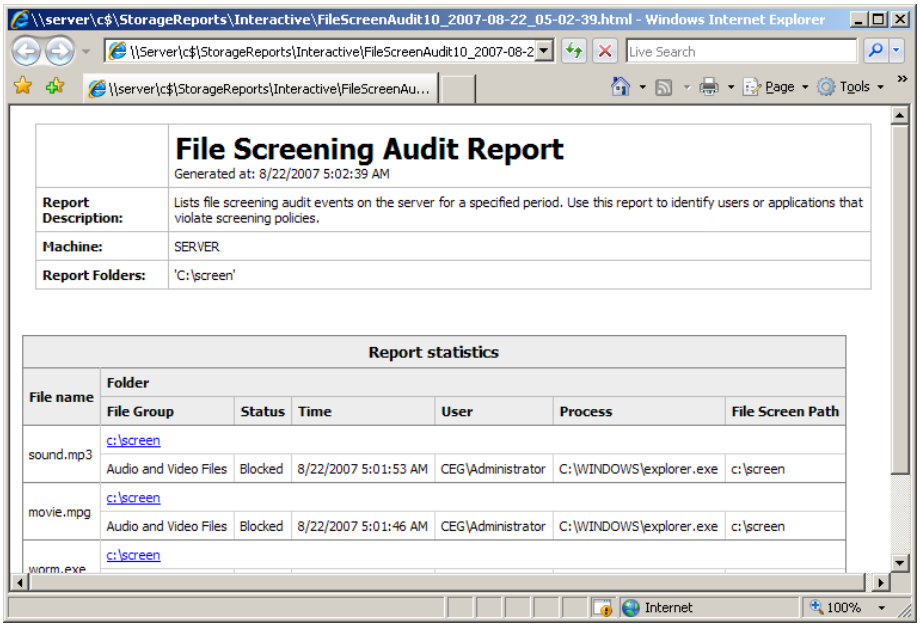
Tárolási jelentések

A tárolási jelentések segítségével részletesen figyelemmel kísérhetjük a fájlkiszolgáló merevlemezein tárolt adatokat. A legtöbb jelentés paraméterezhető (a paraméterek természetesen típusonként különbözők), így egyedileg határozhatjuk meg, hogy pontosan mit tartalmazzon az adott jelentés. Beállíthatjuk például, hogy mely kötetekről vagy mappákról készüljön a jelentés, illetve megadhatunk különféle feltételeket a jelentésbe kerülő bejegyzésekre vonatkozóan.

A jelentések ütemezetten, illetve igény szerint azonnal is előállíthatók a megadott beállítások alapján. Függetlenül az előállítás módjától, a rendszer a megadott formátumban (HTML, XML, CSV, vagy egyszerű szöveg) mentést is készít az egyes jelentésekről. A mentett jelentéseket alapértelmezés szerint a *%SYSTEMDRIVE%\StorageReports* mappa almappáiban találhatjuk meg, de a tárolómappa az FSRM beállítólapján megváltoztatható. A fájlok nevéből megállapítható a jelentés típusa és a készítés pontos dátuma is.

Nyolc különféle jelentést készíthetünk az alábbiak szerint:

- **Nagyméretű fájlok** *(Large Files)* – a jelentés segítségével azonosíthatjuk azokat a fájlokat, amelyek nagyobbak a paraméterként megadott méretnél.
- **Fájlok tulajdonos szerint** *(Files by Owner)* – a jelentésben az egyes fájlokat tulajdonosuk alapján csoportosítva tekinthetjük meg. Paraméterként megadhatjuk, hogy melyik felhasználók fájljaira vagyunk kíváncsiak, és a jelentésbe kerülő állományokat is szűrhetjük a nevükben szereplő minta alapján.
- **Fájlok fájlcsoport szerint** *(Files by File Group)* – a jelentés a paraméterként megadott fájlcsoportokhoz tartozó fájlokat tartalmazza. A kiválasztható fájlcsoportok megegyeznek a fájlszűrés szakaszban megadott csoportokkal.
- **Fájlszűrő naplózás** *(File Screening Audit)* – a jelentés a fájlszűrési szabályok megsértésével kísérletező felhasználókat, illetve alkalmazásokat sorolja fel a paraméterként megadható időtartamra visszamenőleg.



4.19. ábra: *A fájlszűrőhöz kapcsolódó eseményekről szóló jelentés*

- **Duplikált fájlok** *(Duplicate Files)* – a jelentés mappában vagy köteten több példányban megtalálható (vagyis azonos nevű, méretű és módosítási időpontú) fájlokat sorolja fel.
- **Legrégebben használt fájlok** *(Least Recently Accessed Files)* – a jelentés a paraméterként megadott időtartamnál régebben használt fájlokat sorolja fel.
- **Legutóbb használt fájlok** *(Most Recently Accessed Files)* – az előző jelentés ellentéte, vagyis azok a fájlok szerepelnek benne, amiket a megadott időpont óta valaki megnyitott.
- **Kvótahasználat** *(Quota Usage)* – a jelentés azokat a kvótákat tartalmazza, amelyek kihasználtsága magasabb a megadott százaléknál. A jelentés csak a Fájlkiszolgálói erőforrás-kezelő kötetei és mappái számára létrehozott kvótákat tartalmazza, a hagyományos NTFS-kvótákat nem.

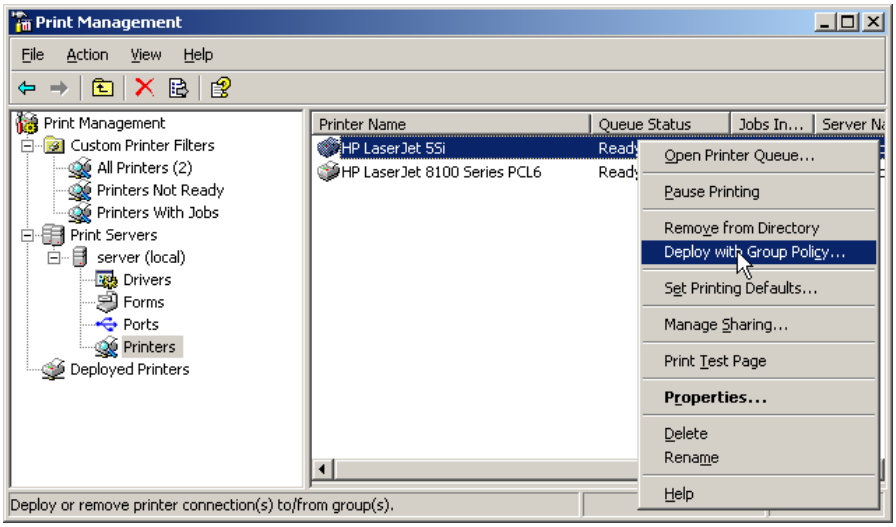
Nyomtatási szolgáltatások (PMC)

A Print Management Console *(Nyomtatáskezelő)* a hálózati nyomtatók központi kezelését és felügyeletét teszi lehetővé. A PMC használata megoldást jelenthet a hálózati nyomtatók kezelésével kapcsolatos problémáinkra; elérhetjük vele, hogy a számítógépek között vándorló felhasználókat kövessék a számukra kiosztott nyomtatók, illetve azt is, hogy egy adott gépen minden bejelentkező felhasználó elérhessen bizonyos nyomtatókat. A konzol segítségével részletes információkat kaphatunk a hálózaton elérhető valamennyi megosztott nyomtató és a nyomtatókiszolgálók állapotáról, az egyedileg meghatározható szűrők pedig lehetővé teszik a hibát jelző nyomtatók egyszerű azonosítását. A beépített webkiszolgálóval rendelkező nyomtatók esetén a konzolablakon belül is könnyen elérhetjük a nyomtató saját felügyeleti weblapját, ahol további információkat kaphatunk – például a rendelkezésre álló festék vagy papír mennyiségéről – és lehetőségünk van különféle felügyeleti műveletek távolról történő végrehajtására.

Bár a konzol csak a Windows Server 2003 R2 változatán futtatható, de képes a régebbi rendszerek (Windows 2000 Server, Windows Server 2003) nyomtatóinak kezelésére is. A konzolhoz hozzá kell adnunk a kezelendő nyomtatókiszolgálókat, amelyek ezután a Print Servers *(Nyomtatókiszolgálók)* csomópont alatt fognak megjelenni, ahol hozzáférünk a rajtuk elérhető nyomtatók és meghajtóprogramok különféle tulajdonságaihoz.

A Nyomtatáskezelő konzol használata
Ebben a screencastban a Windows Server 2003 R2 nyomtatókkal kapcsolatos új és széleskörűen használható komponensét, a Nyomtatáskezelő konzolt próbáljuk ki.
Fájlnév: II-1-1d-PMC.avi

A PMC együttműködik az Active Directory csoportházirend szolgáltatásával, így lehetőséget nyújt arra, hogy a hálózaton elérhető megosztott nyomtatókat automatikusan telepítsük az ügyfélgépekre. A telepítést számítógépre (ekkor az adott számítógépen bejelentkező valamennyi felhasználó elérheti az adott nyomtatót) és felhasználói fiókra is kérhetjük (ekkor a nyomtató „követi" az adott felhasználót, bármelyik gépen is jelentkezik be).



4.20. ábra: *Nyomtató közzététele az ügyfélgépek számára*

Minden nyomtatóhoz megadhatjuk azt a csoportházirend objektumot, amely az adott nyomtatót szállítja majd az ügyfelek számára. A telepítés a csoportházirendnél megszokott módon, vagyis az adott számítógép, vagy felhasználó szervezeti egységhez, illetve biztonsági csoporthoz való tartozása, vagy WMI-szűrő alapján is vezérelhető. (Az Active Directoryval és a csoportházirenddel a következő, a „Tartományi környezet" című fejezet foglalkozik részletesen.)

Windows Vista előtti ügyfélgépek esetén szükség van még rendszerindításkor a pushprinterconnections.exe nevű program futtatására, ami „olvassa" a vonatkozó csoportházirend objektumot, majd telepíti, illetve szükség esetén el is távolítja a nyomtatókat.

A program futtatását a számítógéphez, illetve felhasználóhoz tartozó bejelentkezési parancsfájlból kezdeményezhetjük, célszerű ezt is megadni a nyomtatóbeállítást tartalmazó csoportházirend objektumban. Windows Vista ügyfélgép esetén a program futtatására már nincsen szükség (természetesen a leendő későbbi rendszerek esetén sem fog kelleni).

Hálózati szolgáltatások

A következőkben a Windows Server 2003 különféle hálózati szolgáltatásaival fogunk megismerkedni. Egy rövid ismétlés után áttekintjük a hálózathoz csatlakozó számítógépek TCP-IP konfigurációjának központi megadására alkalmas DHCP-szolgáltatást, majd röviden ismertetjük a korábbi Windows rendszerekben használt névfeloldási módszert, a WINS-szolgáltatást.

Ezután következik a Windows-hálózatok távoli elérését, és különféle útválasztási szolgáltatásokat biztosító RRAS-szolgáltatás, végül pedig a Windows felhasználói felületének továbbítására képes Terminálszolgáltatások *(Terminal Services)* ismertetése.

Egy kis ismétlés: az IP-cím és típusai

Az IP-cím az IP-hálózat csomópontjait azonosító 32-bites szám (IPv4 estén). A hálózat minden csomópontjának egyedi címmel kell rendelkeznie, amely a hálózat azonosítójából és az állomás azonosítójából áll, és amelynek az adott hálózaton belül egyedinek kell lennie. A cím a bájtok decimális értékét tartalmazza pontokkal elválasztva (például 192.168.16.2). Az IP-címek tehát az internetre, (illetve bármilyen IP-hálózatra) kapcsolódó eszközök hálózati csatolófelületeinek egyedi azonosítói.

Az IP-címek osztályokba sorolása annak alapján történik, hogy a cím mekkora része azonosítja a hálózatot, és mekkora rész marad a hálózaton belül az állomás azonosítására. Ennek alapján megkülönböztethetünk A, B és C osztályú címeket (a D és E osztályokkal most nem foglalkozunk).

- **A-osztályú címek** – az A-osztályú címek használatára csak rendkívül nagyszámú állomást tartalmazó hálózatok esetén lehet szükség, mivel ebben az esetben mindössze 7-bit szolgál a hálózat azonosítására, a maradék 24 pedig az egyes állomásokat különbözteti meg. (A hiányzó egy bit a cím típusának jelzésére szolgál.) Ez azt jelenti, hogy összesen 128 – 2 = 126 ilyen hálózat lehet az egész világon. Viszont minden egyes háló-

zat $2^{24} - 2$, vagyis több mint 16 millió állomást tartalmazhat. (Azért kell mindkét számból kettőt levonnunk, mert a csupa nullából álló azonosító az adott hálózatot, illetve állomást jelenti, a csupa egyesből álló cím pedig a szórt *(broadcast)* üzenetek számára van fenntartva.)

- **B-osztályú címek** – a B-osztály esetében 14-bit azonosítja a hálózatot (két bit a címtípust), a maradék 16-bit pedig a hálózaton belül magát az állomást. Ez a címosztály tehát még mindig meglehetősen nagy (legalábbis a magyarországi méreteket tekintve) hálózatokban is használható, mivel a hálózaton belül kioszthatók címek száma több mint 65 ezer. A hálózatot azonosító 14-bit nagyjából 16 ezer ilyen hálózat megkülönböztetésére elegendő.
- **C-osztályú címek** – a C-osztályú címek kisebb hálózatokban való használatra alkalmasak, a hálózaton belül 254 állomást (8-bit) különböztethetünk meg C-osztályú címek használatával. Viszont meglehetősen sok (több mint 2 millió) ilyen hálózat lehet, mivel 21-bit alkotja a hálózat azonosítóját.

Az IP-címen belül a hálózati azonosító és az állomásazonosító az alhálózati maszk *(subnet mask)* alapján választható szét. Az alhálózati maszkok 32-bites számok, amelyekben az egymás utáni „egy" értékű bitek jelzik a hálózatazonosítót, az egymás utáni nullás bitek pedig állomásazonosító részt.

Publikus címek

A publikus címmel rendelkező hálózati csomópontok közvetlenül bekapcsolódhatnak az internet vérkeringésébe, semmiféle közvetítőre nincsen szükségük. Az interneten csak olyan adatcsomagok közlekedhetnek, amelyek feladója és címzettje is publikus címmel rendelkezik, mivel a forgalomirányító eszközök *(routerek)* csak az ilyen csomagokat továbbítják. Ebből mindjárt következik is a publikus címekkel kapcsolatos egyik probléma: minden publikus címnek a **teljes** internetre nézve egyedinek kell lennie, vagyis a publikus címek erősen szűkös erőforrásnak tekinthetők.

Publikus IP-címet tehát akkor használunk, ha:

- közvetlen, akadálytalan internetelérésre van szükség,
- bőven van saját, publikus IP-címünk.

A publikus IP-címekkel kapcsolatos hátrányok egyenes következményei az előnyöknek:

- Mivel egyedinek kell lennie, nincs elég belőle.
- Nincs elég belőle, tehát drága.
- Kevésbé biztonságos, mivel az, hogy közvetlen internetelérésre ad lehetőséget, egyben azt is jelenti, hogy fordítva, az internetről is közvetlenül elérhető a publikus címmel rendelkező számítógép. Ez a felállás pedig csak olyan gépek esetében engedhető meg, amelyek erre teljes mértékben fel vannak készítve, különben igen gyorsan meg fogjuk tapasztalni az internetes világ összetettségét.

Privát címek

A címtér egy része olyan állomások számára van fenntartva, amelyek nem csatlakoznak közvetlenül az internetre, vagyis ezeket a címeket bármely vállalat vagy szervezet szabadon felhasználhatja a belső hálózatán található állomások azonosítására. Három címtartomány tartozik ebbe a kategóriába:

- 10.0.0.0 – vagyis egy A-osztályú hálózat valamennyi címe.
- A 172.16.0.0-től a 172.31.0.0-ig terjedő címtartomány, vagyis 16 egymás utáni B-osztályú hálózat valamennyi címe.
- A 192.168.0.0-től a 192.168.255.0-ig terjedő címtartomány, vagyis 256 egymás utáni C-osztályú hálózat.

Mivel a fenti címeket bárki használhatja, azok természetesen nem egyediek, így nem használhatók az internet közvetlen elérésére. Azok az állomások, amelyek csak privát címmel rendelkeznek, az internetet csak közvetítő (hálózati címfordító) segítségével érhetik el.

Privát címeket tehát akkor használunk, ha:

- nem kell, vagy nem lehetséges közvetlenül elérni az internetet,
- nincs elég publikus IP-címünk.

A privát címek használata számos előnnyel jár, például ebben az esetben nincs szükség semmiféle regisztrációra, gyakorlatilag bármennyi IP-címet kiosztathatunk saját belátásunk szerint. Természetesen a privát címek használata költséggel sem jár, ráadásul biztonságosabb is a publikus címeknél, mivel az ilyen címet használó állomások nem érhetőek el az internet felől közvetlenül.

Ha a privát címeket használó hálózatból mégis ki szeretnénk látni az internetre, szükségünk van egy olyan eszközre, ami a privát címeket az interneten is továbbítható publikus címekké alakítja. Vállalatok esetben a szolgáltató általában biztosít néhány publikus IP-címet, a belső, privát címek kiosz-

tását és a címfordítást pedig a vállalaton belül kell megoldani. Ez a legegyszerűbb esetben azt jelenti, hogy szükség van egy kiszolgáló számítógépre, amely minimálisan két hálózati csatolóval rendelkezik (ideális esetben ez egy tűzfal, amin egyetlen más kiszolgálószolgáltatás sem fut). Az egyik csatoló megkaphatja a szolgáltatótól bérelt publikus címet, a másik pedig a belső hálózatnak megfelelő, privát címmel fog rendelkezni. Az internetre közvetlenül tehát csak ez az egy gép csatlakozik, a többiek pedig az ő szolgáltatásait vehetik igénybe bármiféle internetes adatforgalomhoz.

Egy kis ismétlés: az IP-beállítás módszerei

A következőkben áttekintjük azokat a módszereket, amelyekkel a TCP/IP-t használó állomások hozzájuthatnak a működésükhöz szükséges paraméterekhez. Hogy melyik megoldás a leginkább kedvező, az erősen függ a körülményektől, de természetesen nem kell feltétlenül csak egyetlen módszert választanunk, az is lehetséges, hogy bizonyos eszközök statikus beállításokat használnak, a többi pedig például DHCP-kiszolgálótól kapja az IP-címét és többi TCP/IP-paramétert is.

APIPA (Automatic Privat IP Addressing)

Ha egy számítógépen nincs statikusan beállított IP-cím, és DHCP segítségével sem sikerül címet kapnia, akkor az APIPA (Automatic Private IP Addressing, *automatikus magánhálózati IP-címkiosztás)* szolgáltatást fogja használni az automatikus konfigurációhoz. A gép a 169.254.0.1-től 169.254.255.254-ig terjedő tartományból fog címet kapni a 255.255.0.0 alhálózati maszkkal. Az alapértelmezett átjárót, a DNS-kiszolgálót és a WINS-kiszolgálót az APIPA nem állítja be, mivel az így kiosztott címek csak egyetlen hálózati szegmensben működhetnek, és a gépeknek internetkapcsolata sem lehet (arról nem is beszélve, hogy elég nehezen találhatná ki mondjuk a DNS-kiszolgáló IP-címét). Az APIPA-címhozzárendelést tehát akkor használhatjuk, ha:

- nincs DHCP-kiszolgáló,
- a hálózat egyetlen szegmensből áll,
- nincs szükség a címek feletti kontrollra,
- nincs szükség központi beállításra.

Statikus cím, kézi beállítás

Ha a TCP/IP-protokoll tulajdonságait a hálózati kapcsolat tulajdonságlapján kézzel állítjuk be, meg kell adnunk az IP-címet, az alhálózati maszkot, az alapértelmezett átjárót *(default gateway)*, a DNS-kiszolgálót és esetleg a WINS-kiszolgálót. A kézi beállításra a következő esetekben lehet szükség:

- nincs DHCP-kiszolgáló, és egynél több alhálózatunk van (egy alhálózat esetén használható az APIPA),
- kevés számítógép, illetve hálózatra csatlakozó eszköz van,
- teljes kontrollra van szükség a címek felett.

DHCP – dinamikus

A DHCP (Dynamic Host Configuration Protocol) protokoll alkalmazásával a számítógép bekapcsolásakor a TCP/IP-protokoll beállítása dinamikusan és automatikusan történik. A DHCP-kiszolgáló megfelelő beállítása esetén a számítógépek (és egyéb eszközök) hozzájuthatnak IP-címükhöz, az alhálózati maszkhoz, és az alapértelmezett átjáróval, DNS-kiszolgálóval és WINS-kiszolgálóval kapcsolatos beállítási információkhoz.

Közepes és nagyobb hálózatok esetén a számítógépek többsége számára a dinamikus DHCP címhozzárendelés lehet a legjobb megoldás. A Windows operációs rendszerrel működő számítógépek alapértelmezés szerint DHCP-ügyfelek, vagyis az ügyfélgépeken semmiféle beállításra nincs szükség. Ezt a megoldást célszerű használni, ha:

- van DHCP-kiszolgáló,
- központi beállítás szükséges, és szeretnénk lehetőséget biztosítani a központilag vezérelt változtatásokra.

DHCP – fenntartott

A fenntartott címeket és egyéb paramétereket a DHCP-kiszolgáló osztja ki, de olyan módon, hogy az adott állomás minden esetben egy meghatározott IP-címet kapjon. Akkor használjuk ezt a módszert, ha:

- van DHCP-kiszolgáló,
- egy adott gépen valamilyen ok miatt mindig ugyanarra a címre van szükség,
- de mégis szeretnénk, ha a DHCP-kiszolgálótól kapna címet, például azért, hogy a többi paramétert ne kelljen kézzel beállítanunk.

A DHCP-kiszolgáló

A DHCP egy TCP/IP szolgáltatóprotokoll, amely az állomások számára kiosztható IP-címek bérleti konstrukcióban történő hozzárendelését teszi lehetővé, és más paramétereket is eloszt az ezt igénylő hálózati ügyfelek számára. A DHCP biztonságos, üzembiztos és egyszerű TCP/IP hálózati konfigurációt tesz lehetővé, segítségével elkerülhetjük a címütközéseket, és jelentősen egyszerűsíthetjük az IP-címek kiosztásával kapcsolatos adminisztrációt. A DHCP ügyfél/kiszolgáló modellt használ, amelyben a DHCP-kiszolgáló végzi a hálózatban használt IP-címek nyilvántartását és kiosztását, a DHCP-protokollt támogató ügyfelek pedig hálózati bejelentkezésük részeként meghatározott időtartamra IP-címet bérelhetnek, és egyedi TCP/IP konfigurációt kaphatnak a DHCP-kiszolgálótól.

A DHCP-kiszolgáló beállításai
Ebben a screencastban a Windows Server 2003 DHCP-szolgáltatásának telepítésével és részletes beállításaival ismerkedhetünk meg.
Fájlnév: II-1-2a-DHCP-kiszolgalo.avi

Érdekes kérdés, hogy vajon hogyan működhet egy olyan TCP/IP-alapú szolgáltatás, amelynek az a kiinduló állapota, hogy az egyik résztvevő állomásnak egyáltalán nincsen érvényes IP-címe, és a többi paraméter sincs beállítva. A DHCP-ügyfélnek ráadásul nyilvánvalóan semmiféle elképzelése nem lehet arról, hogy kitől is kellene címet kérnie, nem tudhatja például a DHCP-kiszolgáló IP-címét.

Nos, a DHCP szórt üzenetekkel *(broadcast)* működik, mivel az ügyfél egyetlen dolgot tud biztosan, mégpedig azt, hogy a 255.255.255.255 broadcast címre küldött csomagot mindenki (így, ha van ilyen egyáltalán, akkor a DHCP-kiszolgáló is) meg fogja kapni. Miután bekapcsolunk egy DHCP-címkérésre beállított gépet, az első hálózati művelet egy ilyen csomag kiküldése lesz. A címkérés teljes folyamata négy lépésből áll, vagyis négy hálózati csomagra van szükség:

- **DHCP Discover** *(felderítés)* – ezt a csomagot az ügyfél küldi ki (broadcast), vagyis tulajdonképpen belekiabál az ismeretlenbe: Hahó, valaki! Címet kérek! Ha esetleg senki nem válaszol, akkor jöhet APIPA.
- **DHCP Offer** *(ajánlat)* – ezt a csomagot a DHCP Discover üzenetre válaszul a kiszolgáló küldi vissza, még mindig broadcast címzéssel, vagyis az ügyfélnek az üzenetekben szereplő azonosítószámok segítségével el kell döntenie, hogy a válasz valóban az ő kérésére érkezett-e. A csomag tartalmazza a felajánlott IP-címet és a hozzá tartozó egyéb paramétereket, vagyis szabad fordításban ezt jelenti: Ez jó lesz?

- **DHCP Request** *(kérés)* – ezután az ügyfél még mindig broadcast üzenetet küld, ami azt jelenti: Rendben, jöhet. Talán fölöslegesnek tűnhet ez a plusz kör a folyamatban, hiszen az ügyfél akár mindenféle visszabeszélés nélkül beállíthatná a kapott paramétereket. A pontos egyeztetésre tulajdonképpen csak akkor van szükség, ha több DHCP-kiszolgáló is üzemel a hálózatban.
- **DHCP Ack** *(visszaigazolás)* – az utolsó üzenet a visszaigazolás, az ügyfél az ebben szereplő IP-címet és opciókat fogja beállítani. Szintén ebben az üzenetben szerepel, hogy mikor fog lejárni a címbérlet, vagyis az üzenet tartalma ennyi: OK, nyolc napig a tiéd ez a cím.

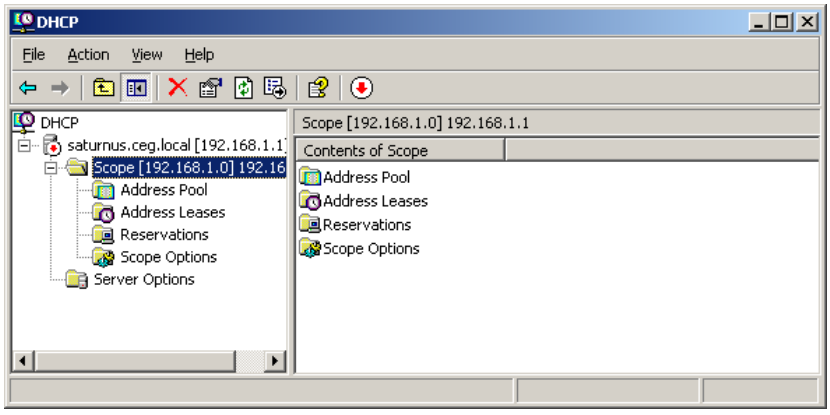
Mivel a szórt üzenetek csak az adott alhálózaton belüli számítógépeket érik el, alapállapotában a DHCP-szolgáltatás csak egyetlen fizikai alhálózaton használható. Ha több alhálózatra szeretnénk egyetlen kiszolgáló segítségével címeket osztani, akkor az alhálózatokat összekötő útválasztókon DHCP-továbbító ügynököket *(DHCP Relay Agent)* kell telepítenünk. Az ügynök fogja a hozzá érkező broadcast DHCP-üzeneteket a többi alhálózatra továbbítani.

A DHCP-szolgáltatás segítségével az IP-címen kívül még számos más paramétert is beállíthatunk, ezek szintén a DHCP Ack üzenetben szerepelnek. A következőkben a leggyakrabban használt paramétereket soroljuk fel:

- **Útválasztó** *(Router)* – a paraméter segítségével az ügyfeleken beállítandó alapértelmezett átjárót *(default gateway)* határozhatjuk meg. Az alapértelmezett átjáró egy olyan cím, amelyre az ügyfél azokat a csomagokat küldi el, amelyeket ő maga nem tud közvetlenül kézbesíteni (vagyis nincsenek a saját alhálózatában). Az ilyen csomagok továbbítása az alapértelmezett átjáróként megadott állomás feladata.
- **DNS-kiszolgálók** *(DNS Servers)* – az ügyfeleken beállítandó DNS-kiszolgálókat adhatjuk itt meg.
- **DNS-tartománynév** *(DNS Domain Name)* – a DHCP-ügyfelek névfeloldási folyamata során használható DNS-tartománynév.
- **WINS-csomóponttípus** *(WINS/NBT Node Type)* – a NetBIOS-névfeloldás módja (4 variáció van).
- **WINS-kiszolgálók** *(WINS/NBNS Servers)* – a DHCP-ügyfelek által használható WINS-kiszolgálók IP-címei.
- A DHCP-kiszolgáló az ügyfeleinek bérbe adható címeket egy általunk előre beállított címtartományból, az úgynevezett hatókörből *(scope)* veszi. A hatókör tehát a DHCP-szolgáltatást használó alhálózat számítógépeihez tartozó IP-címek csoportja. A DHCP-szolgáltatás beállítása

során minden egyes fizikai alhálózat számára létre kell hoznunk egy hatókört, ennek különféle tulajdonságait beállítva határozhatjuk meg az adott hatókörből IP-címet bérlő ügyfeleknek ténylegesen elküldendő paramétereket. A hatókörök létrehozásakor a következő tulajdonságokat kell beállítanunk:

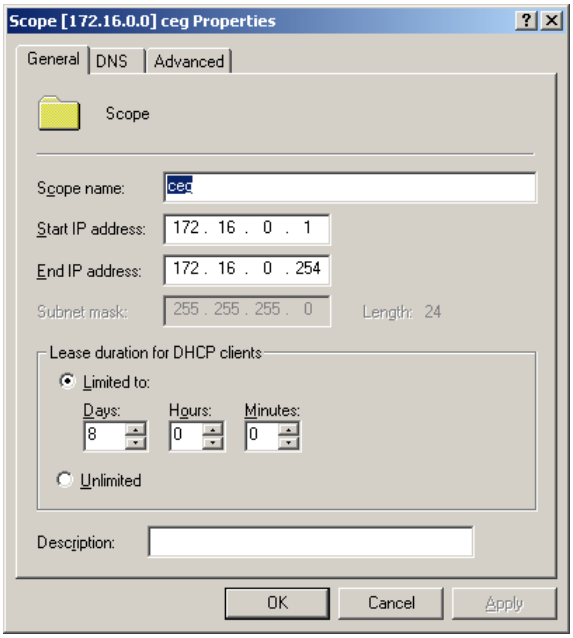
- **Address Pool** *(címkészlet)* – a címkészlet határozza meg a DHCP-szolgáltatás címbérleti szolgáltatásához használható, és az abból kizárt IP-címek tartományát.



4.21. ábra: *A DHCP konzol a hatókör beállítható tulajdonságaival*

- A hatókörön belül azokból az IP-címekből kell kizárási tartományt létrehoznunk, amelyeket a DHCP-kiszolgálónak nem szabad felajánlania az ügyfelek részére. A kizárt IP-címek természetesen használhatók a hálózaton, de ezeket kézzel kell beállítanunk azokon az állomásokon, amelyek nem veszik igénybe a DHCP-szolgáltatást. Statikus IP-címet kell használnunk például magán a DHCP-kiszolgálón, a DNS-kiszolgálón, a tartományvezérlőkön, a hálózati nyomtatókon stb. Ezeket a címeket feltétlenül zárjuk ki a DHCP-kiszolgáló által kiosztható címek közül.

- **Subnet Mask** *(alhálózati maszk)* – az IP-címek alhálózatát határozza meg.
- **Lease Duration** *(bérleti időtartam)* – az az időintervallum (alapértelmezés szerint nyolc nap), ameddig a dinamikus címeket bérlő DHCP-ügyfelek a kiosztott címeket megújítás nélkül használhatják.



4.22. ábra: *A hatókör címkészletének meghatározása*

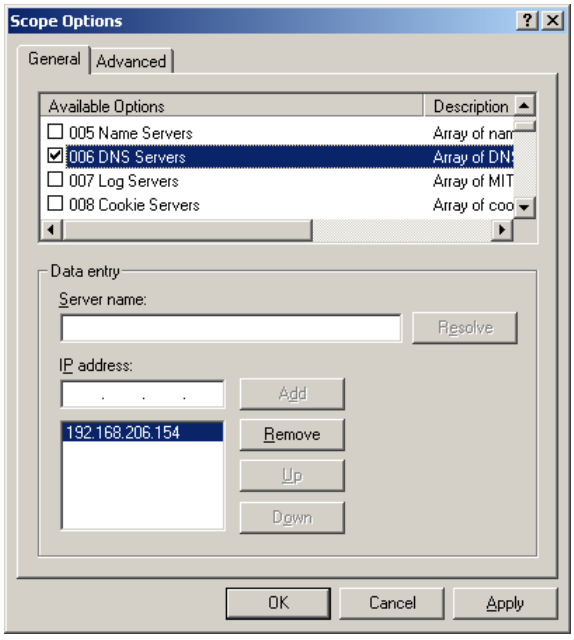
- **DHCP Options** *(DHCP-opciók)* – a DHCP-ügyfeleknek elküldött valamennyi TCP/IP-paraméter.
- **Reservations** *(fenntartások)* – a fenntartások biztosítják, hogy egy-egy adott DHCP-ügyfél mindig ugyanazt az IP-címet kapja meg. Fenntartott cím használatára olyan gépeken van szükség, amelyeknek fix IP-címmel kell működniük, de mégsem szeretnénk statikus beállítást használni, hogy a többi paramétert központilag állíthassuk be. A fenntartott IP-cím beállításához az ügyfélgépen semmi teendőnk nincs, viszont a DHCP-kiszolgálón meg kell adnunk a fenntartott címet igénylő állomás fizikai címét (MAC-address).

Hogy megtudhassuk egy csatoló MAC-címét, szerencsére nem kell feltétlenül odamennünk a kérdéses számítógéphez. Ha megpingeljük az adott gépet, akkor annak MAC-címe bekerül az ARP-protokoll *(Address Resolution Protocol)* helyi gyorsítótárába (és kerek két percig ott is marad), így kiíratható az *arp -a* parancs segítségével. Sajnos, azonban ez a módszer csak az első routerig működik, mivel az útválasztók csereberélik az Ethernet keretekben található MAC-címeket.

Ha új fenntartott címet szeretnénk definiálni a kiszolgálón, akkor ellenőriznünk kell, hogy az adott címre van-e már érvényes bérlet, ugyanis a fenntartás létrehozása önmagában nem szabadítja fel a már kiadott IP-címet. Ha a cím már használatban van, akkor vagy ki kell várnunk a bérleti idő lejártát, vagy az ügyfélgépen ki kell adnunk az *ipconfig /release* parancsot. Hiába hozzuk létre a fenntartást, az adott ügyfél csak akkor kapja azt meg ténylegesen, ha ő maga kéri, a DHCP-kiszolgáló nem fogja kezdeményezni semmiféle cím kiadását. Új cím kéréséhez az ügyfélgépen az *ipconfig /renew* parancsot kell kiadnunk.

A fenti listában már találkozhattunk a DHCP-kiszolgáló által elküldött paramétereket meghatározó DHCP-opciók megadásával, azonban ezeket nem csak a hatókörben, hanem összesen négy különböző szinten is megadhatjuk:

- **Server Options** *(Kiszolgáló beállításai)* – az itt megadott beállítások a DHCP-kiszolgálón definiált valamennyi hatókörre vonatkoznak, vagyis minden ügyfél meg fogja kapni azokat.
- **Scope Options** *(Hatókör beállításai)* – az itt megadott beállítások egy adott hatókörön belüli címbérletet megszerző valamennyi ügyfélre vonatkoznak.



4.23. ábra: *A hatókörhöz tartozó számítógépekre küldendő paraméterek beállítása*

- **Class Options** *(Osztály beállításai)* – ezek a beállítások csak azokra az ügyfelekre vonatkoznak, amelyeket egy cím megszerzésekor a kiszolgáló egy adott felhasználói vagy forgalmazói osztály tagjaként azonosított. A DHCP-osztályokkal kapcsolatos tudnivalókról később még részletesen szót ejtünk.
- **Reservation Options** *(Fenntartott cím beállításai)* – az itt megadott beállítások csak arra az egyetlen ügyfélgépre vonatkoznak, amely az adott fenntartott címet kapja.

A különböző szinteken megadott beállítások öröklődnek is az alsó szintek felé, de ütközés esetén mindig a később megadott paraméter győz a fenti sorrend szerint.

A DHCP-szolgáltatás beállítását tehát a következő módon kell megtennünk. A DHCP-konzolban létrehozunk egy új hatókört és beállítjuk a:

- kioszthatót és a kizárt címeket,
- a címek érvényességének intervallumát,
- a fenntartott címeket,
- az ügyfeleknek küldendő valamennyi opciót.

Ezután még aktiválnunk kell a hatókört és (majdnem) készen is vagyunk. Amennyiben Active Directory környezetben használjuk a DHCP-kiszolgálót, egy engedélyeztetést *(Authorize)* is el kell végeznünk, ugyanis a DHCP-kiszolgálóról az Active Directory címtár is tudni szeretne. Az engedélyezést csak a címtárban definiált Enterprise Admins *(Vállalati rendszergazdák)* csoport tagjai végezhetik el a különféle kalóz DHCP-szolgáltatások zavaró hatása elleni védekezésül. Alapértelmezés szerint a csoportnak egyetlen tagja van, mégpedig az eredeti, beépített Administrator (*Rendszergazda)* felhasználói fiók.

A DHCP-kiszolgáló számára néhány további fontos paramétert is meg kell adnunk (ezek a beállítások minden hatókörre vonatkoznak). Ha a kiszolgáló több hálózati csatolóval is rendelkezik, akkor kiválaszthatjuk, hogy melyik csatolón keresztül válaszoljon a DHCP-ügyfelek kéréseire, és a kiszolgáló tulajdonságlapján megadhatjuk a DHCP- és DNS-szolgáltatás együttműködését befolyásoló paramétereket is. A régebbi ügyfélrendszerek (Windows 2000 előtt) nem képesek a dinamikus DNS-bejegyzések létrehozására, de megfelelő beállítás esetén a címeket kiadó DHCP-kiszolgáló megteheti ezt helyettük. Alapértelmezés szerint a DHCP-kiszolgáló csak akkor próbálkozik a kiadott címek bejegyzésével, ha az ügyfél ezt kifejezetten kéri, a régi ügyfélrendszerek viszont nem tudnak erről a lehetőségről, így ha szükséges, be kell állítanunk, hogy az ő bejegyzéseiket a kiszolgáló kérés nélkül is elkészítse.

A DHCP-kiszolgáló szolgáltatásait igénybe venni kívánó számítógépeken semmiféle beállításra nincsen szükség, mivel a Windows operációs rendszerek alapértelmezés szerint DHCP-ügyfélként kezdik pályafutásukat.

A beállításosztályok

A beállításosztályok további lehetőséget kínálnak, arra, hogy egy hatókör ügyfeleit csoportokba rendezzük, és az egyes csoportok számára különböző beállítás-készleteket határozzunk meg.

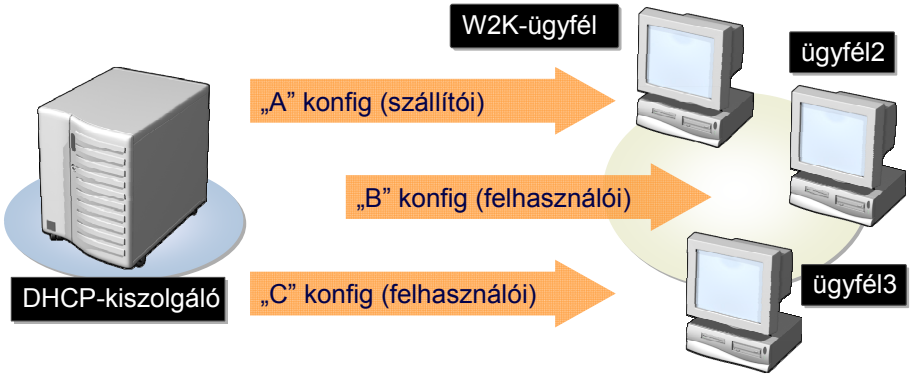
A beállításosztályok a következő két típusba sorolhatók:

- **Felhasználói osztályok** *(User Classes)* – a felhasználói osztályokat teljesen egyénileg definiálhatjuk, de ehhez az ügyfélgépeken egyesével meg kell határoznunk, hogy a gép melyik felhasználói osztály tagja legyen. A felhasználói osztályokkal tehát a hasonló DHCP-beállításokat igénylő ügyfelekhez rendelhetjük hozzá a megfelelő beállításokat.
- **Szállítói osztályok** *(Vendor Classes)* – A szállítói osztályok segítségével azonos szállítói típussal (operációs rendszerrel) rendelkező ügyfelekhez rendelhetők speciális beállítások.

A felhasználói osztályokat a DHCP-kiszolgálón kell létrehoznunk, és minden osztályhoz meg kell adnunk egy osztályazonosítót, ami alapján a kiszolgáló majd megismeri az adott osztályhoz tartozó ügyfeleket. Természetesen minden ügyfélnek is ismernie kell saját osztályának (csoportjának) azonosítóját, ezt az *ipconfig /setclassid* parancs használatával állíthatjuk be az egyes hálózati csatolókra vonatkozóan. Az azonosító segítségével tehát az egy hatókörön belüli, hasonló konfigurációt igénylő ügyfelek csoportosítását végezhetjük el.

A felhasználói osztályok használatára akkor lehet szükség, ha az ügyfélgépek meghatározott csoportjai a szokásostól bizonyos mértékig eltérő beállításokat (például rövidebb címbérleti időt, vagy másik DNS-kiszolgálót) igényelnek. Miután az ügyfélgépeken megtettük a szükséges beállítást (vagyis meghatároztuk, hogy az adott ügyfélgép melyik DHCP-osztályhoz tartozik), a DHCP-kiszolgálóhoz való csatlakozás után a hatókörük számára megadott beállításokon kívül az osztály szintjén definiált paraméterek is eljutnak hozzájuk.

A szállítói osztályok szerint azok a DHCP-ügyfelek kaphatják meg paramétereiket, amelyek a címbérlet megszerzésekor a DHCP-kiszolgálónak küldött üzenetben a szállítótípusuk szerint azonosítják magukat. A Windows Server 2003 DHCP-kiszolgálóján például rendelkezésre áll a „Microsoft Options”, vagy a „Microsoft Windows 2000 Options” szállítói osztály. Ennek segítségével a Microsoft operációs rendszerek, illetve ezen belül a Windows 2000 rendszerek a többi számítógéphez képest eltérő beállításokat kaphatnak a DHCP-kiszolgálótól.



4.24. ábra: *Az ügyfelek osztályuknak megfelelő beállításokat kaphatnak*

Az LMHOSTS-fájl és a WINS-kiszolgáló

A Windows operációs rendszerek korábbi verziói (Windows 2000 előtt) a NetBIOS-neveket használják a hálózaton elérhető számítógépek és egyéb megosztott erőforrások azonosítására. Ezekben a rendszerekben a NetBIOS-nevek használata a hálózati szolgáltatások elérésének alapfeltétele.

A WINS-kiszolgáló telepítése és beállítása
Ebben a screencastban a NetBIOS-névfeloldás biztosítására képes WINS-kiszolgáló telepítésével és beállításaival ismerkedünk meg.
Fájlnév: II-1-2b-WINS-kiszolgalo.avi

A NetBIOS-névtér egyetlen szintből áll, ami azt jelenti, hogy a névtérben található valamennyi névnek egyedinek kell lennie, a NetBIOS-nevek pedig maximálisan 16 karakter hosszúak lehetnek. A NetBIOS munkamenetek minden esetben két névvel azonosított erőforrás között jönnek létre, de két erőforrás között egy időben csak egyetlen NetBIOS-munkamenet lehet. A további fájl-, vagy nyomtatómegosztási kapcsolatok ugyanazon a munkameneten osztoznak.

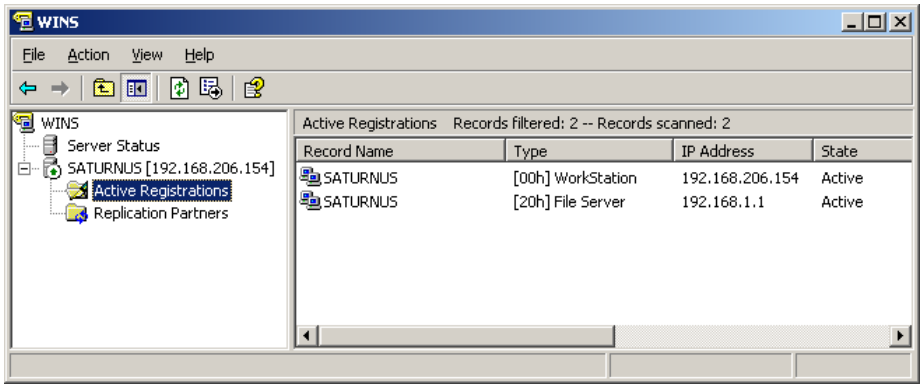
A NetBIOS-neveket használó erőforrások azonosítása szórt *(broadcast)* üzenetek használatával lehetséges, így meglehetősen nagy hálózati forgalommal jár. A hálózati forgalom csökkentéséhez valamilyen módon tárolnunk kell a nevek és címek összerendelését, és ezt az adatbázist elérhetővé kell tennünk a hálózaton. A NetBIOS-nevek és IP-címek összerendelésének nyilvántartására a Windows-rendszerekben két módszer áll rendelkezésre:

- LMHOSTS-fájl használata
- WINS-kiszolgáló (Windows Internet Name Service) használata

Az LMHOSTS a *%SYSTEMROOT%\System32\Drivers\Etc* mappában található, illetve nem található, mivel a mintaként kapott fájl neve *lmhosts.sam*. A fájlt a megfelelő módosítások után a megfelelő átnevezéssel kell élesítenünk. A fájlban megadhatunk egy másik (tetszőleges nevű) központilag tárolt *lmhosts* fájlt is, így megvalósítható a teljes hálózat számára egyetlen, központilag karbantartott *lmhosts* fájl használata is. Az *lmhosts*-fájl azonban még ebben az esetben is kézi feltöltést igényel, vagyis csak egészen kis hálózatokban ajánlható. Teljesen alkalmatlan például a DHCP-szolgáltatással való együttműködésre, minden számítógépen statikus IP-beállításokat kell használnunk.

A WINS-kiszolgáló a hálózaton használt számítógépekhez és csoportokhoz tartozó NetBIOS-nevek és IP-címek összerendeléseinek regisztrálásához és lekérdezéséhez biztosít dinamikusan felépíthető, elosztott adatbázist. A WINS-kiszolgáló teljesen automatikusan építi fel a névszolgáltatás biztosító adatbázist, és lehetőség van a kiszolgálók közötti replikációra is, így gyakorlatilag bármilyen méretű rendszerben használható. A központi adatbázis jelentősen csökkenti a NetBIOS-nevek használatával együtt járó szórt üzenetek számát, és a dinamikusan frissülő adatbázis miatt nem igényel statikus IP-címeket.

A WINS-kiszolgáló tehát kezeli a WINS-ügyfelek névregisztrációs kérelmeit, regisztrálja neveiket és IP-címeiket, és válaszol az ügyfelek által benyújtott NetBIOS-névkérdésekre, vagyis visszaküldi a lekérdezett névhez tartozó IP-címet, amennyiben az szerepel az adatbázisban.



4.25. ábra: *A WINS-szolgáltatás adatbázisa*

A WINS-kiszolgáló felügyeletével a legtöbb esetben nincsen sok gond, a telepítés után a szolgáltatás gyakorlatilag teljesen automatikusan működik. Tiszta Windows Server 2003 tartományokban tulajdonképpen nincsen rá szükség, mivel itt a névfeloldás alapértelmezés szerint a DNS-szolgáltatáson alapul, de tartalék módszerként azért alkalmanként jó szolgálatot tehet, és bizonyos speciális alkalmazások is megkövetelhetik a NetBIOS-névfeloldás használatát.

Az RRAS-infrastruktúra

A Routing and Remote Access Server (RRAS, *Útválasztás és távelérés)* képes biztosítani azt, hogy külső eszközökről (internet, másik hálózat, mobil eszközök stb.) csatlakozhassunk a vállalat hálózatához. A kapcsolódás analóg telefonvonal, ISDN, ADSL, vagy az interneten keresztül megvalósított VPN-kapcsolat segítségével is lehetséges. A távoli felhasználók éppen úgy dolgozhatnak, mintha számítógépük fizikailag csatlakozna a hálózatra. A távelérésű kapcsolatok számára engedélyezett minden olyan szolgáltatás, amely a LAN-kapcsolattal rendelkező felhasználók számára szokásosan elérhető (például fájl- és nyomtatómegosztás, levelezés stb.), és az erőforrások kezelésére a helyi hálózatokban megszokott eszközök használhatók.

Az RRAS további fontos szolgáltatása, hogy szoftveres útválasztóként, illetve átjáró-kiszolgálóként képes működni, így lehetőséget nyújt a külső és belső hálózatok rugalmas összekapcsolására. Az internet használatával megvalósított kapcsolatok biztonságát a PPTP, L2TP és IPSec protokollok támogatása biztosítja. A következőkben megismerkedünk a RRAS különféle képességeivel és az alkalmazott protokollok működésével.

Útválasztás és távelérés (RRAS) és a virtuális magánhálózatok
Ebben a screencastban feltelepítjük és beállítjuk a Windows Server 2003 RRAS-komponensét, majd VPN-kiszolgálót építünk és aztán az ügyfélről ki is próbáljuk.
Fájlnév: II-1-2c-RRAS-infrastruktura.avi

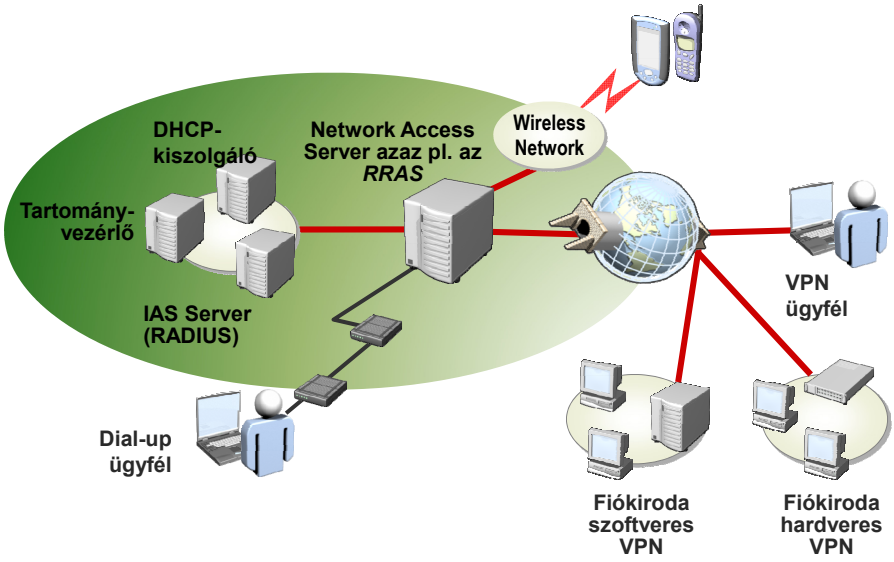
Az RRAS képességei

Az RRAS a következő szolgáltatásokat nyújthatja a hálózat számára:

- **Távoli elérés** *(Remote access)* – Az RRAS használatával a felhasználók távolról kapcsolódhatnak a vállalati hálózathoz betárcsázós kapcsolaton (dial-up connection), illetve VPN (virtuális magánhálózat) használatával az interneten keresztül.

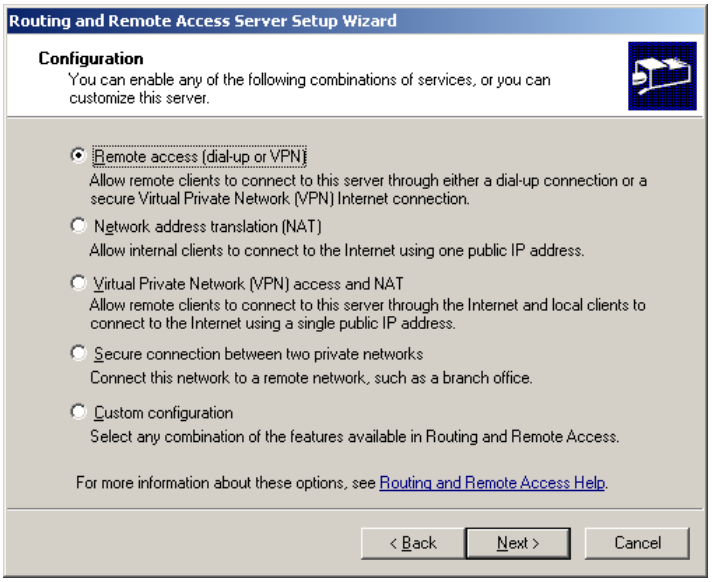
- **Hálózati címfordítás** *(Network address translation, NAT)* – vagyis az RRAS a privát IP-címmel rendelkező gépek számára biztosíthatja az internet elérését, és ezzel kapcsolatban alapfokú tűzfal szerepkör betöltésére is képes. A Network Address Translation *(hálózati címfordítás)* lehetővé teszi, hogy a belső hálózatra kötött, privát IP-címmel rendelkező gépek tetszőleges protokollokon keresztül elérjék az internetet. A hálózati címfordítást végző számítógépben két hálózati csatolóra van szükség, az egyiknek a belső hálózat felé néző privát címmel, a másik-

nak pedig az internethez való közvetlen kapcsolódást biztosító publikus címmel kell rendelkeznie. A belső hálózaton lévő gépek internetes adatforgalomra vonatkozó kéréseit a hálózati címfordítást végző kiszolgáló fogadja, és a beérkező csomagokat az internetre továbbítás előtt úgy módosítja, hogy azok feladójaként a saját publikus IP-címét tünteti fel. Így a csomagok már akadálytalanul eljuthatnak címzettjükhöz. A válaszüzenetek (mivel a csomagok feladója a kiszolgáló volt) szintén hozzá érkeznek be, ezekben most a címzett mezőt kell módosítania a megfelelő privát címre, hogy az eredeti feladó megkaphassa azt. A NAT-szolgáltatást használó ügyfélgépek semmit nem tudnak a csereberéről, vagyis az ügyfeleken semmiféle beállításra nincs szükség.



4.26. ábra: *Az RRAS segítségével megvalósítható kapcsolatok*

- **Telephelyek közötti kapcsolatok** *(Site-to-Site connections)* – az RRAS hálózatok között kapcsolatok megvalósítására is képes, tárcsázós és VPN (állandó, illetve igény szerint tárcsázó [*Dial on Demand, DoD)*] kapcsolódás felhasználásával.
- **LAN-útválasztó** *(LAN router)* – több Ethernet csatoló esetén a belső hálózat szegmensei közötti útválasztó funkció megvalósítása is lehetséges az RRAS használatával.



4.27. ábra: *Az RRAS számos képességgel rendelkezik*

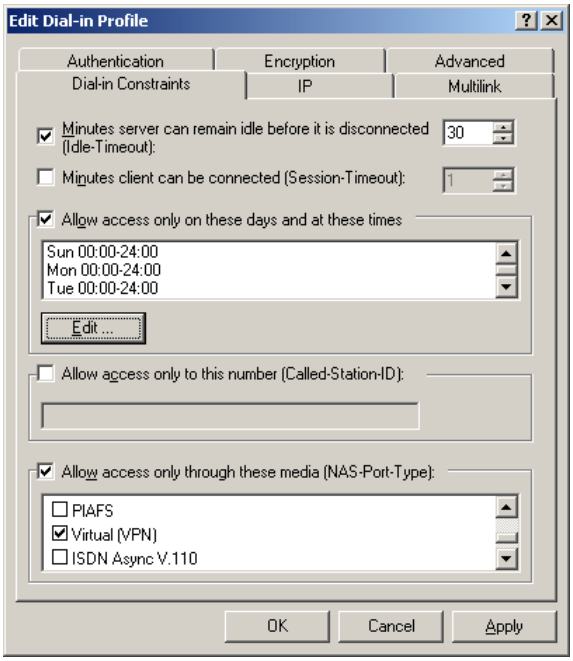
Természetesen a fenti listából nem csak egy tételt választhatunk, az RRAS bármiféle kombinációban képes biztosítani az említett szolgáltatásokat. Az RRAS használatával elérhető teljesítmény (vagyis a megfelelő válaszidővel kiszolgálható kapcsolatok maximális száma) számos tényezőtől függ, de megfelelő hardver és konfiguráció használatával az RRAS képes lehet a közepes kategóriájú hardveres megoldások helyettesítésére.

Az RRAS-szolgáltatás alapértelmezés szerint az operációs rendszer telepítésével együtt felkerül a számítógépre, de ekkor még teljesen kikapcsolt állapotban van. Használat előtt, az engedélyezéssel együtt néhány beállítást is meg kell adnunk, például ki kell választanunk, hogy a RRAS mely funkcióit szeretnénk használni.

Távelérési házirendek

Hiába élesítettük azonban a kiszolgálót, a távoli ügyfelek kapcsolódása még mindig nem lehetséges, mivel a távelérési házirendek *(Remote Connection Policies)* alapértelmezés szerint semmiféle kapcsolatot nem engednek meg. A kapcsolatok engedélyezésével együtt azonban célszerű mindjárt áttekinteni a lehetséges beállításokat, és az éppen elégséges szintre korlátozni a kapcsolódás lehetőségét. Célszerű például megadni azt a tartományi, vagy helyi csoportot, amelynek engedélyezni szeretnénk a távoli hozzáférést.

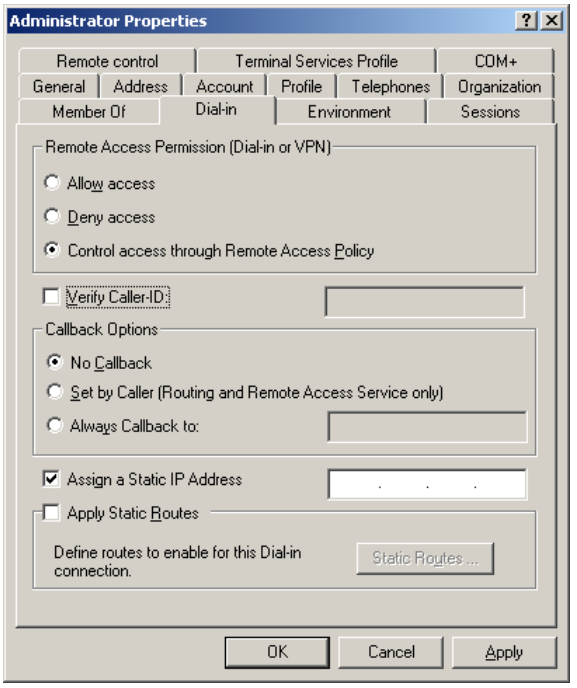
Számos más korlátozás megadására is módunk van, szabályozhatjuk az üresjárati kapcsolatok bontását, megadhatjuk azt az időszakot, amikor a kiszolgáló hajlandó kapcsolatok fogadására stb. Ugyancsak a házirendekben kell beállítanunk a csomagszűrést, valamint a hitelesítésre és a titkosításra vonatkozó paramétereket.



4.28. ábra: *A távelérési házirend beállítása*

Ha több távelérés-kiszolgálót üzemeltetünk, akkor célszerű lehet a közös házirendek használata. A Windows Internetes hitelesítési szolgáltatása *(Internet Authentication Service, IAS)* RADIUS-kiszolgálóként használható, így központosított kapcsolat-hitelesítést és -engedélyezést tesz lehetővé a telefonos és VPN távelérés, az útválasztók közötti kapcsolatok, valamint a vezetéknélküli hálózatok hozzáférési pontjai *(WLAN Acces Points)* számára. A RADIUS a Remote Authentication Dial-In User Service protokoll rövidítése.

Ha a távelérés-kiszolgálót RADIUS-hitelesítés használatára állítjuk be, akkor a rajta tárolt távelérési házirendek helyett a rendszer az IAS-kiszolgálón található házirendeket fogja használni.



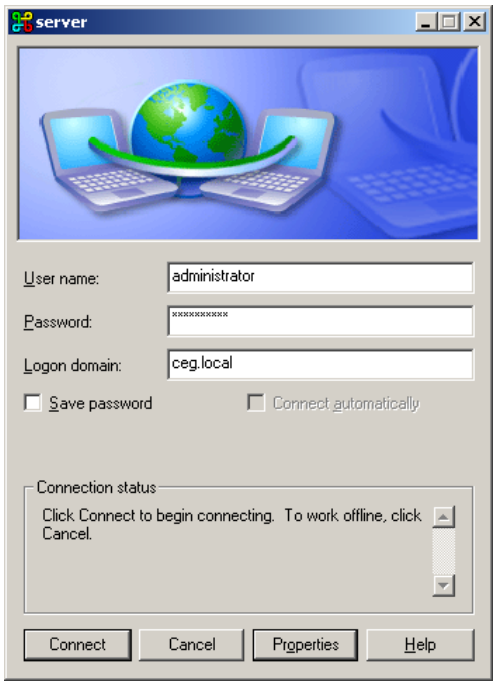
4.29. ábra: *A távoli hozzáférés tulajdonságainak egy része a felhasználó oldaláról szabályozható*

RRAS-beállítások a címtárban

A távoli eléréssel kapcsolatos paraméterek egy részét a hozzáférési házirend mellett, a felhasználók oldaláról a címtárban (Active Directory) is meghatározhatjuk. A tartományi felhasználók tulajdonságlapjának Dial-in *(Behívás)* fülén meghatározhatjuk, hogy az adott felhasználónak legyen-e lehetősége a távoli kapcsolódásra, illetve megadhatjuk azt is, hogy a jogosultság szabályozását a távelérési házirendre bízzuk. Ugyanitt állíthatjuk be az adott felhasználóhoz hozzárendelendő statikus IP-címet, és a csatlakozó számítógép útválasztási tábláját *(routing table)* is kiegészíthetjük az itt megadott bejegyzésekkel. Engedélyezhetjük a betárcsázós kapcsolaton keresztül érkező felhasználók visszahívását (ekkor a cég fizeti a telefonszámlát), illetve megadhatjuk azt a telefonszámot, amelyről az adott felhasználó számára engedélyezzük a csatlakozást.

Connection Manager (*Csatlakozáskezelő)*

A Csatlakozáskezelő sokoldalúan paraméterezhető tárcsázó és kapcsolatfelvételi szoftver, amelynek segítségével az ügyfelek telefonos vagy VPN-kapcsolat kiépítésével csatlakozhatnak az RRAS-kiszolgálóhoz. A Csatlakozáskezelő felügyeleti csomag (Connection Manager Administration Kit, CMAK) segítségével a rendszergazdák olyan, a Csatlakozáskezelő programra épülő csomagokat hozhatnak létre, amelyek tartalmazzák azokat az egyedi paramétereket, amelyekre a hálózathoz való csatlakozáshoz szükség van.



4.30. ábra: *Az előre gyártott tárcsázó csak a felhasználónévre és a jelszóra kíváncsi (esetleg még arra se)*

A csomag részeként rengeteg információ automatikusan eljuthat az ügyfélhez, sőt olyan beállításokat is megtehetünk, amelyekre a „kézi” kapcsolódásnál egyáltalán nincs lehetőség.

Egyedi feliratokat kérhetünk a csatlakozáskor megjelenő ablakba, súgófájlt és különféle telefonszámokat küldhetünk az ügyfeleknek, megadhatjuk a kapcsolódáskor beállítandó TCP/IP paramétereket, előírhatunk biztonsági beállításokat, a kapcsolódás különböző fázisaiban szkripteket indíthatunk stb.

A varázsló segítségével létrehozott, testre szabott telepítőcsomagot (ez tulajdonképpen egy *exe* fájl) az ügyfeleknek eljuttatva (például egy webes letöltés formájában), a felhasználóknak nem kell megadniuk a csatlakozáshoz szükséges különféle paramétereket, mivel ezeket a csomag már tartalmazza, és elvégzi az ügyfélgép szükséges beállításait.

Alapértelmezés szerint a csomagkészítő varázsló nincs feltelepítve, de ezt könnyen pótolhatjuk az Add or Remove Programs *(Programok hozzáadása vagy törlése)* eszköz segítségével. A telepítő a Windows komponensek között lévő Management and Monitoring Tools *(Kezelési és figyelési eszközök)* csoportból indítható.

Telefonos kapcsolódás

A telefonos kapcsolódás azt jelenti, hogy a távoli ügyfél valamiféle kapcsolt vonalon megvalósuló telekommunikációs szolgáltatás (például analóg telefonvonal, ISDN-vonal, vagy X.25 rendszer) segítségével korlátozott ideig fennálló kapcsolatot létesít a távelérés-kiszolgálón lévő valamelyik fizikai porttal. Tipikus példa ilyen kapcsolatra, az analóg telefonvonalra modemmel kapcsolódó ügyfél, aki a távelérés-kiszolgáló egyik fizikai portjához tartozó telefonszámot hív.

Az analóg telefonvonalon vagy ISDN-kapcsolaton keresztül megvalósuló hálózati kapcsolat az ügyfél és a kiszolgáló közötti közvetlen fizikai kapcsolatot jelenti, így nincs feltétlenül szükség az átvitt adatok titkosítására.

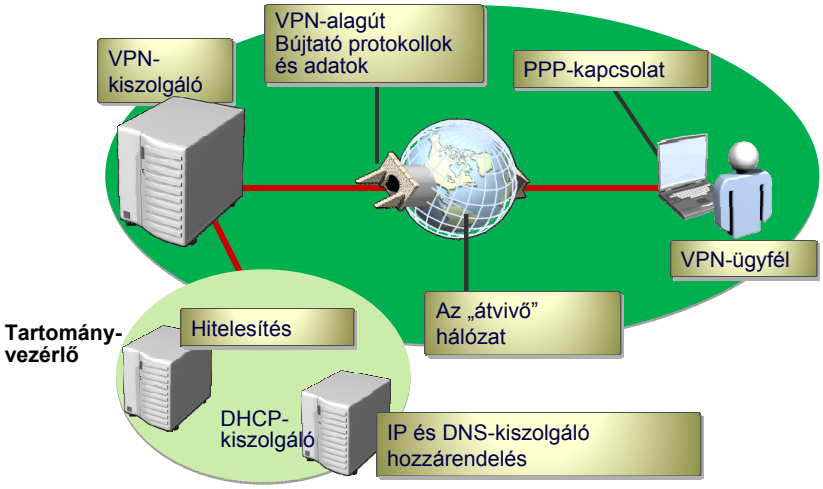
VPN-kapcsolatok

A virtuális magánhálózat *(Virtual Private Network, VPN)* a helyi hálózat olyan kiterjesztése, amely megosztott vagy nyilvános hálózatokon (például az interneten) keresztüli titkosított kapcsolatokat tartalmaz. VPN-kapcsolat használatával úgy küldhetünk adatokat két számítógép között megosztott vagy nyilvános hálózaton keresztül, mintha a két gép közvetlen kapcsolatban lenne egymással. A VPN-kapcsolatot kiépítő számítógép, gyakorlatilag a belső hálózat része lesz (a hálózaton belüli privát IP-címet kap akkor is, ha az interneten keresztül csatlakozik), és hozzáférhet minden olyan szolgáltatáshoz (például fájlmegosztások, DNS-kiszolgáló, címtár stb.), amelyek a vállalat többi számítógépe számára elérhetőek.

A közvetlen kapcsolat emulálása érdekében az átvitt adatokhoz hozzáfűződik egy fejléc (ezt a műveletet nevezzük beágyazásnak), amely a végpont megosztott vagy nyilvános hálózaton keresztül történő eléréséhez szükséges útvonalra (ezt nevezzük VPN-alagútnak) vonatkozó információkat tartalmazza. A VPN-kapcsolatokon átvitt adatok biztonsági szempontok miatt minden esetben titkosítva vannak, így a titkosító kulcsok nélkül az esetlegesen elfogott csomagok megfejthetetlenek.

A mobil, illetve az otthon dolgozó felhasználók VPN-kapcsolatok segítségével nyilvános hálózatokon keresztül tudnak távelérésű kapcsolatot létesíteni vállalatuk távelérési-kiszolgálójával. A felhasználó szempontjából a VPN-kapcsolat közvetlen kapcsolatként jelenik meg a számítógépe (a VPN-ügyfél) és a VPN-kiszolgáló virtuális portjai (és így a belső hálózat) között. VPN-kapcsolatok használata esetén az egyidejű hozzáférések számát csak a kiszolgáló erőforrásai korlátozzák (meg persze a vállalat internetkapcsolatának sávszélessége).

A megosztott vagy nyilvános hálózat pontos infrastruktúrája lényegtelen, mert az adatok logikailag egy állandó összeköttetésű kapcsolaton keresztül közlekednek.



4.31. ábra: *VPN-infrastruktúra*

A VPN-kapcsolatok segítségével a szervezetek földrajzilag különálló irodákkal, vagy más szervezetekkel is létesíthetnek kapcsolatot nyilvános hálózaton keresztül úgy, hogy a kommunikáció biztonságos maradjon. Az interneten keresztüli VPN-kapcsolat logikailag úgy működik, mintha állandó összeköttetésű WAN-kapcsolat (például bérelt vonal) lenne. Ha például mindkét telephely állandó kapcsolattal csatlakozik az internethez, a kapcsolódást kezdeményező ügyfél telephelyének VPN-kiszolgálója automatikusan felépíti a virtuális kapcsolatot és elérhetővé teszi a másik telephely hálózatát, méghozzá olyan módon, hogy az ügyfélgépek (és a felhasználók) ebből semmit nem vesznek észre. Ebben az esetben a VPN-kiszolgálók egyben útválasztóként is működnek, vagyis biztosítják a mögöttük lévő teljes hálózat elérését a másik fél számára. Természetesen nem szükséges, hogy mindkét oldalon RRAS legyen a VPN-kiszolgáló, használhatóak a hardveres megoldások (például egy ADSL router) is.

A fizikai kapcsolatot jelentő telefonos hálózattal szemben, a virtuális magánhálózat mindig logikai, közvetett kapcsolat a virtuális magánhálózati ügyfél és a kiszolgáló virtuális portja között, így VPN-kapcsolatok esetén a biztonságos átvitelhez az adatok titkosítására van szükség.

VPN-protokollok

A PPP (Point-to-Point Protocol) olyan szabványos protokollkészlet, amely lehetővé teszi a távelérést biztosító különféle szoftverek együttműködését. A PPP használatára képes szoftverek képesek minden olyan hálózathoz csatlakozni, amely szabványos PPP-kiszolgálón keresztül érhető el.

A PPP több LAN-protokoll becsomagolására is képes, így hálózati protokollként a TCP/IP és az IPX is használható. Választhatunk több különféle hitelesítési módszer közül, adataink pedig tömörített és titkosított formában is átvihetők. A PPP az alapja az RRAS által a biztonságos VPN-kapcsolatok létrehozásához használt PPTP és L2TP protokolloknak.

- **PPTP (Point-to-Point Tunneling Protocol,** *pont–pont alagútprotokoll)* – a PPTP a PPP (Point-to-Point Protocol) kiterjesztéseként meghatározható alagútprotokoll. A PPTP-protokoll használatát a Windows 9x-től kezdve valamennyi Windows operációs rendszer támogatja (bár a régebbi rendszerek esetén külön kell letölteni és telepíteni). A PPTP-protokoll beágyazza (vagyis hozzáfűzi a saját fejlécét) és titkosítja az átviendő PPP-keretet az MPPE (Microsoft Point-to-Point Encryption, 128-bites RC4) titkosítás használatával az MS-CHAP, az MS-CHAP v2 vagy az EAP-TLS hitelesítési eljárásból generált titkosító kulcsok segítségével. Az EAP-TLS hitelesítési eljárás a SmartCard-alapú hitelesítést is lehetővé teszi. A PPTP-protokoll egyszerűen NAT-olható (ez akkor lehet fontos, ha például az RRAS mögül szeretnénk kifelé VPN-kapcsolatot létrehozni), beüzemelése egyszerű, használata pedig megfelelő biztonságot nyújt.
- **L2TP (Layer Two Tunneling Protocol,** *második rétegbeli alagútprotokoll)* – az L2TP szintén a PPP-keretek beágyazására képes, de ebben az esetben a titkosítási szolgáltatások a hálózati adatok biztonságos átvitelére szolgáló IPSec-protokollon alapulnak. Az L2TP és az IPSec kombinációja L2TP/IPSec-protokollként ismert. A VPN-ügyfélnek és a kiszolgálónak is támogatnia kell az L2TP és az IPSec-protokollt, vagyis az L2TP használata Windows 2000 és 2003 Server kiszolgálók és Windows 2000/XP/Vista ügyfelek számára lehetséges. Az IPSec tanúsítvány alapú hitelesítést használ, így az L2TP alkalmazásához teljes PKI-infrastruktúrára, vagyis tanúsítványkiadó szolgáltatásra (esetleg a jóval kevésbé

biztonságos előre megosztott kulcson *(pre-shared key)* alapuló hitelesítésre) van szükség, ezért beüzemelése lényegesen bonyolultabb, viszont a tanúsítvány alapú hitelesítés használatával fokozottan biztonságos. További nehézséget jelenthet az, hogy a IPSec nem NAT-olható (mivel a NAT-kiszolgáló módosítja a csomagok fejléceit, amit az IPSec integritásvédelme nem enged meg), csak a NAT-Traversal technológia használatával. A NAT-T működése azon alapul, hogy a VPN-forgalom UDP-csomagok képében utazik, ezek fejléceit a NAT-kiszolgáló már minden további nélkül módosíthatja.

VPN-karantén

A VPN-kapcsolatok használatának számos előnye mellett van egy súlyos hátránya is. A felhasználók számára nagyon jó, hogy bárhonnan, egyszerűen és biztonságosan elérik a vállalat hálózatát, a rendszergazda számára viszont a „bárhonnan" kifejezés komoly fejtörést okozhat. A bárhonnan ugyanis jelentheti például kedves kollégánk otthoni számítógépét is, amin a gyerekek sokat szoktak ugyan internetezni, de frissítve esetleg a múlt évezredben volt utoljára. Hogyan engedhetünk be a hálózatba egy olyan gépet, amin esetleg nincs tűzfal, nincs rendszeresen frissített víruskereső, nincsenek javítócsomagok és csoportházirend, viszont ezekből következően nyilván van rajta sok egyéb érdekesség?

A VPN-karantén arra jó, hogy elvárásainkat konkrét formában közöljük a csatlakozni kívánó számítógépekkel, ha pedig nem teljesítik a feltételeket, akkor rövid úton megszakíthatjuk velük a kapcsolatot. Csatlakozás után minden számítógép a karanténban kezdi pályafutását, vagyis egy erősen korlátozó házirend (IP-szűrők és munkamenet időzítők) beállításai érvényesülnek rá. Például csak annyit érhet el a hálózatból, ami a különféle frissítések és egyéb, a megfelelő állapot eléréséhez szükséges elemek letöltéséhez szükséges. Eközben lefut rajta egy teljesen egyedileg összeállítható ellenőrző szkript, ami megvizsgálja tetszőleges programok, registry-kulcsok, fájlok meglétét, megfelelő eredmény esetén feloldja a karantén korlátozásait és a szokásos távelérési házirendet érvényesíti kapcsolatra. A VPN-karantén létrehozásához szükséges eszközök a Windows Server 2003 Resource Kit Tools csomagban *(http://tinyurl.com/6p6cy)* találhatók.

A csomagból négy fájlra lesz szükségünk: *Rqs.exe* (Remote Quarantine Server), *Rqc.exe* (Remote Quarantine Client), *Rqs_setup.bat* (a Remote Access Quarantine Agent szolgáltatás telepítője (a kiszolgálón) és *RqsMsg.dll* (Remote Access Quarantine Agent Message). A csomag telepítése után célszerű frissíteni az *RQS.exe*-t a *http://tinyurl.com/dc2u7* címről letölthető példánnyal.

Terminálszolgáltatások és Távoli asztal

A Windows Server 2003 Terminal Services *(Terminálszolgáltatások)* segítségével elérhetővé tehetjük a Windows-alapú alkalmazásokat, vagy a Windows Asztalt magát szinte bármilyen számítógépről, még azokról is, amelyek nem Windows operációs rendszert futtatnak. A Terminálszolgáltatások csak a program felhasználói felületét továbbítja az ügyfélhez, az pedig a billentyűzet- és az egérmozgatás jeleit küldi vissza a kiszolgálóra, maguk az alkalmazások a kiszolgálón futnak. A kiszolgáló operációs rendszere a felhasználó számára láthatatlanul, és egymástól függetlenül kezeli az ügyfélmunkameneteket. A csatlakozáshoz szükséges ügyfélszoftver számos hardvereszközön futhat, beleértve a számítógépeket és a Windows alapú terminálokat. Egy kiegészítő szoftver segítségével más eszközök, például Macintosh számítógépek vagy UNIX alapú munkaállomások is csatlakozhatnak a terminálkiszolgálóhoz.

Távoli asztal kapcsolatok és a Remote Desktops konzol
Ebben a screencastban engedélyezzük a kiszolgálóhoz való távoli kapcsolódást és megismerkedünk az előre beállított kapcsolatok kezelését megkönnyítő Remote Destops konzollal.
Fájlnév: II-1-2d-RDP.avi

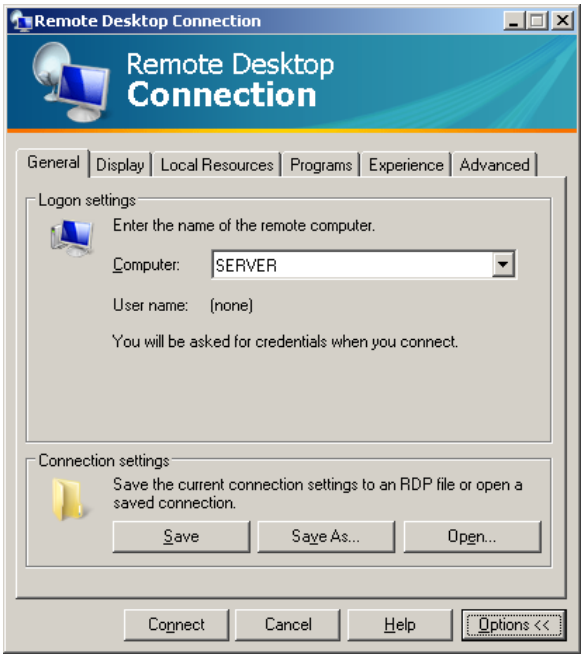
Terminálkiszolgáló használatával, a nagy adatmennyiséggel dolgozó alkalmazásokat is futtathatjuk korlátozott sávszélességet biztosító környezetben (telefonvonal vagy megosztott WAN-kapcsolat), mivel így az adatok helyett csak azok képernyőn megjelenő képét kell átvinnünk a hálózaton. A Terminálszolgáltatások *(Terminal Services)* használata nem igényel túl nagy sávszélességet (akár egy betárcsázós kapcsolaton keresztül is használható), mivel a képernyőképek helyett a képek létrehozásához használt ablakrajzoló parancsokat (GDI, Graphical Device Interface) viszi át a Remote Desktop Protocol (RDP).

A terminálszolgáltatások két különböző üzemmódban futtatható, bár a különbség csak a licencfeltételekben van, az alkalmazott technológia mindkét esetben azonos:

- **Távoli asztal** *(Remote Desktop)* – a távoli asztal a terminálszolgáltatások távfelügyeleti üzemmódja, leginkább arra szolgál, hogy a rendszergazdának ne kelljen a hideg és huzatos szerverszobában üldögélnie akkor sem, ha egészen komoly műtétet kell elvégezni a kiszolgálón. A szolgáltatás használatához nincs szükség telepítésre, egyszerűen a Rendszer *(System)* tulajdonságpanel Távoli használat *(Remote)* lapján engedélyezhetjük a távoli asztalhoz való kapcsolódást. Ebben az esetben a Windows Server 2003 két párhuzamos távoli munkamenet fogadására hajlandó, illetve csatlakozhatunk a konzol munkamenethez is (akár a gép előtt ülve,

akár távolról). A konzol munkamenethez azonban egy időben csak egyetlen felhasználó csatlakozhat, ha ezt egy távoli munkamenet foglalja el, akkor lokálisan már nem lehet a gépre bejelentkezni. Ez a szolgáltatás ügyfélrendszerek esetében is használható (Windows XP és Vista), de ott mindössze egyetlen kapcsolatra van lehetőség (a helyi munkamenettel együtt), vagyis sajnos nem tudunk a felhasználó megzavarása nélkül, vele párhuzamosan bejelentkezni az ügyfélgépekre.

- **Terminálkiszolgáló** *(Terminal Server)* – a terminálkiszolgáló üzemmód csak kiszolgáló operációs rendszereken használható, de ebben az esetben a kapcsolatok számát csak a megvásárolt ügyféllicencek száma, és a számítógép erőforrásai korlátozzák. A licenc kiszolgáló beüzemelésére és az ügyféllicencek megvásárlására 120 nap türelmi időt kapunk. A Terminálszolgáltatások aktiválásához a Terminal Server komponenst kell feltelepítenünk a Programok telepítése és törlése *(Add or Remove Programs)* varázsló segítségével.



4.32. ábra: *Az RDC 6.0 telepíthető a Windows Server 2003-ra, és Windows XP-re is*

A Terminálszolgáltatásokhoz a Remote Desktop Users *(Távoli asztal felhasználói)* biztonsági csoport tagjai csatlakozhatnak, illetve tartományvezérlő esetén figyelembe kell vennünk azt is, hogy alapértelmezés szerint sem a Users, sem pedig a Remote Desktop Users *(Asztal távoli felhasználói)* csoport tagjai-

nak nincs helyi bejelentkezési joga a kiszolgálóra, így nem használhatják a terminálkiszolgálót sem. További problémákat okozhat az a tény, hogy üres jelszóval egyáltalán nem lehet bejelentkezni terminál munkamenetbe, még akkor sem, ha a konzolon ez lehetséges.

A Terminálszolgáltatások ügyfélprogramjának *(Remote Desktop Connection, RDC)* 6.0-ás, legújabb verziója számos újdonságot tartalmaz a korábbi kiadásokhoz képest. Az RDC-program segítségével csatlakozhatunk a Windows-kiszolgálókon futó terminálszolgáltatásokhoz, és az ügyfélgépek távoli asztalához is. Windows XP és Windows Server 2003 esetén az ügyfélprogram 5.2-es verziójával találkozhatunk, de ezekre a rendszerekre is letölthető (az automatikus frissítés segítségével is) a Vistában megjelent 6.0 változat is. A program az mstsc.exe parancs beírásával, illetve a Start menüből indítható.

Az ügyfélprogram és a kiszolgáló között alapértelmezés szerint 128-bites kétirányú RC4 titkosítás védi az adatokat, de ha nem tiltjuk le, lehetséges a régebbi, alacsonyabb titkosítási szintet biztosító ügyfelek csatlakozása is.

A távoli kapcsolatok különféle opciói az Options *(Beállítások)* gomb segítségével érhetők el. A megnyíló tulajdonságlapon megadhatjuk a bejelentkezéssel, a megjelenítéssel, a helyi erőforrásokkal és a munkamenet létrehozáskor automatikusan elinduló programokkal kapcsolatos adatokat. Az RDC segítségével a felhasználók és rendszergazdák elmenthetik és betölthetik a kapcsolatok beállításait tartalmazó, *rdp* kiterjesztésű fájlokat.

Az RDC-program segítségével számos adattípus átirányítását megvalósíthatjuk. Biztonsági okokból minden átirányítás az ügyfélen és a kiszolgálón is letiltható. Figyelmeztető üzenet jelenik meg a fájlrendszerre, valamely portra, vagy smart card-ra vonatkozó átirányítási kérelemkor; a felhasználó megszakíthatja a kapcsolatot, vagy letilthatja az átirányítást.

A következő átirányításokat állíthatjuk be:

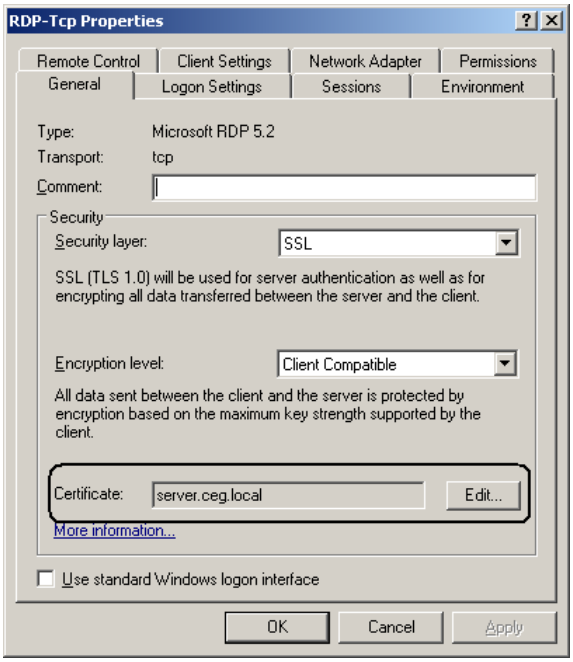
- **Fájlrendszer** – Az ügyfél meghajtói (a hálózati meghajtók is) elérhetők a kiszolgálói munkamenetből. Az engedély egyszerre az összes meghajtóra vonatkozik, ráadásul alapértelmezés szerint a kiszolgálói munkamenetben Everyone > Full Control jogosultsággal jelennek meg az ügyfélgép meghajtói, így az átirányítás használatához némi óvatosság szükséges.
- **Vágólap** – Lehetőség van (csak RDP 6.0 esetén) a vágólap megosztásának engedélyezésére és tiltására, vagyis ilyen módon nagyon egyszerűen cserélhetünk szövegeket és képeket a helyi gép és távoli munkamenet között. Fájlok átvitele viszont nem lehetséges a vágólap használatával.

- **Portok** – Az ügyfél soros portjai elérhetővé tehetők a kiszolgálói munkamenetből, így a kiszolgálón futó szoftverek hozzáférhetnek az ügyfél bizonyos hardvereszközeihez.
- **Nyomtatók** – Az ügyfél valamennyi telepített nyomtatója (a hálózati nyomtatók is) elérhető a kiszolgálói munkamenetből (a Windows 2000 Terminálszolgáltatások csak a helyi nyomtatók átirányítását tette lehetővé). Az átirányított nyomtatók könnyen értelmezhető nevet kapnak.
- **Hangok** – A hibaüzenetekhez kapcsolódó hangjelzések, vagy például az új elektronikus levél érkezését jelző hangok átirányíthatók az ügyfelekre.
- **Smart Card bejelentkezés** – A Windows-rendszer bejelentkezési adatait tartalmazó smart card használható a Windows Server 2003 távoli munkamenetbe történő bejelentkezéshez is. A funkció használatához olyan ügyfél rendszer szükséges, amely önállóan is képes a smart card kezelésére (Windows 2000, XP, Vista).
- **Windows billentyűkombinációk** – Az ügyfél a Windows billentyűkombinációkat *(Alt-Tab, Ctrl-Esc* stb.) alapértelmezés szerint továbbítja a távoli munkamenetnek. A Ctrl-Alt-Del billentyűkombinációt azonban biztonsági okokból mindig az ügyfél dolgozza fel, a kiszolgálón a Ctrl-Alt-End megnyomásával érhetjük el ugyanazt a hatást. Az átirányítás működik Windows 2000 terminálkiszolgáló esetén is, de csak NT-alapú ügyfél operációs rendszerrel (Windows 9x-el nem).
- **Időzóna** – Az RDC-ügyfél képes az időzónára vonatkozó adatok automatikus átadására, illetve a felhasználók manuálisan is beállíthatják a megfelelő időzónát. Így a különböző időzónában lévő felhasználók egyetlen kiszolgálót használhatnak.

Nagyszámú kapcsolat kényelmes kezelését biztosítja a Remote Desktops MMC-konzol, amelyet az Administrative Tools *(Felügyeleti eszközök)* programcsoportból indíthatunk el. A konzolfához hozzáadhatjuk a szükséges kapcsolatokat, beállíthatjuk azok tulajdonságait, megadhatjuk a szükséges felhasználóneveket és jelszavakat. A csatlakoztatott kiszolgálók képernyőképe a konzolon belül jelenik meg. A konzol a korábban már említett Administrative Tools csomag *(adminpak.msi)* telepítése után ügyfélgépeken is használható.

RDP over SSL

A Windows Server 2003 SP1 verziójában jelent meg az a lehetőség, hogy SSL (Secure Socket Layer) protokollt használhatunk az RDP-kapcsolódás hitelesítéséhez és az átvitt adatok titkosításához. Az SSL-kapcsolat kiépítéséhez azonban szükség van egy digitális számítógép-tanúsítványra, amit természetesen beszerezhetünk valamelyik elismert hitelesítés-szolgáltatótól vagy a vállalat saját PKI-infrastruktúrájától, de a SelfSSL.exe program használatával önaláírt tanúsítványt is készíthetünk. (A SelfSSL.exe a *http://tinyurl.com/27n8qs* címről letölthető Internet Information Services (IIS) 6.0 Resource Kit Tools csomagban található). Az elkészített (vagy megvásárolt) tanúsítványt *(Certificate)* kiválasztva már elérhető az SSL-beállítás.

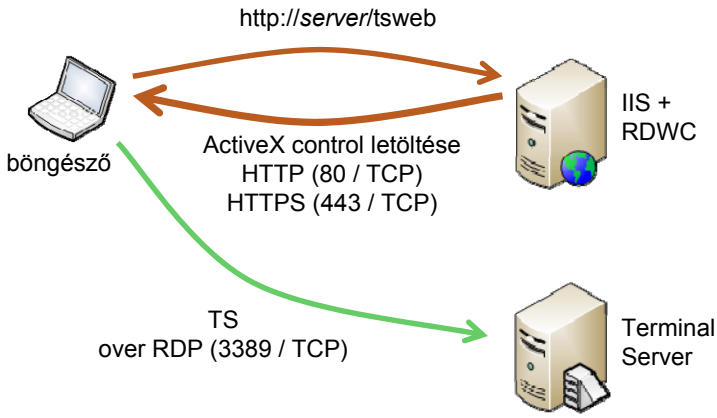


4.33. ábra: *Ha megadjuk a szükséges tanúsítványt, akkor SSL használatával is kapcsolódhatunk a terminálkiszolgálóhoz*

Ügyféloldalon az SSL-kapcsolat használatához Windows 2000, XP, illetve Windows Server 2003 operációs rendszerre, és legalább 5.2-es verziójú RDP-ügyfélre van szükség. Természetesen az is szükséges, hogy a kiszolgáló tanúsítványának kibocsátója, (illetve a kibocsátó root CA-ja) szerepeljen az ügyfél által hitelesnek tekintett tanúsítvány-szolgáltatók között.

Távoli asztal webkapcsolat *(Remote Desktop Web Connection)*

Az Internet Information Server (IIS) webkiszolgáló komponensének részeként telepíthető egy webes (ActiveX) terminálügyfél (nem feltétlenül a terminálkiszolgálóra), amelynek segítségével olyan rendszerekről is elérhetőek a vállalat terminálkiszolgálói, amelyekre nincs RDP-ügyfél telepítve (nincsen például Windows 2000 rendszeren sem). A webes ügyfél persze nem igazi webes alkalmazás, a webes (http, vagy https) csatlakozás csak az ActiveX alapú program letöltéséhez szükséges, ami ezután már a szokásos (3389) RDP-porton kapcsolódik a kiszolgálóhoz, de nem támogatja az RDP over SSL használatát. Telepítés után az ActiveX-ügyfél a http://server/tsweb címen érhető el.



4.34. ábra: *Webes letöltés formájában is rendelkezésre áll egy terminálügyfél*

Egyéb kiszolgálókomponensek

A következőkben a Windows Server 2003 további kiszolgáló-komponensének (SMTP és POP3 kiszolgáló, Tanúsítványszolgáltatások, Internet Information Services, Windows SharePoint Services és Streaming Media Server) egészen rövid, csak a legfontosabb funkciók felsorolására szorítkozó leírása következik. Utolsó témánk, a Windows Server Update Services (WSUS) esetében azonban már a részletekbe is belemegyünk, mert bár a szoftver nem része az alaptelepítésnek, de a kis és közepes vállalatok esetében egy patch management rendszer központjaként nagyon jól használható, és teljesen komplex megoldást nyújt.

Levelezési szolgáltatások (SMTP- és POP3-kiszolgáló)

A Windows Server 2003 önállóan (Exchange Server nélkül) is képes levelezési szolgáltatások biztosítására, a szokásos SMTP-protokoll (Simple Mail Transfer Protocol) biztosítja a levélküldés, a POP3-protokoll (Post Office Protocol) pedig a postafiókok elérésének, és az üzenetek letöltésének lehetőségét. A POP3-szolgáltatás gyakorlatilag minden levelezőprogramból elérhető (Outlook, Outlook Express stb.), így a felhasználók bármilyen ügyfélrendszer használata esetén is hozzáférhetnek leveleikhez.

A levelezési szolgáltatás két önálló kiszolgáló komponensből áll, így beállításaikat is két különböző helyen kell megadnunk (az SMTP-kiszolgáló önállóan is telepíthető). A komponenseket a Configure Your Server Wizard *(Kiszolgáló konfigurálása varázsló)* felületéről (Mail Server), illetve az Add or Remove Programs *(Programok telepítése vagy eltávolítása)* használatával is telepíthetjük.

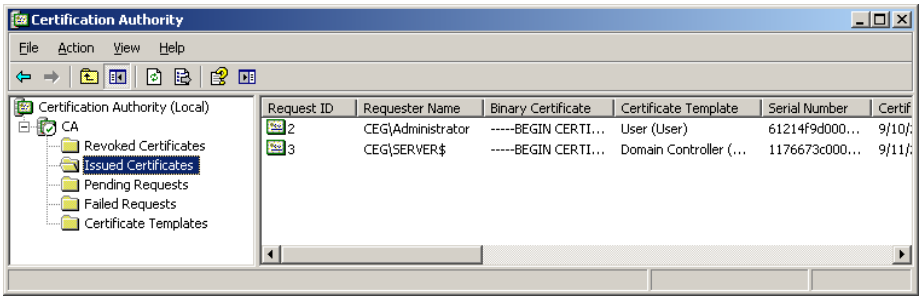
- **SMTP-kiszolgáló** – a leveleket a feladótól a címzett postaládájáig az SMTP-kiszolgálók továbbítják. A felhasználó levelezőprogramja az elküldendő üzenetet átadja a SMTP-kiszolgálónak, az pedig a cím alapján (esetleg több másik kiszolgáló közreműködésével) eljuttatja azt a címzett kiszolgálójáig. A címzett kiszolgálója fogadja a beérkező leveleket, és továbbítja azokat a megfelelő felhasználó postaládájába. A Windows SMTP-kiszolgálója az IIS (Internet Information Services) része, így beállítási lehetőségeit az IIS felügyeleti konzolján találhatjuk meg (Administrative Tools -> IIS Manager). A virtuális SMTP kiszolgálók (több virtuális kiszolgálót is létrehozhatunk, és mindegyik kiszolgáló több e-mail tartomány kezelésére képes) tulajdonságlapján adhatjuk meg a naplózásra, a hozzáférési jogokra, az üzenetek továbbítására stb. vonatkozó különféle beállításokat.
- **POP3-kiszolgáló** – a levelezőprogramok a POP3-szolgáltatás segítségével tölthetik le a felhasználók postaládáiban lévő leveleket az ügyfélgépekre. A levelezőprogram elküldi a felhasználó hitelesítő adatait a POP3-kiszolgálónak, az pedig átadja a megfelelő postaládában lévő üzeneteket. A POP3 szolgáltatás képes az Active Directory-integrált hitelesítés használatára, vagyis a tartományi felhasználók (miután létrehoztuk a felhasználóhoz tartozó postafiókot), a megszokott felhasználónevük és jelszavuk használatával érhetik el üzeneteiket. A sikeres letöltés után az üzenetek törlődnek a kiszolgáló által tárolt postaládából (hacsak az ügyfélprogram nem rendelkezik másképp). A POP3-kiszolgáló felügyeleti felülete az Administrative Tools -> POP3 Service menüpont segítségével érhető el. Itt adhatjuk meg a kiszolgáló által kezelt e-mail tartományok nevét, és itt hozhatjuk létre az egyes felhasználók postaládáit. A POP3-

szolgáltatás telepítésével az SMTP-szolgáltatás is automatikusan települ, hogy a levélküldés is lehetővé váljon a POP3-ügyfelek számára, a POP3 Manager felületén megadott e-mail tartományok pedig automatikusan bekerülnek az SMTP-szolgáltatásba is.

Tanúsítványszolgáltatás *(Certification Authority)*

A tanúsítvány a hitelesítés szolgáltató szervezet által elektronikusan aláírt dokumentum, mely tartalmazza a tanúsítvány tulajdonosának azonosítására szolgáló adatokat (pl. név) és a tulajdonos nyilvános kulcsát. A szolgáltató a tanúsítvány segítségével igazolja, hogy a tanúsítvány tulajdonosa létezik, és valóban az, akinek állítja magát.

A Windows tanúsítványszolgáltatásainak segítségével a vállalaton belül hozhatunk létre olyan hitelesítés szolgáltatót, (illetve hitelesítés szolgáltatókból álló hierarchiát), amely fogadja a felhasználóktól, illetve számítógépektől érkező tanúsítványkérelmeket, ellenőrzi a kérelemben lévő információkat és az igénylő azonosítóját, kiadja a megfelelő tanúsítványokat, és elérhetővé teszi a visszavont tanúsítványok listáját *(Certificate Revocation List, CRL)*. A Tanúsítványszolgáltatás képes a nyilvános kulcsú technológiát alkalmazó biztonsági rendszerekben használt tanúsítványok kiállításának és kezelésének teljes körű megvalósítására, így alapja lehet a vállalat nyilvános kulcsú infrastruktúrájának *(Public Key Infrastructure, PKI)*.



4.35. ábra: *A CA által kiadott felhasználói és számítógép tanúsítvány*

A vállalati hitelesítés szolgáltató által kiadott tanúsítványok segítségével létrehozhatóak digitális aláírások, lehetővé válik a webes adatforgalom biztonságossá tétele a Secure Socket Layer (SSL), vagy a Transport Layer Security (TLS) használatával, az Active Directory alapú tartományba való bejelentkezéshez pedig Smart Card is használható.

A tanúsítványszolgáltatás telepítését az Add or Remove Programs eszköz segítségével végezhetjük el, felügyeletéhez pedig az Administrative Tools -> Certification Authority menüpont segítségével elindítható MMC-konzol használható.

A felhasználók tanúsítványaikat egy webes felületen, vagy a Tanúsítványok *(Certificates)* nevű MMC-modul segítségével igényelhetik a CA-tól, illetve lehetőség van arra is, hogy a különféle alkalmazások észrevétlenül igényeljenek tanúsítványt a felhasználó számára.

Internet Information Services 6.0

Az Internet Information Services (IIS) 6.0 szolgáltatás a Microsoft Windows Server 2003 integrált, megbízható, biztonságos és jól kezelhető alkalmazáskiszolgáló komponense. Az IIS képes weboldalak, FTP-helyek tárolására és kezelésére, hírek és levelek küldésére a Network News Transfer Protocol (NNTP) és a Simple Mail Transfer Protocol (SMTP) protokollok felhasználásával.

Az Internet Information Services kezelése
Ebben a screncastban megismerkedünk az IIS különféle komponenseihez kapcsolódó beállítási lehetőségekkel.
Fájlnév: II-1-3a-IIS.avi

Az IIS tehát a következő alapkomponensekből áll:

- **Web- és alkalmazáskiszolgáló** – a HTML alapú tartalmak szolgáltatásához. A webkiszolgáló lehetővé teszi több egymástól teljesen független webhely üzemeltetését. A hozzá tartozó felügyeleti konzol segítségével beállíthatjuk a biztonsági paramétereket, illetve monitorozhatjuk, felügyelhetjük az egyes webhelyeket. Számos más kiszolgáló komponens is igénybe veszi a webkiszolgáló szolgáltatásait, erre épül például a Windows SharePoint Services és a WSUS is.
- **FTP-kiszolgáló (File Transfer Protocol) –** a fájl le- és feltöltéshez. A komponens segítségével a kiszolgáló meghatározott mappáit tehetjük elérhetővé az FTP-alapú fel és letöltések számára. Az FTP-kiszolgáló képes több (látszólag) önálló FTP-hely kezelésére (különböző hálózati csatolókon, illetve portokon keresztül), és minden helyhez tetszőleges számú virtuális könyvtárat csatolhatunk. Ez azt jelenti, hogy az FTP-ügyfél (például Internet Explorer) segítségével csatlakozó felhasználók egy virtuális könyvtárfát látnak, amelynek elemei a számítógép tetszőlegesen megadott fizikai mappáira néznek. Az FTP-kiszolgálóhoz a számítógépen, (illetve az Active Directoryban) megadott felhasználók csat-

lakozhatnak, viszont mivel az FTP-ügyfelek igen kevéssé biztonságos kódolással (ASCII☺) küldik át jelszavainkat a hálózaton, indokolt lehet némi óvatosság. Beállíthatjuk például, hogy csak hitelesítés nélküli *(Anonymous)* felhasználók jelentkezhessenek be, így nem utaznak a hálózaton könnyen elolvasható jelszavak, viszont nincs mód az FTP-ügyfelek megkülönböztetésére. Korlátozhatjuk a hozzáférést az ügyfelek IP-címe alapján, és lehetőség van a közzétett fájlok hozzáférési jogosultságok beállítására is. Az FTP-könyvtárakhoz való hozzáférési jogok bizonyos mértékig az FTP-kiszolgáló szintjén is szabályozhatók (olvasás, írás), de természetesen a fájlrendszerben megadott NTFS-jogok is érvényesülnek.

- **NNTP-kiszolgáló (Network News Transfer Protocol)** – a hírcsoportok létrehozását és elérését teszi lehetővé.
- **SMTP-kiszolgáló (Simple Mail Transfer Protocol)** – az elektronikus levelek küldésére, illetve továbbításra használható.

A Biztonsági megfontolások miatt az IIS alapértelmezés szerint nincsen telepítve a Windows Server 2003 kiszolgálókon. A telepítést az Add or Remove Programs Windows *(Programok telepítése vagy törlése)* Components szakaszában indíthatjuk el (ügyeljünk a szükséges komponensek kiválogatására, mivel az IIS rengeteg önállóan telepíthető részből áll). Az IIS 6.0 a telepítés után zárolt üzemmódban fut, ami azt jelenti, hogy csak a statikus weboldalak kiszolgálása engedélyezett. Az IIS-re épülő egyéb szolgáltatások (ASP, ASP.NET, CGI parancsfájlkezelés, WebDAV stb.) tiltott állapotban vannak, nem használhatók. Ezeket a szolgáltatásokat, ha szükség van rájuk az IIS Manager *(IIS-kezelő)* Web Sevice Extensions *(Webszolgáltatás-bővítmények)* lapján egyenként engedélyezhetjük.

Windows SharePoint Services

A Windows SharePoint Services (a SharePoint Portal Server kistestvére) olyan központi csoportmunka alkalmazás, amely lehetővé teszi a különféle információk, dokumentumok, feladatok és események megosztását.

A Windows SharePoint Services 2.0 a Windows kiszolgáló operációs rendszerek R2 verzióiban már beépített komponens, és szabadon letölthető *(http://tinyurl.com/2mtgdc)* a legújabb (3.0) verzió is, amelynek telepítéséhez minimálisan Windows Server 2003 SP1 szükséges.

A SharePoint webhelyeken a felhasználók létrehozhatnak dokumentumtárakat, webnaplókat, vitafórumokat, közzétehetnek naptárakat és feladatlistákat. A SharePoint helyek webkijelzőkből és más ASP.NET alapú komponensekből épülnek fel, a kijelzők elhelyezésével és tulajdonságaik beállításával a rendszergazdák és felhasználók teljes alkalmazásokat készíthetnek el egy-egy oldalon. A Windows SharePoint Services számos előre gyártott webkijelzőt is tartalmaz, a jövőben pedig újabbak is fognak készülni.

A Windows Share Point Services telepítése és beállításai
Ebben a screencastben feltelepítjük, beállítjuk és kipróbáljuk a Windows Share Point Services csoportmunka alkalmazást.
Fájlnév: II-1-3b-WSS.avi

A SharePoint felületen létrehozható dokumentumtárak használatával a felhasználók egy központi helyen hozhatnak létre, oszthatnak meg és tekinthetnek át dokumentumokat. A dokumentumtárak több fájltípust, illetve alkönyvtárakat is tartalmazhatnak. Ha a felhasználó megnyit egy dokumentumtárat, a benne lévő fájlok webes hivatkozásként jelennek meg, és az ilyen módon tárolt információk közvetlenül elérhetők a különféle Office-alkalmazásokból. A hivatkozásra kattintva az adott dokumentum az Internet Explorer ablakban, vagy a SharePoint Services szolgáltatással kompatibilis alkalmazás ablakában, (például Word 2003, 2007) nyílik meg.

Az Outlook segítségével megtekinthetők a SharePoint helyeken tárolt naptárak és partnerlisták, illetve lehetőséget nyújt dokumentumszerkesztésre és értekezletszervezésre szolgáló helyek létrehozására.

Adatfolyam-kiszolgáló *(Streaming Media Server)*

A Streaming Media Server segítségével hangból és mozgóképből álló tartalmakat „sugározhatunk” az ügyfelek számára a vállalati intraneten, vagy az interneten keresztül. Az ügyfelek lehetnek olyan számítógépek (vagy mobil eszközök), amelyeken a felhasználók egy lejátszóprogram (például a Media Player) segítségével „veszik az adást”, illetve más médiakiszolgálók, amelyek tárolják és továbbosztják a kapott tartalmat.

A kiszolgálói szerepkör a Configure Your Server Wizard *(Kiszolgáló konfigurálása varázsló)* segítségével telepíthető, a további beállításokat pedig az Administrative Tools -> Windows Media Services MMC-konzol segítségével adhatjuk meg.

Windows Server Update Services (WSUS)

A kiszolgálók és ügyfélgépek javítócsomagjainak telepítése még egy kisebb hálózat esetében is szinte reménytelenül nagy terhet ró a rendszergazdára, ha nem használ valamilyen egységes, automatizált, és központilag felügyelhető megoldást a feladat elvégzésére. A javítócsomagok nagy száma miatt a kellő időben történő telepítés ilyen rendszer nélkül gyakorlatilag megoldhatatlan, ezért gyakran csak több hónapos késéssel kerülnek fel a kritikus fontosságú javítások a számítógépekre.

A Windows Server Update Services telepítése és használata
Ezekben a screencastokban feltelepítjük a Windows Software Update Services 3.0 alkalmazást, és elvégezzük a kezdeti beállításokkal kapcsolatos teendőket. Ezen kívül megmutatjuk a WSUS importálási lehetőségeit a Microsoft Update katalógusból, valamint – érdekességképpen – a több WSUS szerveres környezet részleteiből is felvillantunk néhány lehetőséget.
Fájlnév: II-1-3c-WSUS.avi, II-1-3c-WSUS2.avi, II-1-3c-WSUS3.avi

„Kisebb" hálózatok (nagyjából 1000 számítógépig, ám a támogatás felső határa elvileg 20.000 számítógép) esetén a WSUS (Windows Server Update Services) lehet a tökéletes választás, mivel önálló, komplex és ingyenes megoldást jelent. Természetesen más eszközök is képesek a feladat ellátására (például a Microsoft System Center Configuration Manager, vagy System Center Edition terméke), de ezek nagy, illetve középvállalati felhasználásra tervezett szoftverek, kis hálózatok esetén használatuk túlságosan költséges lenne. Egyébként mindkét említett rendszerfelügyeleti szoftvercsomag tartalmazza a WSUS-t, és ezt használja a javítócsomagok kezeléséhez.

Az önálló WSUS-csomag a Microsoft webhelyéről szabadon letölthető, és ingyenesen használható *(http://go.microsoft.com/fwlink/?linkid=89379).* A közelmúltban jelent meg a WSUS 3.0 végleges változata, amely elődjével ellentétben már nem webes, hanem MMC-alapú felügyeleti eszköz segítségével konfigurálható, használata pedig több szempontból is kényelmesebbé és hatékonyabbá vált.

Természetesen akár azt is megtehetnénk, hogy az egyes számítógépekre (Windows 2000 SP2, XP, Vista) telepített AU (*Automatic Updates, Automatikus frissítések)* ügyfélszoftver segítségével minden gép közvetlenül a Microsoft Update (MU) kiszolgálókról töltögeti le külön-külön a frissítéseket, de ez a megoldás csak az otthoni felhasználók igényeinek felel meg.

Ilyen módon ugyanis, ha hálózatunk például ötven gépből áll, a szükségesnél ötvenszer nagyobb adatmennyiséget kell letöltenünk, ami jelentősen megterheli a vállalat internetkapcsolatát (és esetleg a bankszámláját is).

További problémát jelent az is, hogy nincs mód a javítások esetleges „mellékhatásainak" előzetes felderítésére, és a probléma megoldására, mivel a javítócsomagok ellenőrzés nélkül kerülnek fel a vállalat valamennyi számítógépére.

A WSUS-kiszolgáló tulajdonképpen a MU-kiszolgálók, és a gépeinken futó AU-ügyfél közé kerül; egyetlen példányban letölti, és tárolja az ügyfélgépek összes szükséges javítócsomagját, amelyeket így az AU-ügyfelek már nem az internetről, hanem tőle kapnak meg és telepítenek (de csak akkor, ha a rendszergazda erre engedélyt ad).

A teljes rendszer tehát három komponensből áll (bár ebből csak kettő tartozik a mi fennhatóságunk alá):

- A Microsoft Update kiszolgálók biztosítják a szükséges javítócsomagokat.
- A hálózatunkban Windows 2000/2003 kiszolgálóra telepített WSUS-kiszolgáló ezekről tölti le a csomagokat, majd tárolja őket.
- Az ügyfélgépeken (vagy kiszolgálókon) futó AU-ügyfelek az engedélyezett javításokat letöltik a WSUS-kiszolgálóról, és telepítik azokat.

A WSUS üzemeltetése viszonylag egyszerű, szolgáltatásai pedig a legújabb verzióban már szinte minden igényt kielégítenek. A teljes patch management infrastruktúrát felépíthetjük egyetlen kiszolgáló használatával, de lehetőség van a vállalaton belüli WSUS-hierarchia kialakítására is. Bár a WSUS 3.0 már nem webes felügyeleti felügyeletet használ, a szolgáltatás továbbra is az IIS 6.0 használatára épül. Webes alkalmazás tölti le a frissítéseket, tartja karban az SQL adatbázist, és az ügyfelek is egy webszolgáltatás segítségével érik el a számukra kiosztott frissítőcsomagokat.

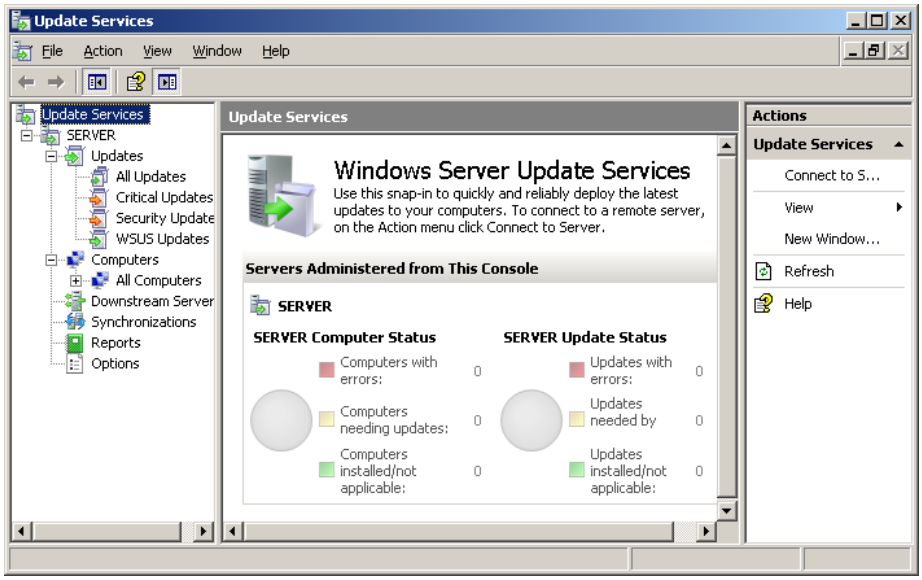
A WSUS telepítése

Hogy a WSUS-t telepíthessük, kiszolgálónknak a következő feltételeket kell teljesítenie:

- Windows Server 2003 Service Pack 1
- Microsoft .NET Framework 2.0
- Internet Information Services (IIS) 6.0
- Microsoft Report Viewer 2005 Redistributable – ez az egy komponens az, amit várhatóan külön kell majd letölteni és telepíteni.
- Microsoft Management Console 3.0
- Opcionálisan SQL Server 2005 SP1

- 1 GB szabad lemezterület a rendszert tartalmazó köteten.
- Minimálisan 20 GB szabad tárolókapacitás a javítócsomagok tárolásához. A szükséges lemezterület erősen függ az ügyfélgépek nyelvi verzióinak számától, mivel minden nyelvhez külön csomagokat kell letölteni és tárolni. A minimálisan ajánlott 20 GB, angol és magyar nyelvű Windows 2000, XP és Vista ügyfelekkel nagyjából elegendő lehet.
- 2 GB szabad terület a rendszer adatbázisának tárolásához. Az adatbázis lehet az SQL Server 2005 SP1 bármelyik kiadása, illetve maga a telepítő is tartalmazza a WMSDE adatbázis-kezelőt.

A telepítés nem mondható túlságosan bonyolultnak, csak néhány kérdésre kell válaszolnunk. Elsőként azt kell eldöntenünk, hogy a teljes kiszolgálót, vagy csak a felügyeleti konzolt szeretnénk telepíteni. Ezután következik a licencszerződés elfogadása, majd meg kell adnunk a letöltött javítócsomagok és a rendszerhez tartozó adatbázis tárolására szolgáló mappákat (mindkettő csak NTFS-köteten lehet). A javítócsomagokat tároló mappát célszerű lehet külön, önálló partícióra helyezni, de mindenesetre lehetőleg ne tegyük a rendszert tartalmazó kötetre. Ez után azt kell kiválasztanunk, hogy a WSUS felügyeleti konzol (és maguk a frissítéscsomagok is) az IIS alapértelmezett webhelyén, vagy külön a WSUS-szolgáltatás számára létrehozott webhelyen legyenek elérhetők.



4.36. ábra: *A WSUS 3.0 MMC-alapú felügyeleti konzolja*

Külön létrehozott webhely esetén az ügyfélszoftver HTTP-protokollon, a 8530-as porton éri el WSUS-kiszolgálónkat, így az ügyfelek beállításakor majd a *http://SERVER:8530* URL-t kell megadnunk.

A telepítés végén azonban a telepítés még nem ér véget, mivel automatikusan elindul a WSUS Server Configuration Wizard *(WSUS-kiszolgáló konfigurálása varázsló)*, amelynek segítségével elvégezhetjük a kiszolgáló beállításának lépéseit. Nem kell azonban feltétlenül a varázslót használnunk, minden beállítási lehetőség elérhető a WSUS 3.0 felügyeleti konzoljáról is, amelyet a Start menü Administrative Tools *(Felügyeleti eszközök)* programcsoportjából indíthatunk el (ugyanitt újra elindíthatjuk a varázslót is).

A konzol természetesen nemcsak a WSUS-kiszolgálón használható, hanem bármelyik ügyfélgépre is telepíthetjük, és lehetőségünk van a felügyeleti jogok delegálására is. Az Active Directory-címtárban, vagy a helyi csoportok között a telepítéskor létrejön a WSUS Administrators *(WSUS-rendszergazdák)*, és a WSUS Reporters *(WSUS-jelentéskészítők)* biztonsági csoport, ezek tagjai teljes jogosultságot, illetve a jelentések elkészítésének lehetőségét kapják.

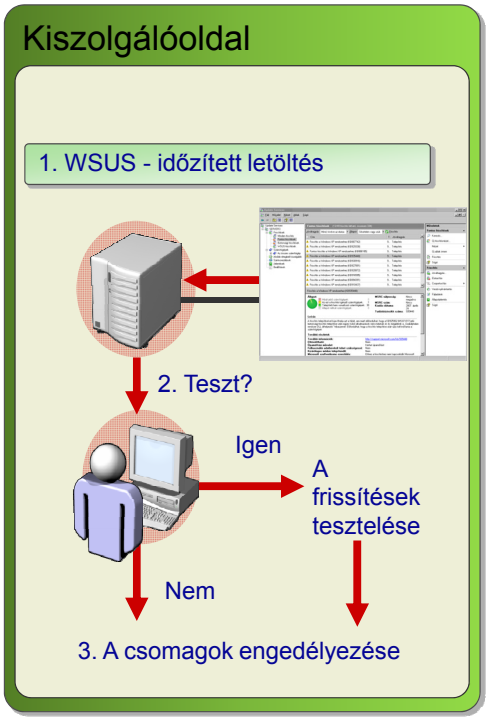
A WSUS-kiszolgáló beállításai

Amint a 4.37. ábra mutatja, a WSUS-kiszolgáló a beállított ütemezésnek megfelelően letölti és eltárolja azoknak a termékeknek a frissítéseit, amelyeket a rendszergazda kiválasztott.

Beállítható automatikus engedélyezés is, ami a megadott feltételek teljesülése esetén a megadott csoportok számára további beavatkozás nélkül engedélyezi a terjesztést, de ezt a lehetőséget csak a kötelező óvatosság figyelembevételével érdemes használni. A tesztgépeinkre például minden további nélkül automatikusan rászabadíthatjuk valamennyi javítócsomagot (éppen ezért vannak), a többi gép esetében pedig az eredmény ismeretében már kézzel végezhetjük el a jóváhagyás beállítását. Beállítható az is, hogy a kevésbé kritikus komponensek (például az Office) valamennyi javítása automatikusan települjön minden gépre. A következőkben áttekintjük a WSUS-kiszolgáló legfontosabb beállítási lehetőségeit, és megismerkedünk az egyes paraméterek jelentésével:

- **Update Source and Proxy Server** *(Frissítés forrása és proxykiszolgáló)* – itt kell kiválasztanunk azt a kiszolgálót, amelyről a WSUS le fogja tölteni a frissítéseket. Kisvállalati környezetben általában nincs szükség több WSUS használatára, de lehetőségünk van a csomagok forrásaként másik kiszolgálót is megadni, így több WSUS-példány használata esetén is csak egyszer kell közvetlenül a Microsofttól letölteni frissítéseket. Ha proxykiszolgálón (például ISA Server) érjük el az internetet, akkor ugyanitt kell megadnunk a kiszolgáló nevét, portszá-

mát, és a kapcsolódáshoz szükséges felhasználói adatokat (természetesen csak akkor, ha a proxy hitelesítést is igényel), hogy a WSUS elérhesse a Microsoft Update kiszolgálókat.



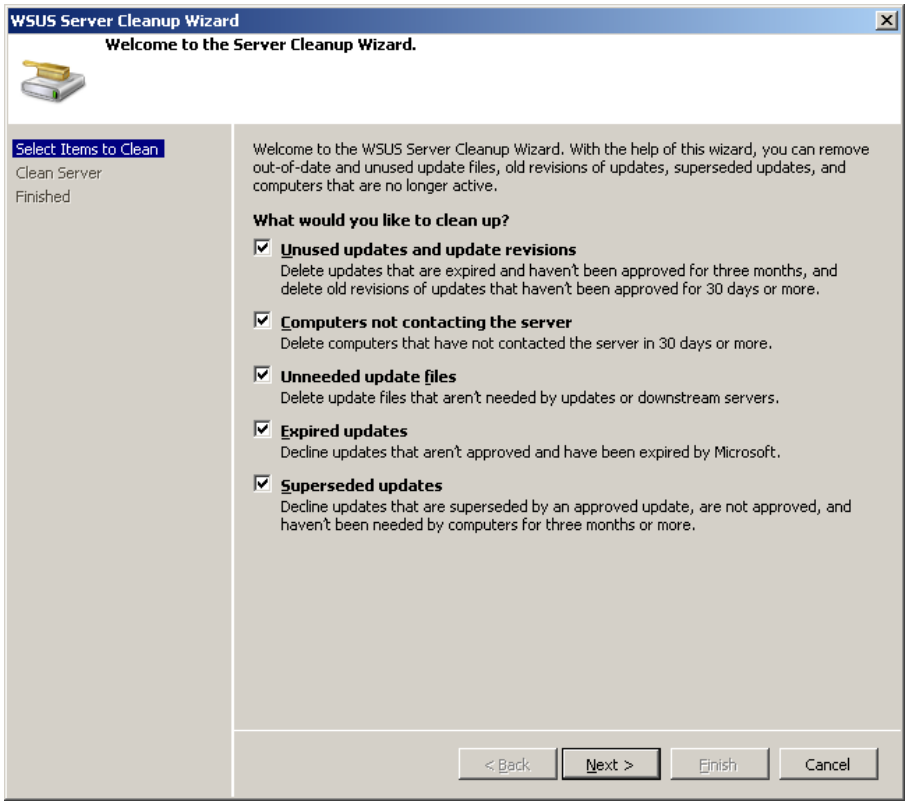
4.37. ábra: *A letöltött csomagokra a rendszergazdának is rá kell bólintania*

- **Products and Classifications** *(Termékek és besorolások)* – itt adhatjuk meg azokat a termékeket, amelyeket A WSUS segítségével szeretnénk frissíteni, illetve itt kell kiválasztanunk a letöltendő csomagok típusát (biztonsági frissítés, javítócsomag stb.). A WSUS gyakorlatilag minden Microsoft termék frissítéseinek kezelésére képes, csak a legfontosabbak: a Windows 2000, XP, Vista valamennyi változata, a Windows Server 2003 különféle kiadásai, Office, Exchange Server, SQL Server, ISA Server, Windows Defender stb.
- **Update File and Languages** *(Frissítésfájlok és nyelvek)* – ebben a szakaszban a frissítőcsomagok letöltésének módját meghatározó paramétereket adhatunk meg, illetve beállíthatjuk azt is, hogy a csomagok maradjanak a Windows Update kiszolgálókon, bár ennek szokványos esetben nyilvánvalóan nincs túl sok értelme. Nagyon fontos pont a letöltendő nyelvi verziók kiválasztása, mivel egyáltalán nem valószínű,

hogy az alapértelmezett viselkedés megfelelő lenne. Ez ugyanis valamennyi nyelv (köztük például az arab, kínai és japán) csomagjainak letöltését jelenti.

- **Synchronization Schedule** *(Szinkronizálás ütemezése)* – A WSUS-kiszolgáló és a Microsoft Update-szolgáltatás szinkronizálása, vagyis a javítócsomagok letöltése történhet automatikusan (ütemezetten), illetve kézi indítással is. Itt választhatunk a két üzemmód között, illetve ütemezett szinkronizáció esetén megadhatjuk a kívánt időpontokat is.
- **Automatic Approvals** (*Automatikus jóváhagyások)* – a letöltött frissítések telepítésének engedélyezése automatikusan is elvégezhető. A módszer (a 3.0-ás változatban) erősen hasonlít például az Outlook levélkezelő szabályaihoz: a frissítés besorolása (biztonsági frissítés, javítócsomag stb.), illetve a frissítendő termék (Office, Windows Vista stb.) alapján kiválogatott csomagokat a kiválasztott csoportok számára automatikusan engedélyezhetjük. A WSUS és az AU-ügyfelek saját frissítései alapértelmezés szerint automatikusan telepítésre kerülnek.
- **Computers** *(Számítógépek)* – egy nagyon fontos beállítást találhatunk itt: ki kell választanunk azt a módszert, amely szerint a WSUS csoportosítani fogja a frissítendő számítógépeket. A csoportosításnak két szempontból is nagy jelentősége van, egyrészt sok ügyfélgép esetén jelentősen javítja az áttekinthetőséget (lehetőség van egymásba ágyazott csoportok létrehozására is, így követhetjük például a vállalat szervezeti egységeinek hierarchiáját), másrészt pedig az automatikus engedélyezést az így kialakított csoportok szerint határozhatjuk meg. A csoportosítás két alapvetően eltérő módszerrel történhet. A csoporttagságot beállíthatjuk közvetlenül a WSUS-konzolon (ebben az esetben tehát a kiszolgáló határozza meg a csoporttagságot), illetve a csoporthoz tartozásukat meghatározhatják maguk az ügyfelek is. A második esetben a kívánt csoportnak a registryben, az AU-ügyfél beállításai között kell szerepelnie, ezt a megfelelő csoportházirend beállítás használatával, vagy esetleg közvetlen registry módosítással érhetjük el. Bármelyik módszert is választjuk, a csoportstruktúrát mindenképpen a WSUS-konzolon kell létrehoznunk. A kiszolgálóoldali csoportosítás elsősorban munkacsoportos környezetben (vagyis viszonylag kevés ügyfélgép esetén) ajánlható, sok számítógép, illetve a csoportosítás gyakori változtatása esetén mindenképpen a csoportházirend használata a megfelelő a csoporthoz tartozás, és a többi ügyfélparaméter beállítására is.

- **Server Cleanup Wizard** *(Kiszolgáló karbantartása varázsló)* – a varázsló segítségével eltávolíthatjuk a kiszolgálóról a zavaró elemeket: a különféle okok miatt lejárt szavatosságú, már nem használt frissítéseket, illetve a csatlakozásra képtelen (például már régen leselejtezett) számítógépeket.



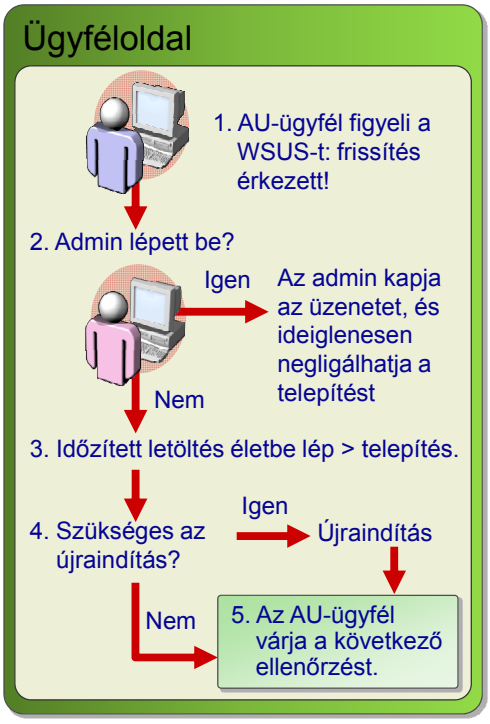
4.38. ábra: *A Server Cleanup Wizard segít a takarításban*

- **Reporting Rollup** *(Jelentések összesítése)* – itt azt határozhatjuk meg, hogy több, hierarchikusan elrendezett WSUS-kiszolgáló között milyen módon történjen a jelentések készítéséhez szükséges adatok áramlása.
- **E-mail Notifications** *(Értesítés e-mailben)* – itt állíthatjuk be a különféle eseményekhez (például új frissítések letöltése) kapcsolódó e-mail értesítésekre vonatkozó paramétereket.
- **Personalization** *(Személyre szabás)* – Az adatok megjelenítésére vonatkozó különféle paramétereket adhatunk meg itt.

Ezzel végére is értünk a kiszolgáló legfontosabb beállításainak, a szinkronizáció (vagyis a javítócsomagok letöltése) után már csak a tesztelés és a frissítőcsomagok jóváhagyása van hátra.

Frissítések jóváhagyása

A Software Update Services szolgáltatást futtató kiszolgáló szinkronizálása alkalmával letöltött frissítések nem válnak automatikusan hozzáférhetővé azoknak a számítógépeknek, amelyek a kiszolgálón lévő frissítések fogadására vannak beállítva. Erre csak akkor kerül sor, ha a rendszergazda jóváhagyja a frissítéseket. Így a rendszergazdának módja nyílik rá, hogy a csomagok telepítése előtt elvégezze a szükséges teszteket.



4.39. ábra: *A WSUS ügyféloldali komponense a Windows-rendszerek beépített Automatic Updates szolgáltatása*

A WSUS-ügyfelek beállításai

A letöltött frissítőcsomagok négy különféle állapotban lehetnek, ezek közül választhatunk a jóváhagyás során:

- **Approved for Install** *(Telepítésre jóváhagyva)* – a frissítés letöltődik és települ az ügyfélgépekre.
- **Approved for Remove** *(Eltávolításra jóváhagyva)* – az adott csomag törlődik az ügyfélgépekről (csak akkor választható, ha a frissítés támogatja).
- **Not Approved** *(Jóvá nem hagyott)* – minden frissítés ebben az állapotban érkezik.
- **Declined** *(Elutasítva)* – az adott frissítésre nincs szükségünk.

A frissítések jóváhagyását elvégezhetjük kézzel (egyenként vagy csoportosan), illetve a korábbiak szerint beállítható a letöltött frissítések automatikus jóváhagyása is. A jóváhagyással együtt szükség esetén megadhatunk egy határidőt is, ameddig az adott frissítésnek mindenképpen települnie kell az ügyfélgépeken.

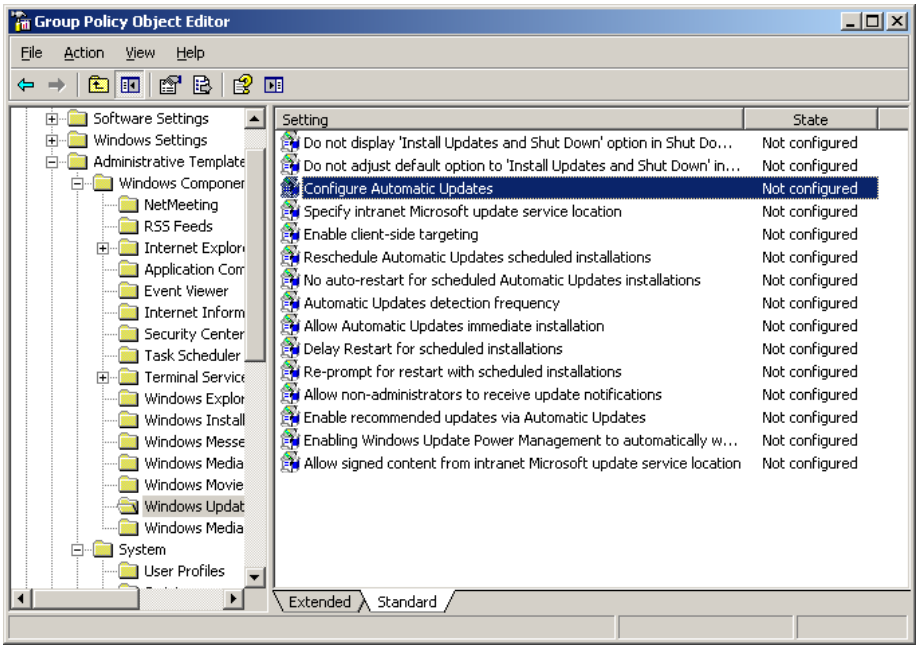
A kiszolgáló beállításai és a csomagok jóváhagyása után már csak az ügyfeleknek kell megmondanunk, hogy új WSUS-kiszolgáló került a hálózatba, legyenek szívesek ezentúl ezt használni a Microsoft Update-kiszolgálók helyett.

Az AU-ügyfelet a Windows 2000 SP2-tól kezdve bármelyik operációs rendszer futtathatja (természetesen a kiszolgálók is). A Windows 2000 SP2, és a Windows XP RTM (vagyis javítócsomag nélküli) változata azonban nem tartalmazza az ügyfélszoftvert, ezekre kézzel (vagy csoportházirenddel) kell telepítenünk a Microsofttól letölthető csomagot.

Az ügyfélszoftver felhasználói felületén (Vezérlőpult → Automatikus frissítések) csak egyetlen beállítási lehetőséget kapunk, minden mást csak a megfelelő csoportházirend-opciók segítségével (vagy esetleg közvetlen registry módosítással) adhatunk meg. A WSUS 3.0 esetén összesen 15 csoportházirend-opció segítségével határozhatjuk meg az ügyfelek viselkedését, a következőkben ezek közül tekintjük át a legfontosabbakat:

- **Configure Automatic Updates** *(Az automatikus frissítés konfigurálása)* – az opció azt határozza meg, hogy az AU-ügyfelek hogyan kapják meg és telepítsék a frissítéseket. Ez az opció érhető el a felhasználói felületen keresztül is, de ott más beállítás nélkül természetesen csak a Microsoft Update kiszolgálókról való letöltésekre vonatkozik. Négy lehetőség közül választhatunk:

- **Notify for download and notify for install** *(Értesítsen a frissítések letöltése előtt, és értesítsen újra a telepítés megkezdése előtt)* – ebben az esetben a letöltés, és a telepítés is „kézzel” indítandó az ügyfélgépen.
- **Auto download and notify for install** *(Töltse le a frissítéseket automatikusan, és értesítsen, amikor készen állnak a telepítésre)* – ha ezt választjuk, akkor már csak a telepítéshez kell az engedélyezés.



4.40. ábra: *Az AU-ügyfeleket vezérlő csoportházirend-opciók*

- **Auto download and scheduled for install** *(Töltse le a frissítéseket automatikusan, és az alább megadott ütemezés szerint telepítse őket)* – a letöltés és a telepítés is automatikusan történik, az időzítést a panel alján állíthatjuk be. Ha ebben az időpontban a gép éppen kikapcsolt állapotban van, akkor a frissítés letöltése és telepítése a következő bejelentkezés után fog megtörténni.
- **Allow local admin to choose setting** *(A helyi rendszergazda adja meg a beállítást)* – A helyi rendszergazda jogosultsággal rendelkező felhasználók maguk választhatnak a fenti lehetőségek közül.

- **Specify intranet Microsoft update service location** *(Adja meg az intraneten található Microsoft frissítési szolgáltatás helyét)* – A WSUS-kiszolgáló, és a statisztikákat tároló kiszolgáló teljes nevét kell itt megadnunk. A statisztikákat egy webkiszolgáló tárolja, amelyre az automatikus frissítést végző ügyfélprogram elküldi az adatokat a letöltött frissítésekről, és azok telepítéséről. A statisztikák elküldésére a program a HTTP-protokollt használja, az adatok a webkiszolgáló IIS naplófájljában jelennek meg.
- **Enable client-side targeting** *(Ügyféloldali célcsoport-meghatározás engedélyezése)* – Ha az opciót engedélyezzük, meg kell adnunk azt a célcsoportot, amelyhez az ügyfélgép tartozni fog.
- **Automatic Updates detection frequency** *(Automatikus frissítések keresési gyakorisága)* – Az AU-ügyfél az itt megadott időközönként keres új frissítéseket a WSUS-kiszolgálón. Az alapértelmezés 22 óra, ami nagyon jó választás, mivel így azokra a számítógépekre is sor kerül előbb-utóbb, amelyek csak egy meghatározott napszakban vannak bekapcsolva.
- **Allow Automatic Updates immediate installation** *(Automatikus frissítések azonnali telepítésének engedélyezése)* – Az opció engedélyezésével azt érhetjük el, hogy az újraindítást nem igénylő, illetve a felhasználót semmilyen más formában nem zavaró frissítések telepítése azonnal a letöltés után megkezdődjön.
- **No auto-restart for scheduled Automatic Updates installations** *(Automatikus újraindítás tiltása ütemezett automatikus frissítések telepítésekor)* – Ha bekapcsoljuk az opciót, a program a frissítések telepítése után nem indítja újra a gépet, hanem értesíti a felhasználót az újraindítás szükségességéről. Ellenkező esetben sem indul újra szó nélkül az ügyfélgép: a felhasználó üzenetet kap, hogy az újraindítás öt perc múlva fog megtörténni.
- **Delay Restart for scheduled installations** *(Újraindítás késleltetése ütemezett telepítéseknél)* – Az opció segítségével azt a várakozási időt adhatjuk meg, ami az első ütemezett újraindítási kísérlet előtt fog eltelni (alapértelmezés szerint 5 perc).
- **Re-prompt for restart with scheduled installations** *(Újbóli rákérdezés az újraindításra ütemezett telepítéseknél)* – Ha a felhasználó nem indította újra a gépet az első figyelmeztetés után, a további figyelmeztetések között az itt beállított várakozási idő lesz érvényes (alapértelmezés szerint 5 perc).

- **Reschedule Automatic Updates scheduled installations** *(Automatikus frissítések ütemezett frissítéseinek átütemezése)* – Az opció értéke 1–60-ig (percben) állítható, a számítógép bekapcsolása után ennyivel fog megkezdődni a hiányzó javítócsomagok letöltése és telepítése.
- **Allow non-administrators to receive update notifications** *(Ne csak a rendszergazdák kapjanak frissítési értesítést)* – Ha az opciót engedélyezzük, valamennyi bejelentkezett felhasználó megkapja a frissítések letöltéséről és telepítéséről szóló értesítéseket.

A WSUS-beállítások terjesztésére három különböző megoldás közül választhatunk (a csoportházirend használatának részleteiről a következő fejezetben lesz szó):

- A leendő WSUS-ügyfelek számítógépfiókjainak külön szervezeti egységeket *(Organizational Unit, OU)* készítünk, és külön GPO-kkal csak ezekhez rendeljük hozzá a WSUS beállításait.
- Nem készítünk külön OU-t, hanem az WSUS GPO-kat a meglevő szervezeti egységek közül rendeljük hozzá a megfelelőkhöz.
- Ha azt szeretnénk, hogy a tartomány összes számítógépe részesüljön a WSUS áldásaiból, módosíthatjuk akár a Default Domain Policyt is.

Jelentések

A WSUS-kiszolgáló jelentéseinek segítségével mindenre kiterjedő információt kaphatunk a rendszer működéséről, lekérdezhetjük az egyes ügyfélgépek vagy frissítések állapotát, a szinkronizációval kapcsolatos eseményeket, illetve összefoglaló jelentést kérhetünk a kiszolgáló valamennyi beállításáról is. Nagyon látványos és részletes jelentést készíthetünk az előzetesen megadható számos beállítási, szűrési paraméternek megfelelően, az eredményt pedig akár Excel-, vagy pdf-formátumban is elmenthetjük, illetve természetesen a közvetlen nyomtatásra is lehetőség van.

ÖTÖDIK FEJEZET

Tartományi környezet

A fejezet tartalma:

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 2003 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-alkal-

mazás 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

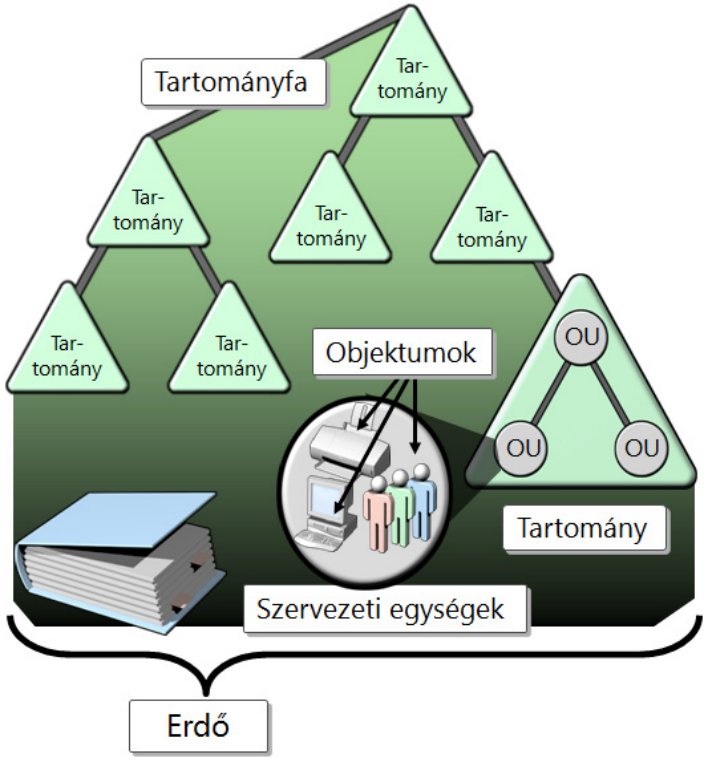
Természetesen ahhoz, hogy kiaknázhassuk az Active Directoryban rejlő lehetőségeket, először be is kell fektetnünk (nemcsak anyagi értelemben), vagyis meg kell szereznünk a hatékony használathoz és üzemeltetéshez nélkülözhetetlen tudást. Minél mélyebben ismeri a rendszergazda az általa üzemeltetett rendszert,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

tomány 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

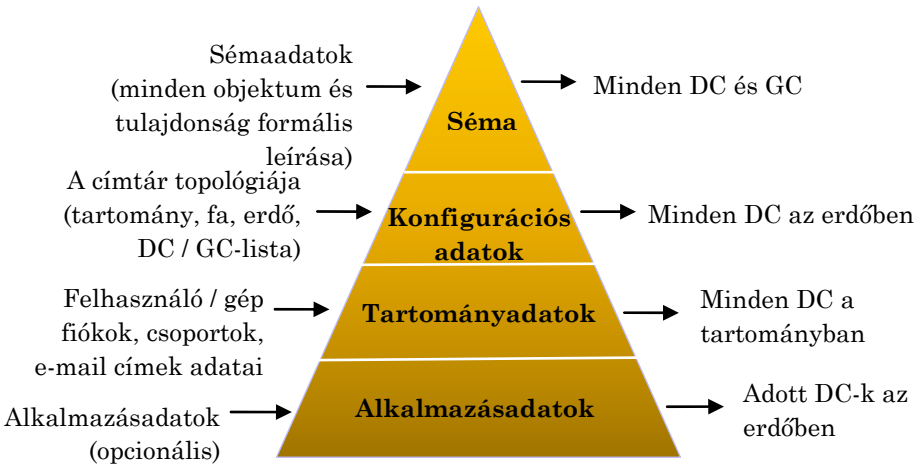
Az Active Directory a multimaster replikációs modellt alkalmazza a címtáradatok tartományvezérlők közötti szinkronizációjához. Ez azt jelenti, hogy a tartományvezérlők mindegyike tartalmazza a teljes címtáradatbázist, és az mindegyik tartományvezérlőn módosítható is. Hogy a címtárpéldányok (replikák) 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.

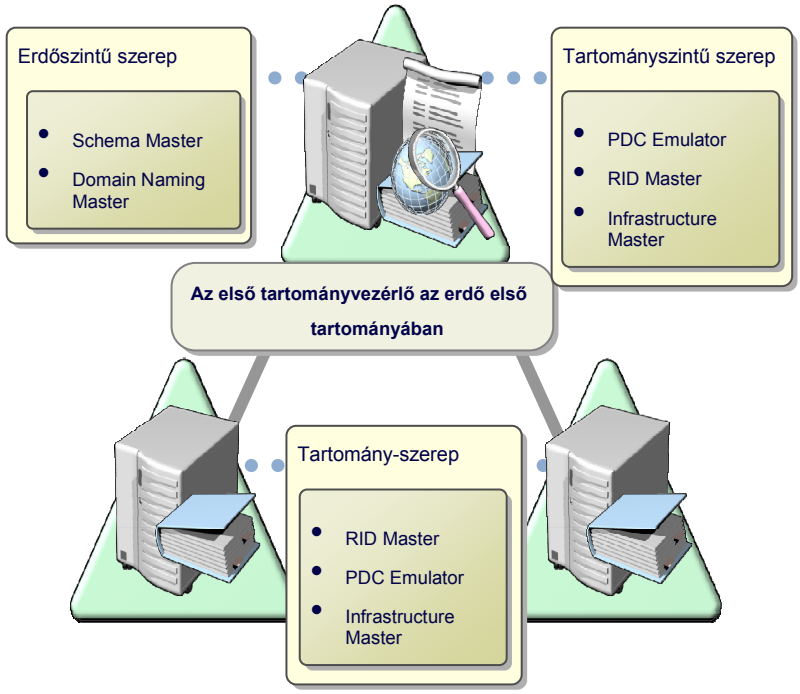
- **Tartomány partíció** *(Domain Partition)* – itt találhatjuk meg a felhasználókra, számítógépekre, csoportokra és egyéb tartomány szintű objektumokra vonatkozó adatokat. A partíció az adott tartomány minden tartományvezérlőjén megtalálható.
- **Alkalmazás partíció** *(Application Partition)* – a Windows Server 2003 rendszert futtató tartományvezérlők a fentieken kívül egy vagy több alkalmazás-címtári partíciót is tárolhatnak.

Az egyedi főkiszolgáló-műveletek (FSMO)

A Windows Server 2003 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.



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

- **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.

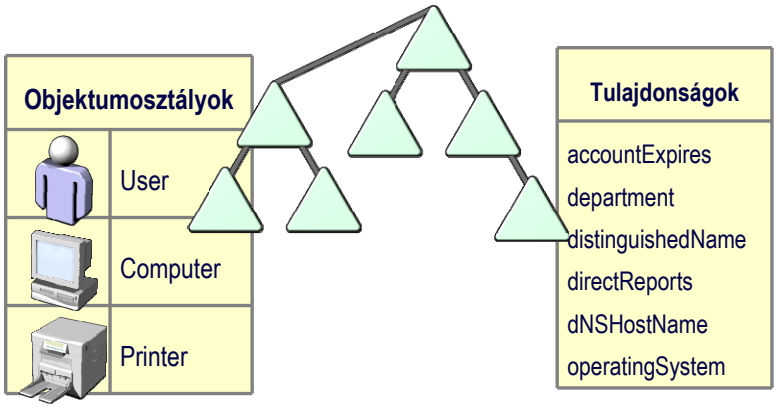
Az erdő első tartományvezérlőjének (ez egyben az elsőként létrehozott tartomány első tartományvezérlője is) telepítésekor valamennyi erdő és tartomány szintű szerepkör erre a kiszolgálóra kerül, de később – ha már több tartományvezérlőnk is van –, az egyes szerepeket tetszés szerint bárhová áthelyezhetjük. 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.



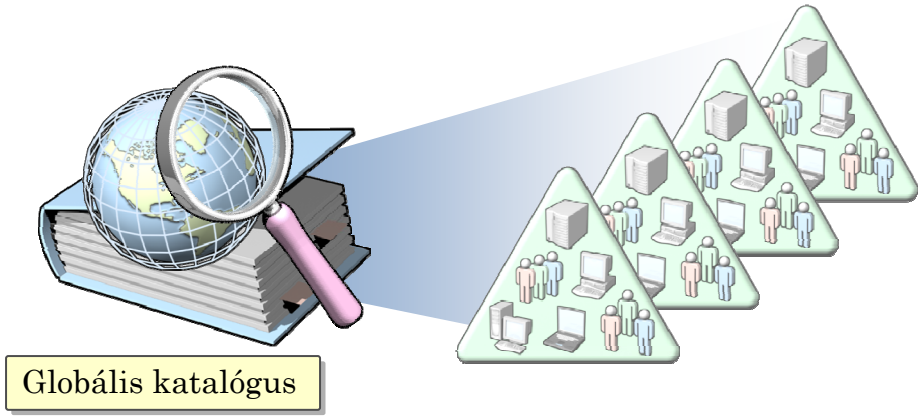
5.4. ábra: *A létrehozható objektumokat, és azok szerkezetét a séma definiálja*

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.



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.

Az egyedi főkiszolgáló-műveletek és a globális katalógus szerepkör
Ebben a screencastban megismerkedünk az egyedi-főkiszolgáló szerepkörök és a globális katalógus szerepkör másik kiszolgálóra való áthelyezésének módszerével, és kipróbálunk két parancssori eszközt, amelyek a tartományvezérlők működésének ellenőrzésére használhatók.
Fájlnév: II-2-1a-FSMO.avi

A működési (funkcionalitási) szintek

A tartományok és erdők Windows Server 2003 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. A tartományokhoz négy működési szint áll rendelkezésre: Windows 2000 – vegyes, Windows 2000 – natív, Windows Server 2003 – átmeneti és Windows Server 2003. A telepítéskor létrejövő tartomány alapértelmezett működési szintje Windows 2000 – natív.

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

Tartomány működési szintje	Támogatott tartományvezérlők
Windows 2000 – vegyes	Windows NT 4.0 Windows 2000 Windows Server 2003 termékcsalád
Windows 2000 – natív	Windows 2000 Windows Server 2003 termékcsalád
Windows Server 2003 – átmeneti	Windows NT 4.0 Windows Server 2003 termékcsalád
Windows Server 2003	Windows Server 2003 család

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 2003 szintre, Windows 2000 Servert futtató kiszolgálókat tartományvezérlőként már nem lehet hozzáadni a tartományhoz. Természetesen továbbra is beléptethető a tartományba a Windows 2000 Server, bármiféle funkciót elláthat, csak tartományvezérlő nem lehet többé.

Az erdők működési szintjének beállításával az erdő összes tartományán engedélyezhetők szolgáltatások. Az erdőkhöz három működési szint áll rendelkezésre: Windows 2000, átmeneti Windows Server 2003 és Windows Server 2003. Alapértelmezés szerint az erdők Windows 2000 szinten működnek, és ezt Windows Server 2003 szintre lehet előléptetni.

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

Erdő működési szintje	Támogatott tartományvezérlők
Windows 2000	Windows NT 4.0 Windows 2000 Windows Server 2003 termékcsalád

Erdő működési szintje	Támogatott tartományvezérlők
Windows Server 2003 – átmeneti	Windows NT 4.0 Windows Server 2003 termékcsalád
Windows Server 2003	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 2003 szintre, Windows 2000 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.

Mentett lekérdezések és a tartomány, illetve erdő működési szintjének emelése
Ebben a videóban megmutatjuk az Active Directory-objektumok közötti keresést és csoportosítást lehetővé tevő Mentett lekérdezéseket *(Saved Queries)*, illetve megemeljük tartományunk, illetve erdőnk működési szintjét.
Fájlnév: II-2-1b-Saved-Queries.avi

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 tárol a tranzakciókról. Átmenetileg ide kerülnek az ntds.dit tömörítése közben eltárolandó adatok is.

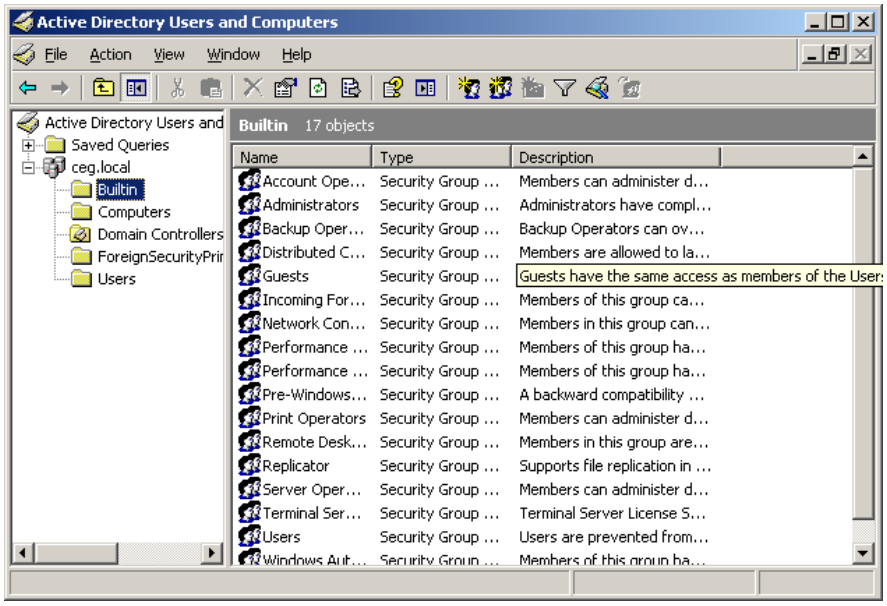
A SYSVOL-mappa

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.

Kezelés és eszközök

A következőkben megismerkedünk az Active Directory felügyeleti eszközeivel, sorra vesszük azokat a grafikus felülettel rendelkező és parancssori 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:



5.6. ábra: *Az Active Directory Users and Computers konzol*

- 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.

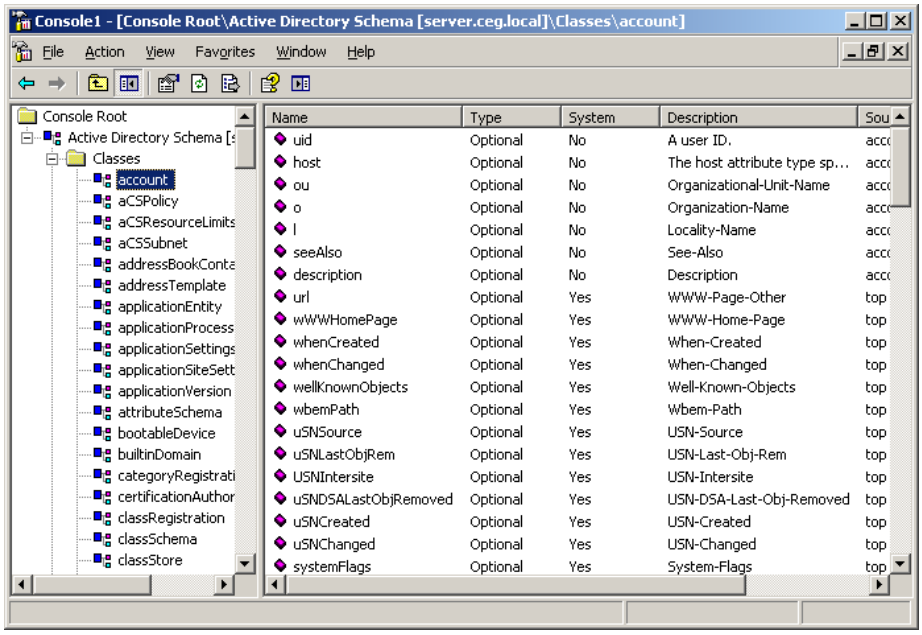
- Az **Active Directory Sites and Services** *(Active Directory – helyek és szolgáltatások)* a telephelyek kialakítására és a tartományvezérlők közötti replikáció beállítására szolgál (lásd később). Ugyancsak ezzel az eszközzel jelölhetjük ki azokat a tartományvezérlőket, amelyek a globális katalógus 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. A Windows 2000 és a Windows Server 2003 erdő tartományai közötti bizalmi kapcsolatok mindig tranzitívak és kétirányúak, így a bizalmi kapcsolatokban mindkét tartomány megbízhatónak minősül. 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. A konzol indítása azonban nem olyan egyszerű, mint a korábbi eszközöké, mivel a modul nincs regisztrálva, így kész parancsikont sem kapunk hozzá. A regisztráláshoz a következő parancsot kell kiadnunk:

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

- Ezután nyissunk egy üres MMC-konzolt és a File *(Fájl)* menüben válasszuk az Add/Remove Snap-in *(Beépülő modul hozzáadása/eltávolítása)*, pontot, majd kattintsunk az Add *(Hozzáadás)* gombra. A listában jelöljük ki az Active Directory Schema sort, majd nyomjunk néhány OK-t. A konzolt tetszés szerinti néven elmenthetjük, és természetesen parancsikont is készíthetünk hozzá.

A fenti konzolokon kívül az Active Directory-objektumainak kezeléséhez számos parancssori segédprogram is használható, a következőkben ezeket fogjuk áttekinteni.

- **DSadd** – felhasználót, csoportot, számítógépet, kapcsolattartót és szervezeti egységet adhatunk segítségével az Active Directoryhoz.



5.7. ábra: *Az Active Directory Séma konzol*

- **DSmod** – a megadott típusú címtárobjektum módosítására használható. Az objektum típusa a következő lehet: felhasználó, csoport, számítógép, kiszolgáló, kapcsolattartó és szervezeti egység.
- **DSquery** – a megadott keresési feltételek alapján kereshetjük és lekérdezhetjük a címtárobjektumokat. Általános üzemmódban bármilyen típusú objektum, speciális üzemmódban pedig a kiválasztott objektumtípusok lekérdezésére használható.
- **DSmove** – a parancs segítségével objektumokat nevezhetünk át, illetve áthelyezhetjük őket az adott tartományvezérlő másik helyére.
- **DSrm** – a megadott típusú objektumot távolít el az Active Directoryból.
- **DSget** – az Active Directory megadott objektumtípusainak kiválasztott attribútumait jeleníti meg.
- **CSVDE** – a program nevéből (Comma Separated Values Directory Export, *vesszővel elválasztott címtárexport)* is kitalálható, hogy az a közismert *csv*, vagyis vesszővel elválasztott értékekből álló fájlformátummal dolgozik. A címtár adatait ilyen fájlokban exportálhatjuk, illetve megfelelő tartalmú *csv* fájl esetén importálhatjuk is azt a címtárba. A csv formátum kiválóan használható, ha az adatokon valamiféle utófeldol-

gozást, módosítást szeretnénk végezni, a fájl akár Excel segítségével is megnyitható és módosítható.

- **LDIFDE** – a program segítségével új címtárobjektumokat hozhatunk létre, illetve módosíthatjuk, törölhetjük a meglévőket. Az LDIFDE segítségével bővíthető a séma, az Active Directory-felhasználó- és csoportadatai exportálhatók más alkalmazásokba vagy szolgáltatásokba, illetve az Active Directory feltölthető más címtárszolgáltatás adataival. Az LDIFDE speciális szövegfájlformátummal dolgozik, amelyben az adatok mellett utasítások is szerepelhetnek. Az LDIF-formátum az LDAP-címtárak közötti replikáció szabványa, így segítségével bármilyen művelet elvégezhető.
- **Ntdsutil** – a program az Active Directory-adatbázisának karbantartására és alkalmazáspartíciók létrehozására használható. A program segítségével van lehetőség a hálózatról nem megfelelően eltávolított (meghibásodott, ablakon kidobott stb.) tartományvezérlőkön maradt egyedi főkiszolgálóműveletek „erőszakos" átadására. Az *ntdsutil* többszintű parancsrendszerrel rendelkezik. Minden szinten használható a help parancs, amely az aktuálisan kiadható utasításokról ad tájékoztatást. Ugyancsak az *ntdsutil*-programot használhatjuk a címtáradatok autoritatív *(mérvadó)* visszaállításához és a címtár-visszaállítási jelszó beállításához. A címtáradatok visszaállításával és a DSRM-üzemmóddal „A címtár mentése és visszaállítása" szakaszban részletesen is foglalkozunk.

A DNS-szolgáltatás

Ha Active Directoryt szeretnénk, akkor a DNS-szolgáltatás használata nem opcionális, a gépek közötti egyszerű névfeloldás, és az Active Directory működéséhez nélkülözhetetlen szolgáltatások azonosítása is a DNS-adatokon alapul. A Windows tartomány nevének ráadásul minden esetben meg kell egyeznie a hozzá tartozó DNS-tartomány nevével, vagyis a két különálló névtér szoros szimbiózisban létezik.

Fontos tisztáznunk, hogy az azonos név ellenére a DNS-tartományok és az Active Directory-tartományok szerepe alapvetően eltér egymástól. Bár a két névtér azonos tartománystruktúrát használ, a tárolt adatok, és így a kezelt objektumok is különbözőek: a DNS-zónákat és erőforrásrekordokat, míg az Active Directory-tartományokat és a tartományhoz tartozó objektumokat tárol. A DNS-erőforrásrekordokat ad válaszul a tartomány- és számítógépnevekre vonatkozó kérésekre, amelyek a DNS-kiszolgálókhoz érkeznek, míg az

Active Directory a tartományvezérlőkhöz intézett LDAP-kérések hatására elvégzi a kért műveletet az adatbázisban tárolt objektumokon.

Ez tehát azt jelenti, hogy egy számítógépet reprezentáló Active Directory-objektum, és az adott számítógéphez tartozó DNS-erőforrásrekord két teljesen különböző névtérben található.

Bár a DNS-kiszolgáló telepítése és beállítása az Active Directory telepítésével együtt, automatikusan megtörténik, és a szükséges erőforrásrekordok bejegyzése is automatikus lehet, alapvető fontossága miatt nem kerülhetjük el a közelebbi ismeretséget, mivel jól beállított DNS-kiszolgáló nélkül az Active Directory alapfunkciói is működésképtelenek.

A DNS (Domain Name System) az IETF (Internet Engineering Task Force) névszolgáltatási szabványán alapuló szolgáltatás, az interneten használt névazonosítás alapja. A DNS olyan nemzetközi, többszintű elosztott rendszer, amelynek segítségével a hálózati számítógépek a tartomány-, illetve hostnevek bejegyzését és feloldását valósítják meg. A DNS-adatbázis a számítógépnevekről (és más szolgáltatásokról) és az egyes nevekhez, illetve szolgáltatásokhoz tartozó IP-címekről tárol információt. Ezeket a neveket használjuk például az internethez csatlakozó számítógépek erőforrásainak kereséséhez és használatához is. A 13 darab úgynevezett „root" DNS-kiszolgálót az InterNIC nevű (természetesen amerikai székhelyű) szervezet tartja fenn. Mivel erősen elosztott rendszerről van szó, az IP-címek és hostnevek összerendelését tároló adatbázis sok ezer önálló DNS-kiszolgálón található. A DNS három fő alkotórészből áll:

- A tartománynévtér és a kapcsolódó erőforrásrekordok elosztott adatbázist alkotnak.
- A DNS-névkiszolgálók tárolják a tartomány névterét és az erőforrásrekordokat, továbbá válaszolnak a DNS-ügyfelek kérdéseire.
- A DNS-ügyfelek részét képező DNS-lekérdezők *(resolver)* felveszik a kapcsolatot a névkiszolgálókkal, és névlekérdezéseket küldenek, hogy hozzájussanak az erőforrásrekordokhoz, vagyis az IP-címekhez.

A névfeloldás menete

A következőkben végigkövetjük a névlekérdezés menetét, megvizsgáljuk, hogy a lekérdezést kezdeményező alkalmazás honnan, és milyen módon juthat hozzá a kért adatokhoz. Minden alkalmazás a DNS-ügyfél részét képező resolver szolgáltatáshoz fordul, ha egy megadott névhez tartozó IP-címre (vagy fordítva) van szüksége.

A resolver először is a lokálisan tárolt DNS-gyorsítótárban (lásd később) próbálja megkeresni a kért rekordot, ha ez sikeres, akkor a kérés egyáltalán nem hagyja el a számítógépet. Ha a keresett adat nem található a gyorsítótárban, akkor a resolver a TCP-IP-paraméterek között megadott DNS-kiszolgálóhoz fordul, neki teszi fel a kérdést. Ha a kiszolgáló az általa tárolt adatbázis-töredék alapján képes a válaszra, akkor visszaküldi a kérdéses rekordot.

Ha a rekord itt sem található, akkor a kérés tovább utazik fölfelé a hierarchiában, a DNS-kiszolgáló a továbbítóként megadott kiszolgálónak (vagy jobb híján közvetlenül a rootkiszolgálóknak) küldi el azt. Innen a lekérdezés megindul újra „lefelé" a hierarchiában, egészen addig, amíg meg nem találja azt a kiszolgálót, ami az elosztott adatbázisnak éppen azt a szeletkéjét tárolja, amelynek alapján a kérés megválaszolható. Nincs azonban mindig szükség a teljes kör végigjárására, mivel minden egyes DNS-kiszolgáló is gyorsítótárazza a lekérdezéseket, így a gyakrabban előforduló címekért nem kell tovább kérdezősködnie, a kérés sok esetben a gyorsítótárból is kiszolgálható.

Hogy a lekérdezés útja jobban követhető legyen, nézzünk végig egy konkrét esetet:

Egy számítógépen futó böngészőprogram a *www.microsoft.com* címen található weboldalt szeretné betölteni, ehhez természetesen szüksége van a névhez tartozó IP-címre. Feltételezzük (bár valós esetben valószínűleg nem így lenne), hogy a címhez tartozó erőforrás-rekord nem szerepel egyetlen gyorsítótárban sem. A DNS-kérést a gép saját DNS-kiszolgálója csak akkor tudja megválaszolni, ha a microsoft.com tartomány saját kiszolgálójáról van szó, a tartományban lévő *www* nevű gép erőforrásrekordja csak itt található meg.

Általában ez nyilván nem így van, vagyis a kérés (hacsak a DNS-kiszolgálón nincs továbbító megadva, ahová a lekérdezéseket el kell küldeni) a root kiszolgálókhoz kerül. Ők tudják azt, hogy kik a *com* tartomány DNS-kiszolgálói, tehát a kérést ezekhez fogják elküldeni. A *com* tartomány kiszolgálói ismerik a microsoft.com DNS-kiszolgálóját, ott pedig már valóban megtalálható a *www* nevű gép erőforrásrekordja, ez fog visszajutni a lekérdezést elindító resolverhez.

A DNS-névfeloldás nemcsak az interneten, hanem a modern, Active Directory alapú Windows tartományokban is alapvető szolgáltatás, amelynek esetleges hibája drámai hatással van a teljes belső hálózat életére. A Windows hálózatokban is a DNS használatával történik a gépek közötti kommunikációhoz szükséges névfeloldás, a kiszolgálói szerepek és szolgáltatások (tartományvezérlő, globális katalógus stb.) megkeresése. Jól működő DNS-re van szükség, hogy új gépeket léptethessünk be a tartományba, részben a DNS-adatokon alapul a tartományadatok replikációja, és még sok, sok más nélkülözhetetlen szolgáltatás is. A régi – NetBIOS alapú – névfeloldás csak vésztartalékként jöhet szóba, a DNS-kiszolgáló hibája esetén nyerhetünk vele némi időt.

A DNS-gyorsítótár *(DNS Resolver Cache)*

A Windows DNS-ügyfelei támogatják a DNS-adatok gyorsítótárazását, így csökkentve a DNS-lekérdezések által generált hálózati forgalmat, és gyorsítva a gyakrabban használt nevek feloldását. A DNS Resolver Cache Service támogatja a negatív gyorsítótárazást is, ami a következők szerint működik: Ha egy névlekérdezés negatív eredményt ad (vagyis egyetlen DNS-kiszolgáló sem volt képes a kért cím biztosítására), az adott névre vonatkozó további kérések már közvetlenül a gyorsítótárból kapnak negatív visszajelzést (alapértelmezés szerint 5 percig).

Még egy funkciója van a negatív gyorsítótárazásnak: ha a lekérdezett DNS-kiszolgálók közül egyik sem érhető el, alapértelmezés szerint 30 másodpercig minden további lekérdezés a timeout periódus kivárása nélkül azonnal negatív választ kap a gyorsítótárból. Ez a szolgáltatás különösen a számítógép indulásakor takaríthat meg jelentős időt: ha a DNS-kiszolgáló nem válaszol, nem kell az induló, DNS-lekérdezést végrehajtó szolgáltatások mindegyikének kivárni a timeout periódusok lejártát. Az ügyféloldali gyorsítótár tartalmát az alábbi parancs segítségével tekinthetjük meg:

```
C:\>ipconfig /displaydns

Windows IP Configuration

    1.0.0.127.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 1.0.0.127.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 604667
...
```

Bizonyos esetekben a gyorsítótár problémákat is okozhat, mivel a DNS-kiszolgálón végzett módosítások csak késve érkeznek meg az ügyfelekre. Ilyenkor mindig arra kell gondolnunk, hogy a gyorsítótár még a módosítás előtti adatokat tartalmazza. Az ügyféloldali gyorsítótárat az alábbi parancs segítségével törölhetjük:

```
C:\>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
```

Magán a DNS-kiszolgálón is van gyorsítótár, ami esetleg szintén okozhat hasonló problémákat. A gyorsítótárat a DNS-kiszolgálóhoz tartozó MMC konzolról (Action -> Clear Cache), illetve az alábbi parancs segítségével törölhetjük:

```
C:\>dnscmd server.ceg.local /clearcache
server.ceg.local completed successfully.
Command completed successfully.
```

Ez a parancs nemcsak a kiszolgálón, hanem bármelyik ügyfélgépen is lefuttatható.

A *dnscmd* program a Windows Support Tools része, így azt külön kell telepíteni *(\support\tools\suptools.msi* a telepítő CD-n).

A DNS-zóna

Zónának nevezzük a DNS-adatbázisokban a DNS-fa egy összefüggő részét, amelyet a DNS-kiszolgáló önálló egységként kezel. Minden zóna tartalmazza a hozzá tartozó nevekhez kapcsolódó valamennyi erőforrásrekordot. Zóna például a *ceg.hu*, a *ceg.local,* a *ceg.priv* stb. A zóna beállításainak (például a nevének) megadásakor nagyon fontos, hogy tekintettel legyünk a publikus és a tartományon belüli DNS-szolgáltatás szigorú elkülönítésére. Semmiképpen nem célszerű például a belső DNS-tartomány neveként a vállalat regisztrált, internetes tartománynevét használni, sokkal jobb választás a *ceg.local* típusú név.

A DNS-kiszolgálók minden zónát önálló fájlban tárolnak (ha nem Active Directory integrált zónáról van szó, lásd később), így a zóna a replikáció, vagyis a DNS-adatok szinkronizálásának alapegysége is. Az adatok visszakeresésének iránya alapján két zónafajtát különböztetünk meg:

- **Forward Lookup Zone** *(Címkeresési zóna)* – a címkeresési zónákban a DNS-kiszolgáló a kérésben szereplő IP-cím alapján hostnevet tud visszaadni, vagyis a zóna az egyes hostnevekhez tartozó IP-címeket tárolja.
- **Reverse Lookup Zone** *(Névkeresési zóna)* – a névkeresési zónákban fordított irányú keresésre van lehetőség, vagyis a DNS-kiszolgáló a lekérdezett IP-címhez tartozó hostnevet tudja visszaadni.

A zónák típusai

A Windows kiszolgálók DNS-kiszolgálói három különböző zónatípust képesek tárolni.

- **Standard Primary** *(szabványos elsődleges)* – a zóna eredeti, módosítható példányát tárolja, ez fog a másodlagos zónákba replikálódni. A zónában történő bármiféle változtatás csak az elsődleges zónában történhet. Az elsődleges zóna tárolására minden esetben egy egyszerű szöveges ál-

lomány, a zónafájl szolgál. A zónafájlok kiterjesztése *dns*, és a DNS-kiszolgálót futtató számítógép *%windir%\System32\Dns* mappájában találhatjuk meg őket. A fájlok neve megegyezik a zóna teljes nevével.

- **Standard Secondary** *(szabványos másodlagos)* – a másodlagos zóna adatai csak olvashatók, az minden esetben az elsődleges zóna egy másolatát tárolja. A másodlagos zónák használata sok DNS-kérés esetén jelentősen lerövidítheti a válaszidőt, az elsődleges zónát tároló számítógép meghibásodása estén pedig azonnal készen álló tartalékként szolgálhat. A Windows Server 2003 DNS-kiszolgálóján azt tapasztalhatjuk, hogy a másodlagos zóna is írható, de ez csak azért tűnik így, mert az ilyen kéréseket a kiszolgáló automatikusan átirányítja az elsődleges zónát tároló számítógéphez.
- **Stub Zone** *(helyettes zóna)* – a helyettes zóna csak bizonyos rekordokat tartalmaz, amelyek alapján az adott zóna mérvadó DNS-kiszolgálói azonosíthatók.

A zóna tárolása

A zónaadatokat tárolhatjuk a szokásos módon fájlokban, illetve lehetőségünk van Active Directory integrated *(Active Directory-integrált)* tárolási típus használatára is. Ez a tárolási mód a Microsoft saját megoldása, ebben az esetben a zóna adatai (vagyis az elsődleges és a helyettesítő zónák rekordjai) közvetlenül az Active Directory-adatbázisban tárolódnak a többi objektummal együtt. Ebből persze egyenesen következik, hogy ilyen zónát csak tartományvezérlőn hozhatunk létre. Az integrált zóna használata még egy fontos következménnyel jár: ebben az esetben az Active Directory replikációja egyben a DNS-adatok replikációját is jelenti. A címtárban csak elsődleges zónák tárolhatók, de ha minden zónát az Active Directoryban tárolunk, akkor a multimaster replikáció miatt egyáltalán nincs szükség másodlagos zónák használatára. Ha DNS-kiszolgálónkat elsősorban az Active Directory névszolgáltatásának biztosítására szánjuk, akkor mindenképpen célszerű ezt a tárolási módot választani a következő előnyök miatt:

- Címtárba integrált zónatárolás esetén a DNS-zóna mindegyik példánya írható, a szinkronizálás a multimaster replikációs modell alapján történik.
- Különösen fontos, hogy ebben az esetben a zóna mindegyik kiszolgálója képes a DNS-ügyfelektől érkező zónafrissítési kérelmek fogadására, amíg van hozzáférhető és elérhető tartományvezérlő.

- Címtárba integrált zónák használatakor hozzáférés-vezérlési lista kapcsolható valamennyi erőforrásrekordhoz, így differenciált hozzáférést adhatunk akár minden egyes rekordhoz.
- Integrált tárolás esetén egységesen kezelhető és felügyelhető az Active Directory és DNS-zónák replikációja.
- Az Active Directory replikációja az objektumok tulajdonságainak szintjén történik, így a rendszer a lehető legkisebb adatmennyiséget mozgatja a zónaadatok szinkronizációjához is.

A hagyományos módon, vagyis szövegfájlban tárolt zónák esetében mindenképpen előnyös az önálló, jól átlátható tárolás (ez például a zóna mentését is egyszerűbbé és gyorsabbá teszi), viszont a zónák közötti szinkronizáció beállítása, illetve az elsődleges és másodlagos zónákat tároló kiszolgálók kiválasztása több odafigyelést és manuális munkát igényel.

A névkiszolgálók típusai

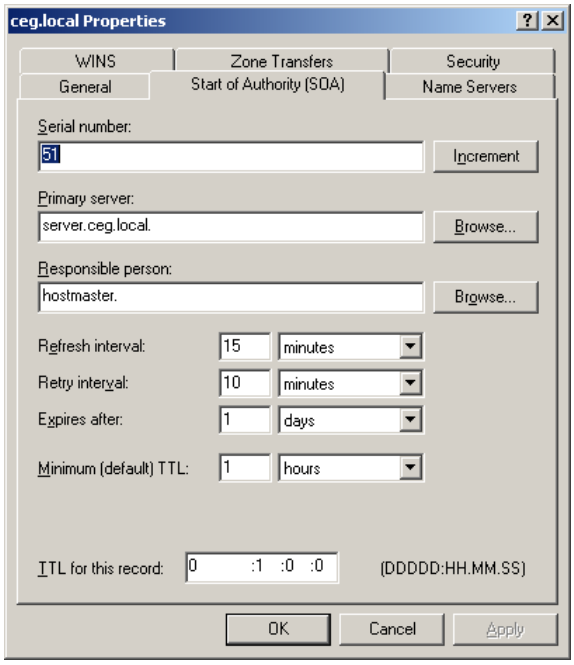
A névkiszolgálók csoportosítása az általuk tárolt (vagy nem tárolt) zóna típusa alapján történik, megkülönböztetünk elsődleges, másodlagos, illetve gyorstárazó kiszolgálókat:

- **Primary DNS Server** *(elsődleges DNS-kiszolgáló)* – az elsődleges kiszolgáló felelős a zóna karbantartásáért, ő a zóna tulajdonosa, a bejegyzett rekordokhoz teljes jogosultsága van.
- **Secondary DNS Server** *(másodlagos DNS-kiszolgáló)* – a másodlagos névkiszolgáló legfontosabb feladata az, hogy a névszolgáltatás az elsődleges kiszolgáló kiesése esetén is hozzáférhető legyen, az ügyfelek továbbra is lekérdezhessék a tartomány számítógépeihez tartozó IP-címeket. A másodlagos kiszolgáló a zóna másolatát tartalmazza, és a SOA-rekordban meghatározott időközönként (ha az elsődleges zóna megváltozott) zónaátvitelt kezdeményez, vagyis átveszi az elsődleges zóna tartalmát (pontosabban csak a változásokat).
- **Cache-only DNS Server** *(gyorstárazó DNS-kiszolgáló)* – a gyorstárazó DNS kiszolgáló nem tárol zónaadatokat, létének egyetlen értelme a kiszolgáló-oldali gyorsítótár fenntartása.

Ez a fajta csoportosítás csak a fájlban tárolt zónák (így például az interneten használt publikus névkiszolgálók) esetén érvényes. Active Directory-integrált zónatárolás esetén valamennyi kiszolgáló adatbázisa módosítható, a zónafrissítés pedig a címtár replikációjával együtt automatikusan megtörténik.

Milyen rekordokat tartalmaz egy zóna?

A DNS-zónák adatai rekordokban, vagyis strukturált adatkupacokban tárolódnak, a lekérdezésekre adott válasz minden esetben egy teljes rekord. A különböző típusú rekordok különféle adatmezőket tartalmaznak, és így különféle adatok tárolására alkalmasak. A Windows kiszolgálókon tárolt DNS-zóna számos különböző típusú rekord befogadására és visszaadására képes, a következőkben ezeket fogjuk áttekinteni.



5.8. ábra: *A DNS-tartomány SOA-rekordja*

- **SOA-rekord** – (Start of Authority) A SOA-rekord minden szabványos zóna esetén a zóna első rekordja. Felelős a zóna inicializásáért és a többi kiszolgáló számára jelzi a zóna hitelességét. A SOA-rekord határozza meg a zónaátvitel időzítését, a másodlagos kiszolgálók pedig az itt tárolt (és a zóna minden módosításakor növekvő) sorszám alapján

dönthetik el, hogy szükséges-e a zóna letöltése. Ugyancsak a SOA-rekordban tárolt érték szabja meg, hogy az ügyfelek mennyi ideig tárolhatják saját gyorsítótáraikban a letöltött rekordokat.

- **A-rekord**: az A-rekordok egy számítógép nevének és IP-címének összerendelését határozzák meg, a lekérdezések többségére a megfelelő A-rekord a válasz.
- **NS-rekord**: az NS-rekordok a zóna további mérvadó névkiszolgálóinak kijelölésére szolgálnak. A DNS-kiszolgáló alapértelmezés szerint csak a zóna NS erőforrásrekordjaiban szereplő kiszolgálókra engedélyezi a zónaletöltést.
- **CNAME-rekord**: Egy másodnevet, vagyis aliast rendel a megadott A-rekordhoz, (illetve esetleg másik CNAME-rekordhoz). Általában CNAME használatával születnek a külvilágnak szóló *www, ftp, mail, proxy* stb. gépnevek, így a valódi gépnév (ami az A-rekordban szerepel) követheti a szervezeten belül kialakított elnevezési szokásokat, illetve a terhelés megosztása miatt több gép is elérhetővé tehető egyetlen név használatával.
- **MX-rekord**: Az MX-erőforrásrekordot az elektronikus levelezésre szolgáló alkalmazások használják az üzenetek címzésében szereplő tartomány levelező kiszolgálójának azonosítására. A rekord annak a számítógépnek (vagy számítógépeknek) a nevét tartalmazza, amely az adott tartományba érkező levelek fogadásáért felelős. A számítógép nevén kívül a rekord tartalmaz egy számot is, ami az adott kiszolgáló prioritását jelzi (az alacsonyabb érték magasabb prioritást jelent).
- **PTR-rekord**: a PTR (pointer, *mutató)* erőforrásrekordok a névkeresési műveletek támogatására szolgálnak, egy IP-cím és egy hostnév összerendelését határozzák meg.
- **WINS-rekord**: A WINS-erőforrásrekordban egy WINS-kiszolgálót adhatunk meg, ide továbbítódnak majd a DNS-adatok alapján meg nem válaszolható IP-cím lekérdezések.
- **WINS-R-rekord**: ugyancsak egy WINS-kiszolgáló címét adhatjuk meg ebben a rekordban, ide a sikertelen fordított lekérdezések (ilyenkor név alapján keresünk IP-címet) fognak továbbítódni.
- **SRV-rekord**: az SRV-rekordok az Active Directoryhoz kapcsolódó szolgáltatások megtalálását teszik lehetővé.

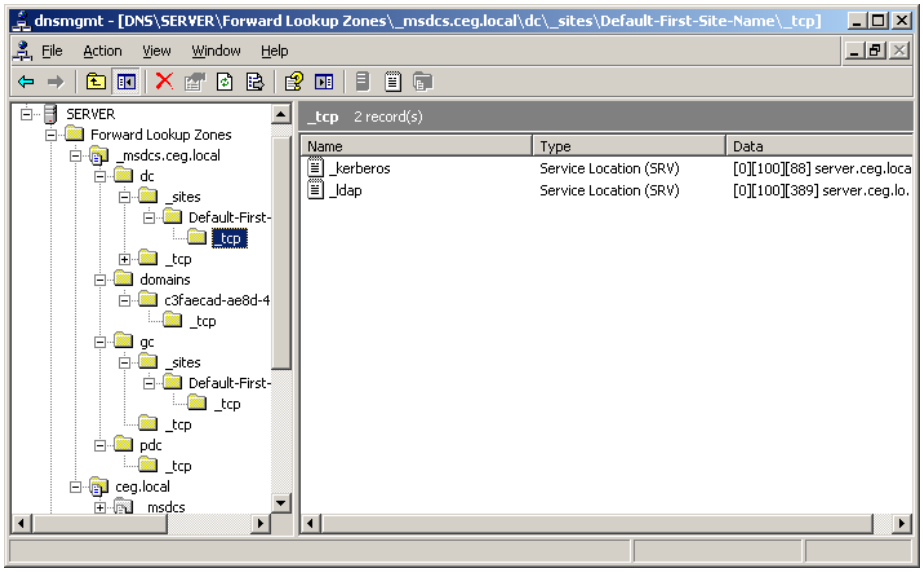
Az utolsó három rekordtípus csak az Active Directory-tartomány belső DNS-kiszolgálóiban fordul elő, a publikus névkiszolgálók ezeket nem tartalmazzák.

Az SRV-rekordok formátuma

Az SRV-rekordok tehát az Active Directory-szolgáltatások eléréséhez szükségesek. Használatukkal lehetővé válik az, hogy több, hasonló TCP/IP-alapú szolgáltatást nyújtó kiszolgálót egyetlen DNS-lekérdezési művelettel keressünk meg. A DNS-lekérdezés ebben az esetben nem egy konkrét kiszolgálóra, hanem magára a szolgáltatásra vonatkozik, a lekérdező pedig az SRV-rekordok által tárolt kiszolgálólistából fogja megkapni azt, amelyik a beállított prioritások alapján jár neki. Ilyen módon történik például az LDAP-protokoll segítségével a 389-es TCP-porton keresztül elérhető Active Directory-szolgáltatás megkeresése is. Az ügyfélgépek ebben az esetben nem egy konkrét számítógép IP-címét kérdezik le a névkiszolgálótól, ők csak annyit tudnak, hogy az adott tartomány egyik (bármelyik) tartományvezérlőjével kívánják felvenni a kapcsolatot, vagyis egy szolgáltatás (amit általában több konkrét számítógép is képes nyújtani) IP-címét fogják megkapni.

Az SRV-erőforrásrekordok egyes mezőinek rendeltetése a következő:

- **Szolgáltatás** – A keresett szolgáltatás szimbolikus neve. A szolgáltatás neve lehet például *_ldap* vagy *_kerberos*.
- **Protokoll** – Az átviteli protokoll típusát jelzi. Ez általában TCP vagy UDP, bár elméletben más protokollok is használhatók.
- **Név** – A DNS-tartománynév, amelyhez az erőforrásrekord tartozik.



5.9. ábra: *Az LDAP-szolgáltatás elérését biztosító egyik SRV-rekord*

- **Prioritás** – Meghatározza a cél mezőben szereplő kiszolgáló prioritását. Az SRV-erőforrásrekordokat lekérdező DNS-ügyfelek a legalacsonyabb sorszámú (vagyis legmagasabb prioritású) elérhető kiszolgálóval próbálják meg felvenni a kapcsolatot.
- **Súlyozás** – A prioritás mellett a súlyozás is terheléselosztásra használható. Azonos prioritású kiszolgálók esetén ez az érték határozza meg a lekérdezés eredményét.
- **Port** – A célállomás kiszolgálóportjának száma, amelyen az adott szolgáltatás elérhető.
- **Cél** – A kért szolgáltatás nyújtására képes kiszolgáló DNS-tartománynevét tartalmazza. Az itt szereplő névhez tartoznia kell egy megfelelő állomáscím (A) erőforrásrekordnak, amely alapján a kérdéses IP-cím meghatározható.

Az alábbi sorokban egy példa SRV-rekord látható, felül az egyes mezők neve, alul pedig egy lehetséges értéke:

```
Service_.Protocol.Name  Ttl  Class  SRV Priority Weight Port Target
_ldap._tcp.ceg.local 600 IN SRV 0 100 389 server.ceg.local
```

A DNS-kiszolgáló beállításának lépései

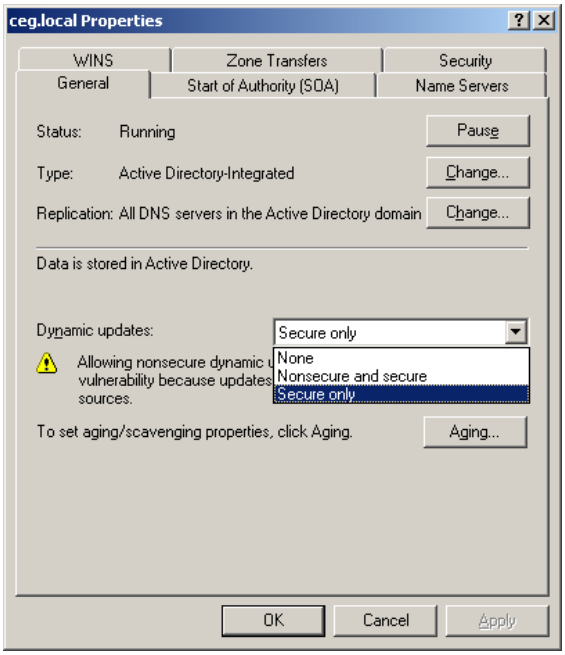
A DNS-kiszolgáló telepítése az első tartományvezérlő telepítése közben automatikusan megtörténik, a létrejövő zóna neve pedig megegyezik az Active Directory-tartomány nevével. Minden tartományban érdemes legalább két DNS-kiszolgálót létrehozni, célszerűen ezek a tartományvezérlők lehetnek. A DNS-szolgáltatást nyújtó gépek kiválasztásánál azonban mindenképpen figyelembe kell vennünk, hogy Active Directory-integrált zóna kizárólag tartományvezérlőn hozható létre.

A DNS-kiszolgáló beállítási lehetőségei
Ebben a screencastban áttekintjük az Active Directory alapjául szolgáló DNS-kiszolgáló beállítási lehetőségeit és részletesen megismerjük az egyes opciók jelentését.
Fájlnév: II-2-2-DNS.avi

A telepítés után azonban néhány fontos beállítást ellenőriznünk, illetve módosítanunk kell, hogy a névszolgáltatás működése minden szempontból megfelelő lehessen. A beállítások két nagy csoportba tartoznak; elsőként a zóna, majd a teljes kiszolgáló opcióit fogjuk áttekinteni.

A DNS-kiszolgáló felügyeletére a DNS nevű MMC beépülőmodul szolgál, amit legkönnyebben a Start menü Administrative Tools *(Felügyeleti eszközök)* mappájából indíthatunk el. A zóna opcióinak megjelenítéséhez a bal oldali fában nyissuk ki a kiszolgálónk neve alatt található Forward Lookup Zones *(Címkeresési zónák)* csomópontot, kattintsunk jobb gombbal a tartományunk nevének megfelelő sorra, majd válasszuk a Properties *(Tulajdonságok)* parancsot!

Amint az alábbi képen is látható, az Active Directory telepítése közben automatikusan létrehozott zóna alapértelmezés szerint Active Directory-integrált, vagyis az erőforrásrekordok a címtár objektumainak képében tárolódnak. Az alapértelmezett állapot szerint engedélyezett a zónaadatok dinamikus frissítése *(Dynamic updates)* is, vagyis az ügyfélgépek maguk kezdeményezhetik A és PTR rekordjaik bejegyzését, illetve módosítását.

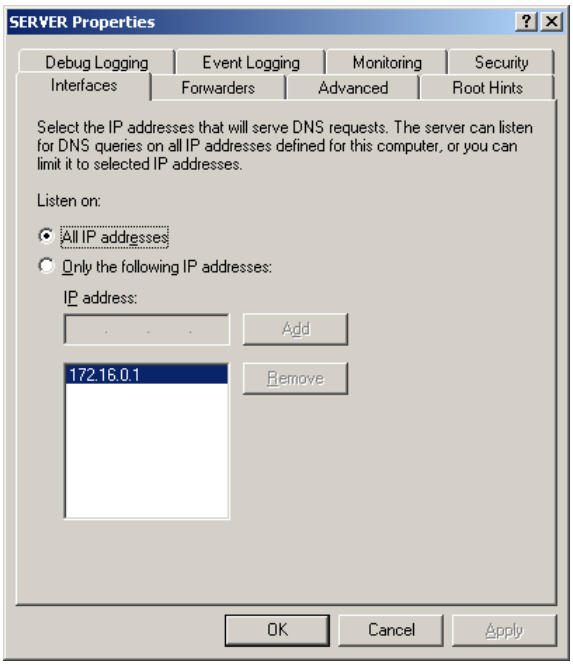


5.10. ábra: *Az AD telepítése közben létrehozott DNS-zóna tulajdonságai*

- A **Name Servers** *(Névkiszolgálók)* lap a másodlagos DNS-kiszolgálók felvételére szolgál, az itt megadott számítógépek számára NS-rekord készül a zónában.
- A **Zone Transfers** *(Zónaátvitel)* lapon engedélyezhetjük a zóna más kiszolgálókra történő átmásolását. Ha minden kiszolgálón Active Directory-integrált zónát használunk, akkor egyáltalán nincs szükség zónaátvitel beállítására, mivel ebben az esetben a címtár replikációja a zónaadatok átvitelét is magában foglalja.

A zóna beállításai után következzenek a kiszolgáló opciói, ezek az adott kiszolgálón létrehozott valamennyi zónára vonatkoznak majd. Keressük meg a fában a kiszolgálónk nevét, kattintsunk rá a jobb gombbal, és válasszuk a Properties *(Tulajdonságok)* parancsot!

Ha több hálózati csatoló is van a gépben, akkor nagyon fontos, hogy a megfelelő csatolóra korlátozzuk a DNS-szolgáltatást. Nyilvánvalóan teljesen felesleges (sőt káros), ha például a tartományon belüli neveket kezelő kiszolgáló a külső (az internet-szolgáltató felé néző) csatolóra érkező kérésekre is válaszol. Az Interfaces *(Kapcsolatok)* lapon választhatjuk ki a kiszolgáló IP-címei közül azokat, amelyeken keresztül válaszolni kívánunk a beérkező DNS-kérésekre.



5.11. ábra: *A DNS-kiszolgálónak nem kell feltétlenül minden csatolón keresztül válaszolnia (bár, ha csak egy van, akkor mégis)*

A Forwarders *(Továbbítók)* lapon azokat a DNS-kiszolgálókat adhatjuk meg, ahová továbbhalad egy helyben nem feloldható (pl. internetre irányuló) lekérdezés. Ha nem adunk meg egyetlen továbbítót sem, az azt jelenti, hogy DNS-kiszolgálónk minden, a hálózaton kívülre irányuló lekérdezést végső sorban a gyökérmutatók (vagyis a root DNS-kiszolgálók) használatával fog feloldani. Ennek eredményeként nagy mennyiségű belső, esetleg kritikus fontosságú DNS-információt küldhetünk ki az internetre. A biztonsági és adatvédelmi probléma mellett ez a módszer jelentős külső forgalommal is jár, terhelve a vállalat internetkapcsolatát.

Ha továbbítót jelölünk ki (jellemzően az internetszolgáltatónk DNS-kiszolgálóját), akkor őt tesszük felelőssé a külső forgalom kezeléséért. A továbbító ráadásul várhatóan rengeteg külső DNS-információt gyűjt össze a gyorsítótárában, így a külső DNS-lekérdezések jó részét az itt tárolt adatok használatával is fel tudja majd oldani.

A továbbító használatára beállított DNS-kiszolgáló az alábbiak szerint próbálja megválaszolni a hozzá érkező lekérdezéseket:

- A DNS-kiszolgáló a beérkező lekérdezéseket először a gyorsítótárból, majd a rajta tárolt elsődleges és másodlagos zónák rekordjai közötti kereséssel próbálja feloldani.
- Ha az előző keresések sikertelenek voltak, akkor a lekérdezés a továbbítóként megadott DNS-kiszolgálóhoz kerül.
- A DNS-kiszolgáló meghatározott ideig vár a továbbító válaszára, majd megpróbál kapcsolatba lépni a gyökérmutatóiban megadott DNS-kiszolgálókkal.

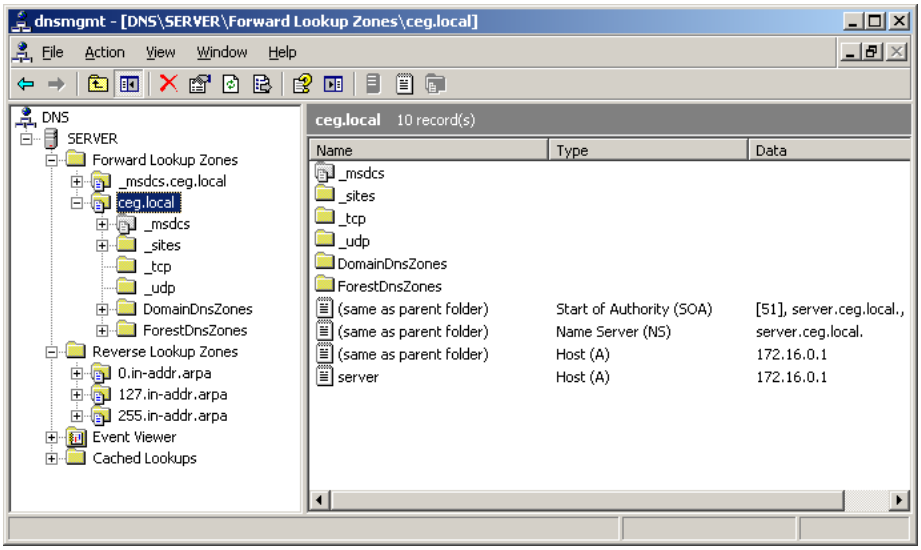
Utolsó lépésként, ha szükséges, létre kell hoznunk a megfelelő névkeresési zónákat a névlekérdezési műveletek támogatására. Az alapbeállítások helyes megadása után a DNS-kiszolgálóval nem lesz túl sok gondunk; az erőforrásrekordok (A, PTR, SRV stb.) bejegyzése, törlése, átnevezése teljesen automatikus. Alapértelmezés szerint a statikus TCP/IP-paraméterekkel rendelkező hálózati csatolók megpróbálják dinamikusan regisztrálni állomás (A) és mutató (PTR) típusú erőforrásrekordjaikat. A regisztrált név a számítógépnév, és a számítógép elsődleges DNS-utótagjának összefűzéséből alakul ki. Az elsődleges DNS-utótag alapértelmezés szerint megegyezik a tartomány nevével.

A dinamikus címbejegyzés (DDNS) kiváltható a következő parancs használatával:

```
C:\> ipconfig /registerdns
```

Régebbi ügyfelek használata (Windows 9x, Windows NT) esetén a dinamikus bejegyzés csak a DHCP-szolgáltatás közreműködésével lehetséges. A DHCP a kiosztott címeket (megfelelő beállítás esetén) megpróbálja a DNS-kiszolgálón is regisztrálni.

Egy jól működő tartományvezérlő DNS-zónafájlja az alábbi ábrához hasonlóan néz ki:



5.12. ábra: *A jól működő DNS-zóna*

Két címkeresési zónánk van, az *_msdcs.ceg.local* (Microsoft Domain Controllers) tovább bontható *dc, domains, gc* és *pdc* bejegyzésekre. A *gc* a globális katalógust jelenti, a *pdc* bejegyzés pedig a PDC-emulátorra utal. A *ceg.local* alatt az alábbi altartományokat kell találnunk:

- *_sites* – itt a tartományvezérlőket telephelyek szerinti bontásban találjuk, ez alapján találják meg a munkaállomások a hozzájuk legközelebb eső kiszolgálókat
- *_tcp* és *_udp* – az egyes szolgáltatások felbontása TCP-csatorna-elérési szempontból

Amennyiben ezek a bejegyzések hiányoznak, az Active Directory még alapfunkcióit sem fogja tudni ellátni. Ha nincs meg minden, vagy üres a zóna, a következőt tehetjük: Ha engedélyeztük a DNS-adatok dinamikus frissítését, akkor a tartományi SRV-rekordok regisztrációjáért a NetLogon-szolgáltatás felelős, amely a bejegyzéseket induláskor hozza létre. Adjuk ki tehát a következő parancsokat:

```
C:\>net start netlogon
C:\>net stop netlogon
```

Az Active Directory telepítése

A Windows-kiszolgálók életében az Active Directory is csak olyan, mint bármelyik másik szolgáltatás; tetszés szerint telepíthető, illetve eltávolítható a kiszolgálóról. Ennek ellenére a telepítés, illetve eltávolítás egyáltalán nem tekinthető mindennapos rutinműveletnek, ezért csak komoly odafigyeléssel és megfelelő előkészületek után célszerű elvégezni. A következőkben áttekintjük a telepítés előfeltételeit, a telepítőprogram által elvégzett műveleteket és azokat a hibalehetőségeket, amelyek a telepítés közben felmerülhetnek.

Az Active Directory telepítése a kiszolgálóra
Ebben a screencastban feltelepítjük kiszolgálónkra lépésről lépésre az Active Directory-szolgáltatást, és megismerkedünk a telepítőprogram által bekért különféle paraméterek jelentésével.
Fájlnév: II-2-3-AD-Telepites.avi

A telepítés feltételei

Az Active Directory használatához Windows Server 2003 operációs rendszer szükséges, ügyfélrendszerekre a címtár nem telepíthető. A telepítőprogram futása közben meg kell adnunk a címtár adatfájljainak leendő helyét (alapértelmezés szerint *%WINDIR%\NTDS).* A megadott mappának mindenképpen NTFS fájlrendszerű köteten kell lennie, a minimális helyigény pedig nagyjából 250 MB. Nagyobb igénybevétel esetén indokolt lehet az önálló, csak erre a célra használt címtárpartíció létrehozása. Mit nevezünk nagy igénybevételnek? Egy átlagos magyar vállalatnál előforduló terhelést semmiképpen sem. A gyakorlatban több ezer, de még inkább néhány tízezer tárolandó objektum esetén lehet szükség erre a megoldásra.

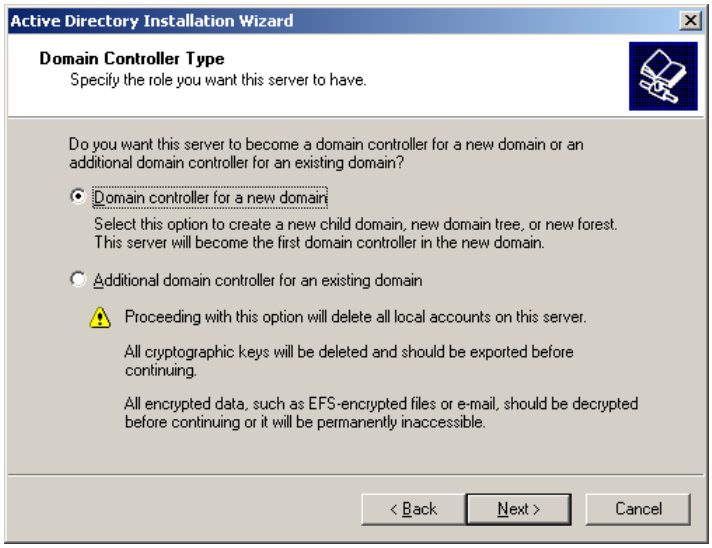
A címtár telepítéséhez rendszergazda jogosultság szükséges egyrészt az adott számítógépen, másrészt, ha már létező tartományhoz csatlakozunk, akkor a tartományban is.

Alapfeltétel a tökéletesen beállított TCP/IP, elsősorban a DNS-kiszolgáló miatt. Az Active Directory alapszükséglete a jól működő névszolgáltatás, ha a telepítő nem talál a hálózaton használható DNS-szolgáltatást, akkor a telepítés közben ő maga hoz létre egyet.

Mi történik a telepítés közben?

Az Active Directory telepítését a Start menü Administrative Tools *(Felügyeleti eszközök)* csoportjában található Configure Your Server Wizard *(Kiszolgáló konfigurálása varázsló)* segítségével végezhetjük el; a Domain Controller *(Tartományvezérlő)* szerepkört kell kiválasztanunk. Egyébként a telepítőprogram neve DCPromo.exe, akár a Run *(Futtatás)* menüből, akár parancssorból közvetlenül is elindíthatjuk.

A DCPromo először is bekéri az új tartományvezérlőre vonatkozó adatokat:



5.13. ábra: *A DCPromo első kérdése*

- Új tartományt hozunk létre, vagy meglévő tartományhoz csatlakozunk? Ha meglévő tartományhoz csatlakozunk, akkor meg kell adnunk a tartomány nevét, és a megfelelő hitelesítési adatokat. Új tartomány esetén pedig jön a következő kérdés:
- A tartomány egy új erdőben lesz, egy már létező tartományfára szeretnénk felfűzni, esetleg új tartományfát hoznánk létre számára egy létező erdőben?

Tételezzük fel, hogy még nincs Active Directory a hálózatban. Ebben az esetben nyilvánvalóan új tartományt hozunk létre, de egyben természetesen új fát és új erdőt is, vagyis egyszerűen elfogadhatjuk az alapértelmezett opciókat.

A tartományvezérlőkön (a tartomány többi számítógépével ellentétben) nincs helyi felhasználói adatbázis. A tartományvezérlővé történő előléptetés közben (új tartomány esetén) a DCPromo a létező helyi felhasználói fiókokat átmásolja az Active Directoryba, a helyi Administrator (Rendszergazda) felhasználó például tartományi rendszergazdává alakul. Amennyiben azonban nem új tartományt hozunk létre, hanem egy már létező tartományhoz csatlakozunk, a gépen tárolt helyi felhasználói fiókok nem kerülnek be az Active Directory-adatbázisban, hanem egyszerűen eltűnnek. A DCPromo futtatása után tehát mindkét esetben csak a tartományi felhasználónevek és jelszavak használatával fogunk tudni bejelentkezni.

Ezután már csak az új tartomány leendő DNS és NetBIOS nevét, valamint az adatbázisfájlok és a SYSVOL megosztás helyét kell megadnunk, és kezdődhet is a telepítés. Futása közben a telepítőprogram az alábbi műveleteket végzi el:

- Amennyiben a telepítő nem talál elérhető és használható DNS-szolgáltatást, és nem utasítjuk kifejezetten az ellenkezőjére, akkor a telepítés részeként megtörténik a DNS-kiszolgáló telepítése és beállítása is.
- Létrehozza a címtárpartíciókat, magát az Active Directory-adatbázist és a naplóállományokat.
- Ha egy új erdő első tartományvezérlőjét telepítjük, akkor létrehozza az úgynevezett *forest root domain*-t, tehát az erdő első (gyökér) tartományát.
- Létrehozza és megosztja a SYSVOL-mappát (az ügyfélgépek innen töltik majd le a házirendeket, szkripteket stb.).
- Beállítja az adott tartományvezérlő telephely tagságát.
- Beállítja a címtárszolgáltatás és a replikált mappák jogosultságait.
- Bekéri és eltárolja a címtár-visszaállítási jelszót. A Directory Services Restore Mode jelszavára akkor lehet szükségünk, ha a gépen valamilyen ok miatt (valamelyik csökkentett módban *(Safe Mode)*, illetve a címtárszolgáltatások helyreállítási üzemmódjában *(Directory Services Restore Mode, DSRM)* történő rendszerindítás, a Recovery Console *(helyreállítási konzol)* használata, esetleg valamiféle rendszerhiba) nem áll rendelkezésre az Active Directory, így az abban tárolt felhasználói fiókok használatával nem tudunk bejelentkezni. Ekkor kell ezt a jelszót megadnunk, amelynek azonosítása a System Account Manager (*rendszer fiókkezelő, SAM)* adatai alapján történik.

Hibalehetőségek

Az Active Directory telepítése a korábban felsorolt feltételek teljesülése esetén rutinművelet, a legritkább esetben fordul elő olyan hiba, ami megakadályozná a telepítés sikeres befejezését. Az alábbi táblázatban mégis felsorolunk néhányat a leggyakrabban előforduló hibajelenségek és a lehetséges okok közül.

A jelenség	A lehetséges okok
„A hozzáférés megtagadva” üzenet, amikor létrehoznánk, vagy hozzáadnánk egy tartományvezérlőt	Nem vagyunk tagjai a helyi Administrators csoportnak. Nem vagyunk tagjai Domain Admins vagy az Enterprise Admins csoportoknak.
Hiba a DNS vagy a NetBIOS-tartománynév megadásakor	Létezik és elérhető ugyanilyen DNS vagy NetBIOS nevű tartomány
A már meglévő tartománnyal nincs kapcsolat	Hálózati (pl. TCP/IP) vagy DNS-hiba. Tűzfal probléma
A „lemez megtelt” üzenet	Az adott partíción nincs meg a minimum lemezhely

Tipikus címtárobjektumok

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.

Szervezeti egységek, felhasználók és számítógépfiókok kezelése
Ebben a screencastban az Active Directory felügyeletének leggyakrabban használt eszközét, az Active Directory Users and Computers konzolt ismerhetjük meg. Bemutatjuk a napi üzemeltetési gyakorlat általános feladatait: szervezeti egységeket és felhasználói fiókokat hozunk létre és beállítjuk a felhasználói fiókok legfontosabb jellemzőit.
Fájlnév: II-2-4a-ADUC.avi

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 egységek felépítésének tervezése

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:

Modellek	Az OU tervezés szempontjai
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

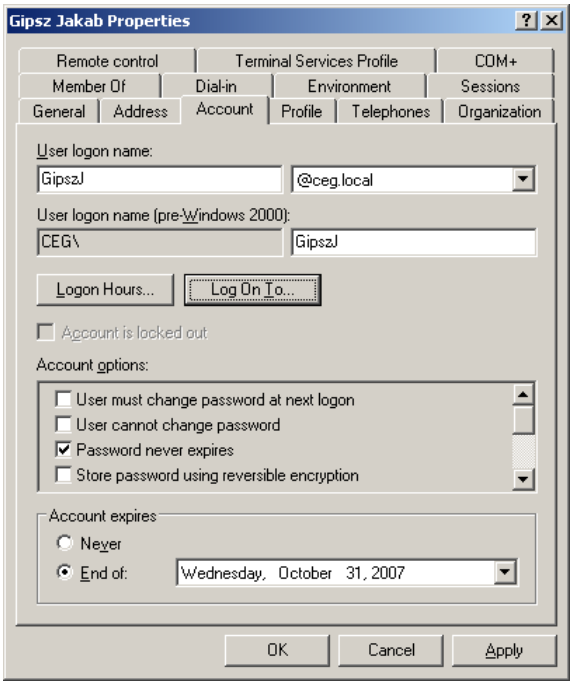
A felhasználói fiók

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).

Felhasználók létrehozása sablon alapján
Ebben a screencastban bemutatunk egy egyszerű módszert, amelynek segítségével több felhasználói fiók létrehozását előre beállított sablon alapján végezhetjük el.
Fájlnév: II-2-4b-User-Template.avi

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.



5.14. ábra: *A felhasználói fiók alapadatai*

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.

Ügyfélgép beléptetése a tartományba
Ebben a screencastban egy ügyfélgépet léptetünk be az Active Directory-tartományba, majd megvizsgáljuk a belépés közben – a címtárban – létrejött új számítógépfiókot.
Fájlnév: II-2-4c-Join-Domain.avi

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 e-mailek 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:

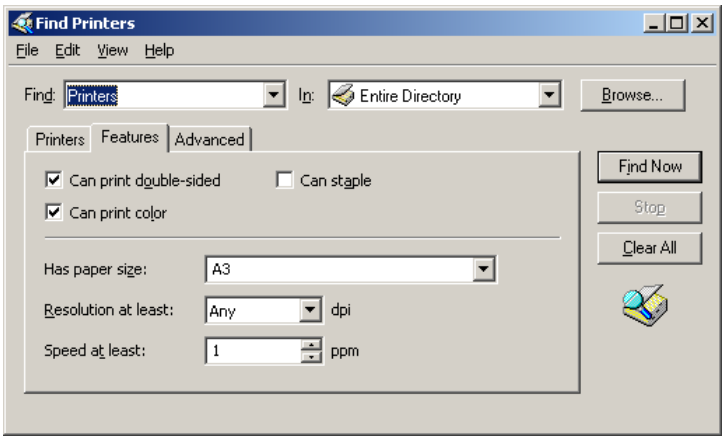
- **Helyi csoport** *(Machine Local Group)* – Olyan biztonsági csoport, amely csak annak a számítógépnek az erőforrásaihoz kaphat jogokat és engedélyeket, amelyen a csoportot létrehozták. A helyi csoportok tartalmazhatják bármely megbízható hely, például a tartomány, vagy más megbízotti kapcsolatban 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 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.

Megosztott mappák és nyomtatók

A hálózatban található megosztott mappákat és nyomtatókat közzétehetjük (Windows 2000 előtti rendszerekét is) az Active Directory-címtárban, így azok egyszerűen elérhetők, megtalálhatók lesznek a felhasználók számára. A mappákhoz és nyomtatókhoz tartozó címtárobjektum tárolja azt, hogy az adott erő-

forrás pontosan hol található, milyen módon érhető el, és milyen tulajdonságokkal rendelkezik. A felhasználók könnyen megkereshetik például azokat a nyomtatókat, amelyek színes, kétoldalas, A3 méretű nyomtatásra képesek.



5.15. ábra: *Lesz vajon ilyen nyomtató?*

Az ilyen módon megvalósítható központi nyilvántartás segítségével minden egy helyen érhető el, a felhasználóknak nem kell tudnia, hogy az adott erőforrás melyik kiszolgálón, milyen megosztási néven érhető el. Ráadásul így megszabadulhatunk az üzenetszóráson *(broadcast)* alapuló, és így nagyobb hálózatokban rendkívül erőforrás-pazarló számítógép-tallózó *(Computer Browser)* szolgáltatástól is.

A tallózó szolgáltatással ellentétben, a címtárban való közzététel a másik IP-alhálózatban lévő erőforrások elérésére is használható, sőt az erőforrást tartalmazó számítógépnek nem is kell feltétlenül az Active Directory-tartomány tagjának lennie. A megosztott mappákhoz és nyomtatókhoz tartozó címtárobjektumok létrehozásához az Active Directory Users and Computers konzolt használhatjuk, illetve nyomtató esetén a megosztáshoz tartozó tulajdonságlapon is beállítható a *List in the Directory (Listázás a címtárban)* opció. Az utóbbi módszer esetén azonban az Active Directory Users and Computers felületén nem jelenik meg a létrehozott objektum (de a kereséseknél igen).

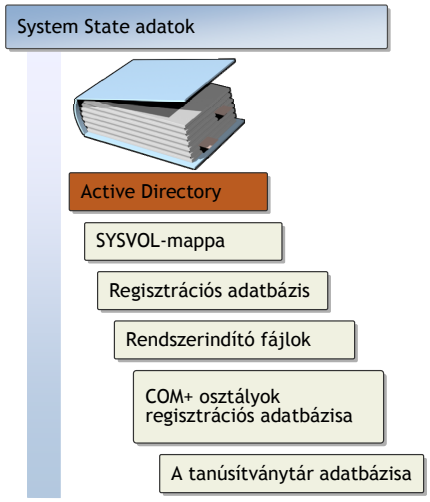
Miután felvettük a megosztott erőforrást, ennek elérhetőségére, vagy akár meglétére vonatkozó ellenőrzés nem történik, a címtárobjektum és az erőforrás között nincsen kapcsolat. A rendszergazdának kell tehát gondoskodnia róla, hogy az eltávolított, vagy hosszabb ideig nem elérhető erőforrások kikerüljenek a címtárból.

A címtár mentése és visszaállítása

Az Active Directory felügyelete nem lehet teljes, ha nem gondoskodunk a címtár rendszeres biztonsági mentéséről. A címtár és a hozzá kapcsolódó adatok mentését az NTBACKUP segítségével érdemes elvégezni például szalagos meghajtóra, de legrosszabb esetben is egy önálló, a rendszertől független merevlemezre.

Az Active Directory mentése és visszaállítása
Ebben a screencastban biztonsági mentést készítünk az Active Directory adatbázisról, majd a kiszolgálót DSRM-üzemmódban elindítva visszaállítjuk az elmentett adatokat.
Fájlnév: II-2-5-AD-Backup-Restore.avi

A System State mentés



5.16. ábra: *A System State mentés tartalma*

Az Active Directory mentése a System State *(Rendszerállapot)* mentés része, az NTBACKUP felületén ezt kell kiválasztanunk. A rendszerállapot adatok biztonsági mentésekor és visszaállításakor a rendszer a számítógéphez kapcsolódó összes rendszerállapot-adat biztonsági mentését vagy visszaállítását végrehajtja, az egyes összetevők önálló mentése vagy visszaállítása nem lehetséges.

Az ábráról leolvasható, mi tartozik a Rendszerállapot mentéshez: az Active Directory-adatbázis, a SYSVOL-megosztás tartalma (házirend fájlok, logon szkriptek stb.), a regisztrációs adatbázis, a rendszerindító fájlok, a COM+ osztályok regisztrációs adatbázisa, és a tanúsítványtár.

A System State mentés önállóan és egy általános mentés részeként is elvégezhető. A mentés a tartományvezérlő online állapotában történik, sem leállításra, sem újraindításra nincs szükség.

A címtár visszaállítása

Közel sem ilyen egyszerű azonban a címtár visszaállítása, első alkalommal legjobb ezt egy tesztrendszeren kipróbálni, hogy éles helyzetben kevésbé remegjen a rendszergazda keze.

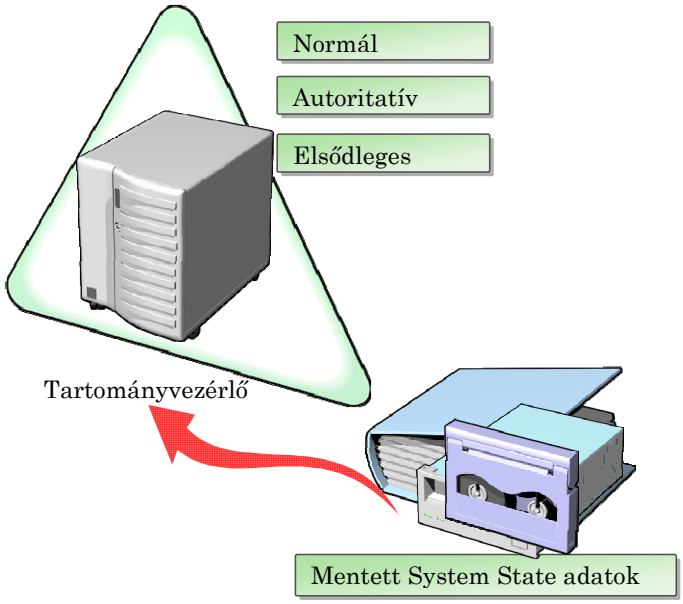
A számítógép indítása közben a megfelelő pillanatban (a grafikus képernyő előtt) meg kell nyomnunk az F8 billentyűt, ennek hatására az alábbi képen látható menühöz jutunk:

```
Windows Advanced Options Menu
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable VGA Mode
    Last Known Good Configuration (your most recent settings that worked)
    Directory Services Restore Mode (Windows domain controllers only)
    Debugging Mode

    Start Windows Normally
    Reboot
    Return to OS Choices Menu

Use the up and down arrow keys to move the highlight to your choice.
```

A címtár visszaállítását a Windows egyik speciális biztonsági üzemmódjában a Directory Services Restore Mode-ban *(Címtárszolgáltatások visszaállítási üzemmódja)* végezhetjük el. Az F8 pontos időzítése után a következő rázós pont a bejelentkezés: nincs Active Directory, így nem használhatók a megszokott felhasználónevek és jelszavak. Egyetlen módon juthatunk be: a címtár-visszaállítási üzemmód jelszavát valamikor régen, a címtár telepítése közben kellett megadnunk, a jelszóhoz tartozó felhasználónév pedig az eredeti, beépített Administrator *(Rendszergazda)*. Ha sikerült bejutnunk, akkor következhet az NTBACKUP indítása, és a System State visszatöltése a mentési fájlból.

Mivel az Active Directory esetén egy elosztottan tárolt adatbázist kell visszaállítanunk, a címtár visszaállítása három különféle módszerrel történhet, bizonyos esetekben igen fontos lehet, hogy a megfelelőt válasszuk:

- **Normal** *(normál)* – Normál visszaállítás során az adatok (például az Active Directory-objektumok) megtartják eredeti frissítési sorszámukat. Az Active Directory replikálórendszere a sorszám alapján érzékeli és továbbítja az Active Directory változásait a tartományvezérlők között. Így a normál módon visszaállított adatok régi adatként jelennek meg az Active Directoryban, vagyis ezeket az adatokat a rendszer már biztosan nem továbbítja a többi tartományvezérlőre. A visszaállított objektumokat tehát a replikáció szinte azonnal felülírja a többi tartományvezérlőről érkező példányokkal. Ha a visszaállított adatokat szeretnénk elterjeszteni a tartományban, akkor autoritatív *(mérvadó)* visszaállítást kell használnunk.

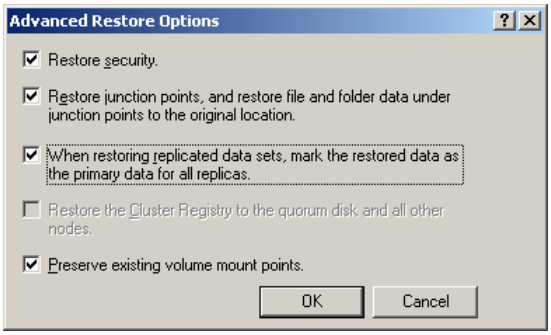


5.17. ábra: *A rendszerállapot adatok három különböző módon is visszakerülhetnek a tartományvezérlőre*

- **Authoritative** *(mérvadó)* – Az Active Directory adatainak mérvadó visszaállításához a rendszerállapot-adatok visszaállítása és a kiszolgáló újraindítása után (de még az első replikáció előtt) futtatnunk kell az ntdsutil.exe segédprogramot. Az *ntdsutil* segítségével az Active Directory-objektumokat mérvadó visszaállításhoz jelölhetjük meg. Ez azt jelenti, hogy az *ntdsutil* úgy frissíti az objektumok sorszámát, hogy azok biztosan nagyobbak legyenek bármelyik másik replikán tárolt sorszámnál, így a visszaállított adatok fogják felülírni a többi tartományvezérlőn tárolt objektumokat. Mérvadó visszaállításra például akkor lehet szükség,

ha véletlenül töröltünk, vagy módosítottunk egy Active Directory-objektumot (például az összes felhasználó- és számítógépfiókot tartalmazó szervezeti egységet), és a változás már replikálódott a többi tartományvezérlőre is. Ha ilyen esetben normál módon állítjuk helyre az objektumot, akkor a replikáció a helytelen állapotot tekinti újabbnak, vagyis ismét ez fog replikálódni a visszaállított kiszolgálóra is.

- **Primary** *(elsődleges)* – elsődleges visszaállítási módszert akkor kell használnunk, ha nincs egyetlen működőképes tartományvezérlőnk sem, vagyis a visszaállítani kívánt kiszolgáló a replikált adatkészlet egyetlen példányát fogja tartalmazni. Általában tehát csak akkor van szükség elsődleges visszaállításra, ha a tartomány minden tartományvezérlője használhatatlan, és a teljes tartományt a biztonsági másolatból kell visszaállítani. Elsődleges visszaállítás végrehajtásához az NTBACKUP felületén (visszaállítás közben az Advanced szakaszban) be kell jelölnünk a *Replikált adatkészletek visszaállítása esetén a visszaállított adatok megjelölése az összes másolat elsődleges adatkészleteként* opciót.



5.18. ábra: *Az elsődleges visszaállítás kissé elrejtett, de nagyon hosszú nevű opciója*

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. Windows Server 2003 SP2 és Windows XP SP2 esetén a beállítható paraméterek száma 1800 körül van, Vista ügyfél használata esetén pedig még több, nagyjából 2400 opció áll rendelkezésre.

A csoportházirend kezelésének eszközei
Ebben a screencastban megismerkedünk a csoportházirend kezelésének szokásos eszközeivel, és kipróbáljuk azok legfontosabb lehetőségeit.
Fájlnév: II-2-6a-Group-Policy-Management.avi

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.

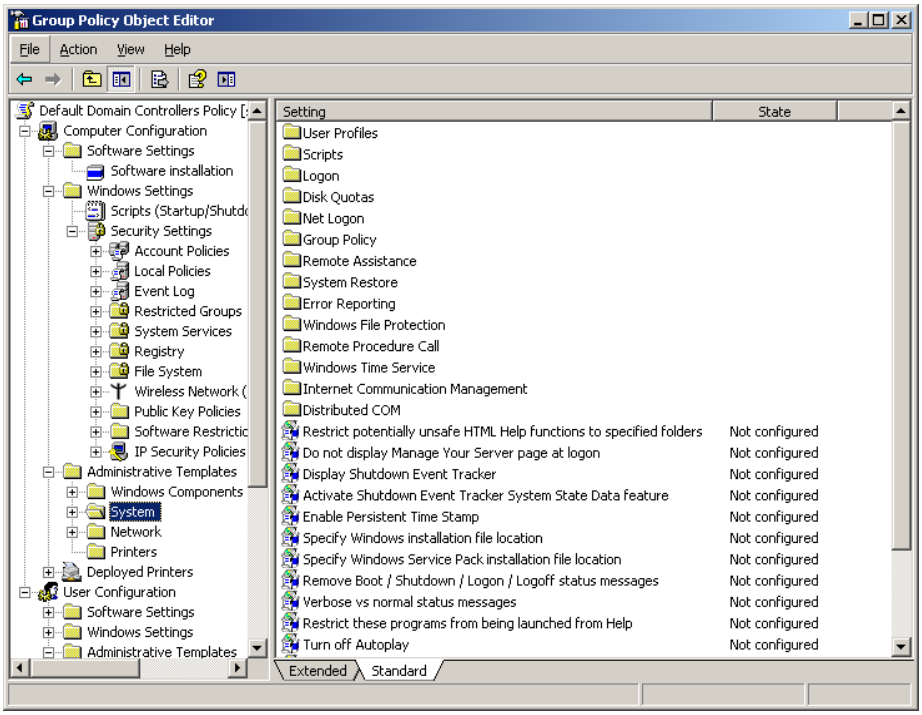
A csoportházirend esetében a beállítások az Active Directory tárolóihoz (telephely, tartomány, szervezeti egység) kapcsolhatók és az adott tárolóban lévő összes számítógép-, illetve felhasználó objektumra érvényesek lesznek. A helyi házirendben is szereplő beállítások mellett a csoportházirend számos 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. A számítógépek funkciója szerint elkészített sablonokat a *%sys-*

temroot%\security\templates mappában találhatjuk meg. 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.



5.19. ábra: *Könnyű eltévedni a beállítási lehetőségek tengerében*

- **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.

A következőkben felsorolunk néhány konkrét példát a csoportházirend felhasználására:

- Eltüntethetjük az Asztalról és a Start menüből azokat az ikonokat, amelyeket az adott felhasználó számára fölöslegesnek ítélünk (Sajátgép, Hálózati helyek, Futtatás stb.).
- Megtilthatjuk a Control Panelhez *(Vezérlőpult)*, illetve annak egyes elmeihez való hozzáférést.
- Letilthatjuk a parancssor, illetve a parancssori végrehajtás (cmd fájlok) használatát.
- Megtilthatjuk a registry közvetlen szerkesztését (regedit).
- Eltávolíthatjuk a megadott menüpontokat és paneleket az Internet Explorer felületéről.
- Megadhatjuk az Internet Explorer proxybeállításait és tetszőleges elemeket adhatunk a Kedvencek listához.
- Beállíthatjuk az egyes rendszerszolgáltatások indítási módját, vagyis engedélyezhetjük és tilthatjuk futásukat.
- Megadhatjuk a vezetéknélküli hálózatok beállításait.
- A felhasználó bejelentkezéséhez üdvözlő, illetve figyelmeztető üzenetet kapcsolhatunk.
- Megtilthatjuk bizonyos alkalmazások futtatását.

Csoportházirend objektumok létrehozása és beállítási lehetőségek
Ebben az előadásban csoportházirend objektumokat hozunk létre és áttekintünk néhány, ezekben az házirendekben megadható beállítási lehetőséget.
Fájlnév: II-2-6b-GPO.avi

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 hatásának szűrése

Minden GPO-hoz tartozik hozzáférés-vezérlési lista, aminek segítségével egyrészt megóvhatjuk az objektumot az illetéktelen módosításoktól, másrészt biztonsági csoportok szerint szűrhetjük is az objektum hatását. Ha nem szeretnénk, hogy a GPO hatása egy adott biztonsági csoportra érvényesüljön, egyszerűen elvehetjük az adott csoport Read/Apply *(olvasás/alkalmazás)* jogát. Fordított esetben, ha csak meghatározott csoportnak (csoportoknak) adunk Read/Apply jogot, akkor a házirend hatása a kiválasztott csoportok tagságán kívül senki másra nem fog érvényesülni. Természetesen a szűrés nemcsak felhasználókra, hanem számítógépekre is érvényesíthető, mivel a biztonsági csoportoknak a számítógép objektumok is tagjai lehetnek.

A fentieken kívül a csoportházirend hatókörét WMI-szűrők segítségével is módosíthatjuk. Ebben az esetben a megadott WMI-szűrő az adott számítógép valamely tulajdonságát (például a memória mennyisége, a processzor architektúrája, valamely program, vagy javítócsomag megléte stb.) kérdezi le, és a csoportházirend objektum érvényesítése a lekérdezés eredményétől függően megy végbe.

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

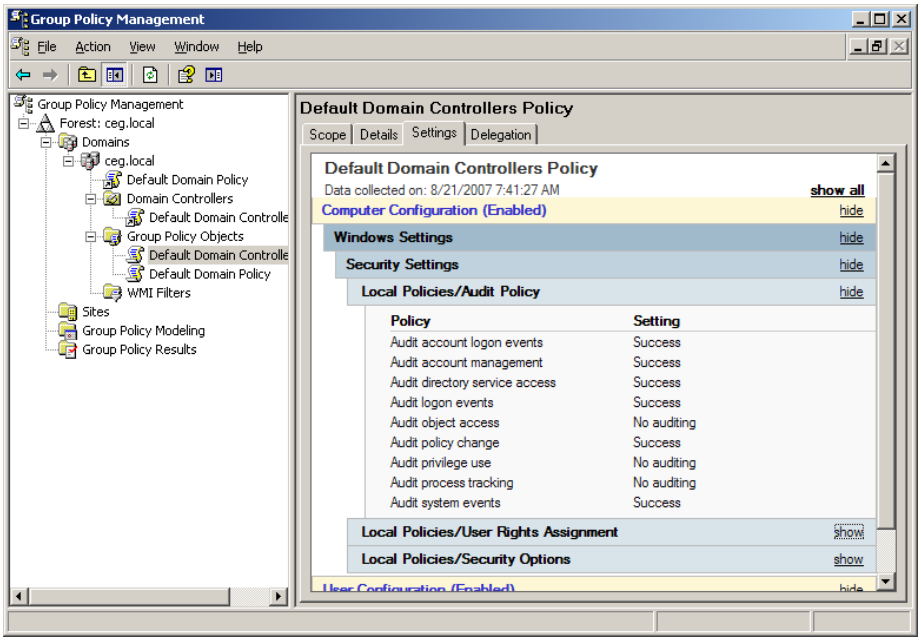
A csoportházirend objektumokon végrehajtott változások nem érvényesülnek azonnal a számítógépeken, illetve felhasználókon. Az automatikus frissítés az ügyfélgépek esetében 90, a tartományvezérlőknél pedig 5 percenként történik.
A türelmetlenebbek azonban kézzel is kikényszeríthetik a frissítést a *gpupdate* (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. Az MMC-bővítmény jelenlegi legújabb (SP1) verziója ingyenesen letölthető a Microsoft webhelyéről *(http://go.microsoft.com/fwlink/?linkid=21813)*. 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, bár csak Windows Server 2003 rendszerre telepíthető. A Windows Vista operációs rendszerben a konzol beépítetten megtalálható.



5.20. ábra: *A Group Policy Management konzol*

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

A replikáció és a telephelyek

Az Active Directory-hálózat növekedésnek egy pontján elkerülhetetlenné válik, hogy szembenézzünk a telephelyek kialakításának problémáival. Természetes igény, hogy a központtól távol dolgozók is részesüljenek a központilag (vagy éppen elosztottan) felügyelt címtár, a csoportházirend, vagy például az Exchange áldásaiból. Korlátozott sávszélesség esetén mindenképpen a helyszínen üzemelő tartományvezérlő a jó megoldás, ekkor viszont a lokális hálózaton üzemeltetett címtár esetében nem jelentkező problémák fognak felmerülni. Hogyan és milyen gyakorisággal történik a tartományvezérlők közötti replikáció? Milyen sávszélesség szükséges ehhez, és persze hogyan lehetne csökkenteni a szükségleteket? A telephelyen lévő számítógépeknek nyilván a

helyben lévő tartományvezérlő használatával kellene bejelentkezniük, onnan kellene letölteniük a csoportházirend objektumokat, logon szkripteket stb. De honnan fogják tudni az ügyfélgépek, hogy melyik a saját, közelben lévő tartományvezérlőjük, amikor a DNS-től csak egy szinte véletlenszerűen kiválasztott IP-címet kapnak?

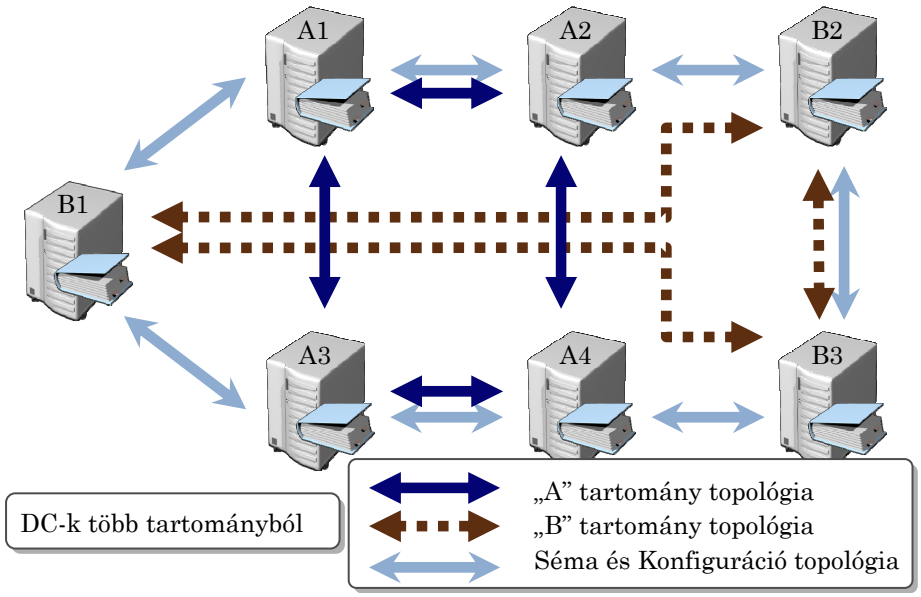
A következőkben ezekre a kérdésekre keresünk választ, megismerkedünk a replikáció finomhangolásának módszereivel, és az egészséges telephelystruktúra kialakításához szükséges ismeretekkel.

A replikáció

A replikáció segítségével képes az Active Directory-címtárszolgáltatás a különböző tartományvezérlőkön tárolt címtár-adatbázisok folyamatos szinkronban tartására. A tartomány összes tartományvezérlőjén módosíthatóak a címtár adatai, ezért az összes tartományvezérlő automatikusan részt is vesz a replikációban, tehát a címtáradatok bármilyen módosítását a rendszer a tartomány összes tartományvezérlőjére replikálja. Az Active Directory több főkiszolgálós (multimaster) replikációs modellt használ, amely lehetővé teszi, hogy a címtár módosítását bármelyik tartományvezérlőn elvégezhessük, majd a változások az összes tartományvezérlő címtárpéldányába bekerüljenek.

Ahogyan már korábban említettük, az adatokat az egyes tartományvezérlőkön a címtáradatbázis tartalmazza, amely logikailag címtárpartíciókra tagolódik. Mindegyik partíció különböző típusú adatokat tárol, ezek lehetnek a tartomány objektumai, a séma, különféle konfigurációs adatok, vagy alkalmazásadatok. Az adott erdőn belül valamennyi tartományvezérlőn megtalálható a séma- és konfigurációs partíció másolata, az egyes tartományok vezérlőin pedig a tartományobjektumokat tartalmazó replika. Amint az 5.21. ábrán látható, a különböző címtárpartíciók esetén különböző replikációs topológia alakul ki, mivel a tartományadatok replikációja csak az egyes tartományokon belül, míg a séma és konfigurációs partíció az erdő valamennyi tartományvezérlője között replikálódik.

A multimaster replikáció segítségével valamennyi tartományvezérlő szinte folyamatosan frissíti az általa tárolt példányt a többi példány változásainak megfelelően. A replikáció természetesen teljesen automatikusan történik, a rendszer minden objektum esetében az utolsóként történt változtatásokat érvényesíti a másolatokban. Szintén automatikusan megtörténik a replikáció konfigurációja, vagyis a tartományvezérlők feltérképezése és a kapcsolatok kialakítása is, külön minden egyes címtárpartícióra vonatkozóan.



5.21. ábra: *Replikációs topológia több tartomány esetén*

A replikáció csak akkor jelent tényleges adatátvitelt, ha van mit szinkronizálni, vagyis változások történtek az adatbázisban. Ilyen változás például:

- ha bővítjük a címtár-adatbázist (pl. egy felhasználó létrehozása),
- ha megváltoztatunk egy objektumot (pl. jelszóváltoztatás),
- ha megváltoztatjuk egy konténer (szervezeti egység) nevét,
- ha törlünk egy objektumot.

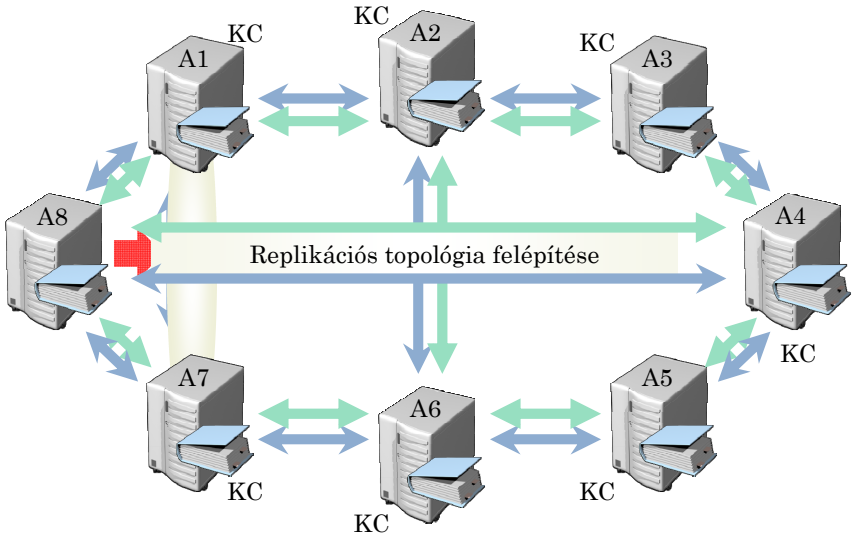
A változások követése, és az adatok átvitele az objektumok tulajdonságainak szintjén történik, vagyis például, ha megváltozik egy felhasználó telefonszám mezője, akkor nem az egész objektum, hanem önállóan csak a megváltozott tulajdonság (a telefonszám) replikálódik a többi tartományvezérlőre.

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, gyűrűs replikációs 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.



5.22. ábra: *A KC új tartományvezérlőt illeszt be a replikációs topológiába*

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,

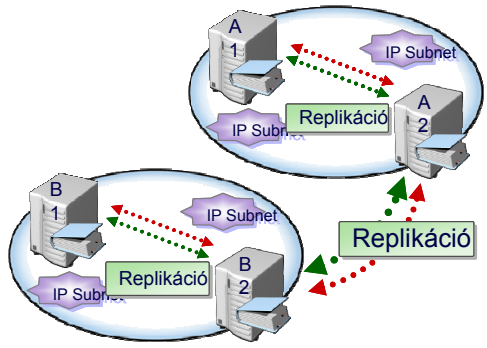
sőt esetleg nincs is állandó kapcsolat. A telephelyek közötti replikáció a sávszélesség minél hatékonyabb kihasználását próbálja elérni; a címtárfrissítések automatikusan mennek végbe egy beállítható ütemezés alapján (alapértelmezés szerint háromóránként). A telephelyek közötti replikációval kapcsolatos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

A telephelyek

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.

Az Active Directory telephely koncepciójának alapvetően két célja van:

- Egyrészt növelhetjük vele a replikáció hatékonyságát. A gyors kapcsolattal rendelkező számítógépek csoportjaként definiált telephelyeken belül gyakoribb a replikáció, így a telephelyen belüli tartományvezérlők kapják meg leggyorsabban a frissítéseket. A telephelyek közötti lassúbb kapcsolaton keresztül ritkábban történik meg a címtáradatok szinkronizálása.



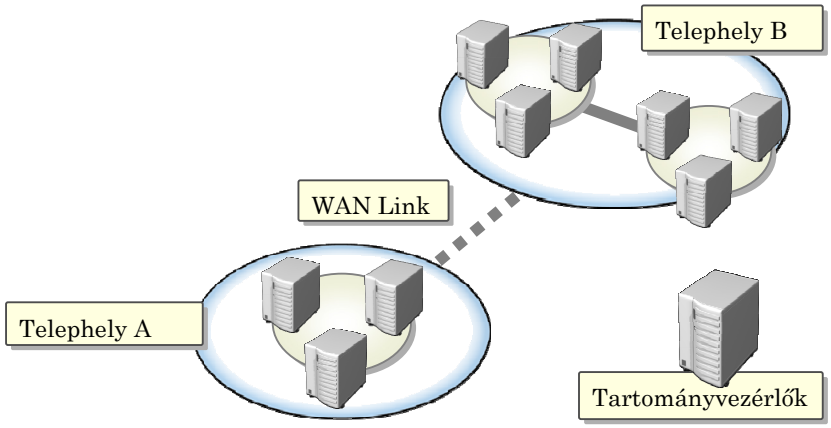
- Másrészt meghatározhatjuk, hogy a telephelyen lévő számítógépeket a telephelyen lévő tartományvezérlő jelentkeztesse be, innen töltsék le a csoportházirend objektumaikat, bejelentkezési szkriptjeiket stb.

A fenti két pont alapján mindjárt le is vonhatunk két fontos következtetést a telephelyek kialakítására vonatkozóan:

- Nem érdemes (hacsak nincs valami különleges indok) helyben lévő tartományvezérlő nélküli telephelyet definiálni, mivel ebben az esetben a fenti két előnyös tulajdonság egyike sem jelentkezhet.

- Nem érdemes telephelyeket definiálnunk olyan helyszínek esetében, amelyek között gyors (10Mb/sec, vagy még gyorsabb) hálózati kapcsolat van. A gyors kapcsolattal rendelkező IP-alhálózatok telephellyé alakítása nem növeli, hanem inkább csökkenti a teljesítményt.

A telephelyek és a tartományok közötti legfontosabb különbség az, hogy a telephelyek a hálózat fizikai felépítését, a tartományok pedig a szervezet logikai szerkezetét követik. A telephelyek és tartományok között bármiféle átfedés lehetséges, egy telephely tartalmazhat több tartományt, és egy tartomány is kiterjedhet több telephelyre. A lényeg minden esetben a replikációhoz, valamint az ügyfelek és a tartományvezérlők közötti adatforgalomhoz szükséges sávszélesség optimális feltételekkel történő biztosítása.



5.23. ábra: *A telephelyek közötti kapcsolat általában lassúbb és kevésbé megbízható*

Számítógépek hozzárendelése a telephelyekhez

Az ügyfélgépek telephelyekhez rendelése IP-címük és alhálózati maszkjuk alapján történik. Minden ügyfélgép az adott telephely IP-alhálózatához kiszolgálóként megadott tartományvezérlőt fogja előnyben részesíteni a bejelentkezés során. A telephelyekhez tartozó alhálózatok és kiszolgálók meghatározását az Active Directory Sites and Services *(Active Directory helyek és szolgáltatások)* MMC-modulban tudjuk elvégezni. A művelet négy lépésből áll:

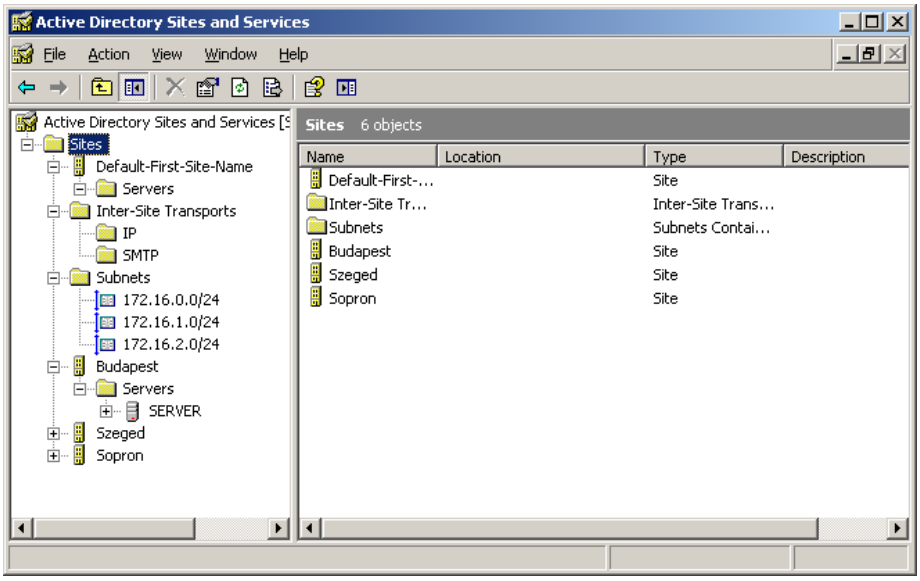
- Elsőként létre kell hoznunk az új telephelyet a Sites tárolóban.
- Az új telephely alatt létrejövő Servers tárolóhoz hozzá kell adnunk a telephely kiszolgálását végző tartományvezérlőt (vagy tartományvezérlőket).
- A Subnets tárolóban létre kell hoznunk a telephely IP-alhálózatainak megfelelő bejegyzéseket.

- Végül a létrehozott IP-alhálózatok tulajdonságlapjain ki kell választanunk azt a telephelyet, amelyhez az adott alhálózat tartozik.

Az itt megadott instrukciókat a DNS-kiszolgáló fogja közölni az ügyfelekkel, akik így saját IP-címük és alhálózati maszkjuk alapján eldönthetik, hogy melyik telephelyhez tartoznak, a telephely alapján pedig kiválaszthatják, hogy melyik tartományvezérlőhöz kell csatlakozniuk.

Telephelyek tervezése

A telephely-struktúra megtervezése nem minden esetben egyszerű feladat, az épületek egymástól való fizikai távolságán kívül sok esetben más szempontokat is figyelembe kell vennünk. A legfontosabb kérdés, amit el kell döntenünk, hogy biztosan érdemes-e telephelyet fabrikálni az adott helyszínből, vagy nyugodtan használhatják a központban lévő kiszolgálókat, esetleg mindenképpen az Active Directoryn kívül kell maradniuk. Általánosan használható receptet adni valószínűleg lehetetlen, de azért megpróbáljuk felvonultatni a legfontosabb szempontokat:



5.24. ábra: *Minden telephelyhez kiszolgáló(ka)t és alhálózato(ka)t rendelhetünk*

- Milyen következményei vannak az új telephely földrajzi elhelyezkedésének?

- Hány számítógép működik a telephelyen? – két számítógépnek valószínűleg nem érdemes külön tartományvezérlőt kivinni a telephelyre, tartományvezérlő nélkül pedig értelmetlen a telephellyé alakítás, egyszerűbb a központban lévő kiszolgálókat használni.
- Van-e esetleg már kiszolgáló, vagy tartományvezérlő? – komoly érv *lehet* a telephellyé alakítás mellett, ha van már a helyszínen kiszolgáló. Ha erre szükség volt, (és nincs nagyon gyors hálózati kapcsolat), akkor valószínűleg érdemes a kiszolgálóból tartományvezérlőt, a helyszínből pedig telephelyet gyártani.
- Milyen IP-alhálózatokból áll az új telephely?
- Milyen típusú és sebességű WAN-kapcsolat jellemzi az új telephelyet, milyen költségekkel jár a hálózati kapcsolat?

Végezetül még néhány tipp a korrekt és praktikusan működő telephelyi környezethez:

- Egy „egészséges” telephelyen célszerűen van tartományvezérlő.
- Egy – az adott helyszínen használt – célalkalmazás is igényelheti a telephelyet.
- Ha a fentiek közül egyik sem teljesül, akkor valószínűleg nem érdemes telephellyé alakítani az adott helyszínt.
- Mindig specifikáljuk az összes telephely, összes IP-alhálózatát, mivel az ügyfélgépek ez alapján találják meg a hozzájuk közel lévő tartományvezérlőt.

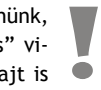
HATODIK FEJEZET

Hibakeresés és -elhárítás

A fejezet tartalma:

Ami elromolhat, az el is romlik, egyáltalán nem mindegy azonban, hogy a hibaelhárítás két percig, vagy két hónapig tart – sajnos, akár azonos hiba esetén is előfordulhat mindkét véglet, a dolog egyszerűen azon múlik, hogy ki az, aki a hibaelhárítással próbálkozik, és milyen eszközök állnak rendelkezésre a probléma megkereséséhez és elhárításához. Bár a hibaelhárítás természeténél fogva nem sablonművelet, vagyis nem lehet minden helyzetben használható receptet adni, ebben a fejezetben megpróbálkozunk az alapelvek, és felhasználásra érdemes alapeszközök bemutatásával.

A hibák elhárításához általában a programok felhasználói felülete mögé kell merészkednünk, így mindenképpen indokolt az óvatosság; nem számíthatunk a megszokott „bolondbiztos” viselkedésre, vagyis egy meggondolatlan mozdulattal az eredetinél akár sokkal nagyobb bajt is okozhatunk. Egy fontos szabályt tehát mindig célszerű betartani: Ha nem **tudod**, hogy mit csinálsz, és pontosan mit akarsz vele elérni, akkor inkább ne csináld!



A fejezetben a következő témákkal fogunk megismerkedni:

- **Hibakeresés és javítás mélyebben** – elsőként azokkal a hibákkal foglalkozunk, amelyek megakadályozzák az operációs rendszer szokásos módon való indítását, illetve a rendszer leállásával járnak, vagyis kezelésükhöz speciális, általában grafikus felület nélküli eszközökre van szükség.
    - **A rendszerindítás folyamata és az indítómenü elemei** – ebben a részben részletesen megismerkedünk a Windows-rendszerek indítási folyamatának lépéseivel, és a hibakeresésre szolgáló üzemmódokat lehetővé tevő indítómenüvel.

    - **A helyreállítási konzol** *(Recovery Console)* – áttekintjük a Windows telepítőlemezéről indítható Recovery Console lehetőségeit. Az eszköz segítségével hozzáférhetünk a más módon már nem indítható operációs rendszer fájljaihoz és más beállításaihoz.
- **A „kék halál"** – megismerkedünk a Windows-rendszerek leállását kísérő hírhedt kék képernyő kiváltó okaival, és a megjelenő adatok jelentésével.
- **Grafikus ellenőrző- javító eszközök** – a sikeres rendszerindítás után rendelkezésünkre áll a Windows valamennyi beépített hibakereső-, javító és ellenőrző eszköze. Ebben a részben ezek közül fogunk a legfontosabbakkal megismerkedni.
- **Adataink biztonsága** – Ha már minden más módszer csődöt mondott, akkor a biztonsági mentésből való visszaállításhoz kell folyamodnunk. Ebben a részben a mentési rendszer megtervezéséről és használatáról lesz szó.
- **Külső eszközök** – a Windows beépített eszközein kívül számos külső programot is igénybe vehetünk a hibakereséshez. Ebben a részben a Sysinternals cég által készített eszközök közül ismerkedünk meg a legfontosabbakkal.

Bár témánk alapvetően a Windows Server 2003 R2, a fejezetben leírtak gyakorlatilag teljes mértékben érvényesek a régebbi kiszolgálórendszerekre (Windows 2000 Server) és az ügyfélrendszerekre is (Windows 2000 és XP). A Windows Vista esetén természetesen vannak bizonyos (esetenként jelentős) különbségek és újdonságok is, de ezek legnagyobb részéről a könyv első részében már szót ejtettünk.

Hogyan lehet észlelni a hibákat?

A hibák kezelésével kapcsolatban rendkívül fontos kérdés, hogy milyen módon szerzünk tudomást arról, hogy valamiféle hiba történt a rendszer, vagy egy számítógép működésében. Természetesen, ha elég sokáig várunk, akkor egészen nyilvánvaló jelek is várhatók (például sűrű fekete füst a szerverszobában☺), de sokkal jobban járunk, ha elébe megyünk az ilyen helyzeteknek és rendszeresen ellenőrizzük például az eseménynaplót és az egyes komponensek önálló naplófájljait is. A legjobb persze az (és a különféle rendszerfelügyeleti szoftverek, például a System Center Essentials, vagy a System Center Operations Manager használatával ez meg is valósítható), ha kiszolgálóink és az ügyfélgépek is önállóan jelzik, ha valamiféle probléma miatt beavatkozást igényelnek.

A legnehezebben felderíthető hibák azok, melyek nem járnak konkrét, jól beazonosítható jelenséggel (például hibaüzenet), nincs nyomuk az eseménynaplóban, csak bizonyos homályos, nehezen, vagy egyáltalán nem reprodukálható tünetek utalnak arra, hogy valami nincs teljesen rendben a kiszolgálóval. A következő jelenségekre érdemes figyelmet fordítani:

- A kiszolgáló a szokásosnál lassabban működik, esetleg néha minden különösebb látható ok nélkül újraindul.
- Az ügyfelek a szokásosnál lassabban érik el a kiszolgálót, esetleg bizonyos műveletek (például névfeloldás) elvégzésére sokat kell várakozni.
- Különféle hálózati szolgáltatások elérése bizonytalan, néha gond nélkül működik, máskor egyáltalán nem érhető el.
- Rejtélyesnek tűnő hardverproblémák jelentkeznek (melegedés, hangok stb.)

Ha a megfigyelt jelenségek alapján már biztosak vagyunk benne, hogy valami probléma lehet a kiszolgálóval, akkor az alábbi eszközöket vethetjük be a konkrét hibajelenség azonosításához:

- Task Manager *(Feladatkezelő)* – a futó (vagy nem futó) folyamatok azonosítására és az erőforrások foglaltságának ellenőrzésére
- Services *(Szolgáltatások)* MMC – a rendszerszolgáltatások állapotának ellenőrzéséhez
- Event Viewer *(Eseménynapló)*
- Alkalmazás- és rendszernaplófájlok (AD, IIS, ISA, SQL stb.)
- System Information eszköz (Msinfo32)
- Külső (pl. Sysinternals) eszközök

Hibakeresés és javítás mélyebben

Ebben a részben olyan hibákkal foglalkozunk, amelyek megakadályozzák az operációs rendszer megszokott módon való indítását. Az ilyen hibák kezelése azért nehezebb a szokásosnál, mert nem használhatjuk a jól ismert és rendszeresen alkalmazott eszközöket, minden műveletet egy kevésbé komfortos és általában kevésbé ismert környezetben kell elvégeznünk.

A rendszerindítás folyamata és az indítómenü elemei

A következőkben megismerkedünk a Windows-rendszerek indítási folyamatával, hogy a folyamat közben keletkező hibák hatékonyabban felderíthetők és elháríthatók legyenek. Hogy megtalálhassuk a hibák valódi okait, ismernünk kell az adott folyamat végrehajtásának részleteit, mivel egy tetszőleges rendszer vagy program hibájának elhárításához pontosan kell tudnunk, mi történik akkor, ha a rendszer vagy program hibátlanul működik.

Hogyan indul az operációs rendszer?

A számítógép bekapcsolása után az alaplapon lévő flash memóriában tárolt program betöltődik a memóriába, és nekikezd a POST (Power-on Self Test) nevű művelet végrehajtásának. A POST által elvégzett konkrét műveletek teljes mértékben az adott hardver gyártójának hatáskörébe tartoznak, de a legtöbb esetben ilyenkor történik meg a különféle feszültségszintek ellenőrzése, a RAM, a grafikus kártya, a különféle bővítőkártyák és a legfontosabb perifériák működőképességének vizsgálata. A BIOS Setup program segítségével általában bizonyos mértékig befolyásolhatjuk a POST futását, kérhetünk további teszteket (például a memóriára vonatkozóan), és szabályozhatjuk a képernyőn megjelenő üzenetek mennyiségét.

Szintén a BIOS Setupban határozhatjuk meg, hogy mi történjen a POST után, vagyis milyen sorrendben próbálkozzon a számítógép a különféle eszközökről (merevlemez, CD-ROM, hajlékonylemez, hálózat stb.) történő rendszerindítással. Ha a számítógép a merevlemezről indul, akkor a sikeres POST után a BIOS ellenőrzi a fő rendszertöltő rekordot (*Master Boot Record, MBR).*

Az MBR minden particionált merevlemezen megtalálható (a particionáláskor kerül rá), mégpedig a lemez legelső fizikai szektorában (vagyis a teljes mérete 512 bájt). Az MBR tartalmaz némi végrehajtható kódot *(Master Boot Code),* az adott lemez egyedi azonosítóját *(Disk Signature)* és a négyszer 16 bájt méretű partíciós táblát. Az MBR végén található partíciós tábla tehát négy bejegyzést tartalmazhat. Az egyes bejegyzésekben szerepel az adott partíció első és utolsó szektorának azonosítója, a partíció szektorainak száma, és a fájlrendszerre utaló érték. Ha a bejegyzés utolsó két bájtjának értéke 0x8001, akkor aktív partícióról van szó. Az MBR utolsó két bájtja egy speciális érték (0x55AA), amely a szektor végét jelzi, és amelynek hiánya komoly problémákat okozhat.

Ha az MBR utolsó két bájtja nem 55AA, akkor a BIOS azt feltételezi, hogy az MBR sérült, vagy a lemez egyáltalán nincsen particionálva. Ekkor általában (bár a pontos szöveg BIOS-függő) az *Operating system not found* üzenet jelenik meg, a számítógép pedig természetesen nem folytatja az indítást. Ha a

BIOS megfelelőnek ítéli az MBR-t, akkor betölti és elindítja a benne található programot. Az MBR programja végigolvassa a partíciós táblát, és kiválasztja belőle az aktívként megjelölt partíciót. Ha ez valami miatt nem sikerül (például egyáltalán nincs aktív partíció) akkor az *Operating System not found*, vagy az *Invalid partition table* üzenet jelenik meg. Ha sikerült megtalálni az aktív partíciót, akkor az MBR-kód betölti az adott partíció boot-szektorát a memóriába és ellenőrzi azt.

A bootszektor az egyes partíciók első szektora, amely az adott partícióra telepített operációs rendszer indítását lehetővé tevő programkódot, és a partícióra vonatkozó különféle információkat tartalmazza. A bootszektor a partíció formázásakor jön létre, tartalma pedig a fájlrendszer típusától függ. Az MBR-hez hasonlóan a bootszektor végét is az 0x55AA érték jelzi.

Ha a bootszektort nem sikerül betölteni (például, mert a partíció nincs formázva), akkor az *Error loading operating system* üzenet jelenik meg és a betöltés leáll. Amennyiben a bootszektor végén nincs ott a mágikus 55AA érték, a *Missing operating system* üzenet jelenik meg, és a betöltés természetesen ebben az esetben sem folytatódik. Ha minden rendben van, akkor az MBR-kódtól a vezérlés a boot szektor kódjához kerül, és folytatódik a rendszerindítás.

A bootszektor programjának feladata az, hogy megkeresse és elindítsa a Windows betöltő programját az NTLDR-t, amelynek az indító partíció gyökerében kell lennie. Ha ez valamilyen ok miatt nem sikerül, akkor ezen a ponton kaphatjuk a *Missing NTLDR* hibaüzenetet (NTFS fájlrendszer esetén). Ha sikerült elindítani az NTLDR-t, akkor az első lépésként 32-bites védett módba kapcsolja a processzort és engedélyezi a memórialapozást, így ezután már rendelkezésre áll a teljes 4 GB-os címezhető tartomány (32-bites processzor esetén).

Az NTLDR ezután a következő műveleteket végzi el [az NTLDR tartalmazza az NTFS (és FAT, illetve FAT32) fájl-rendszerrel formázott partíciók olvasásához és írásához szükséges programkódot]:

- Megvizsgálja a gyökérmappában található *hiberfil.sys* állományt, és ha talál benne alvó állapotban lévő operációs rendszert, akkor visszatölti azt a memóriába, a végrehajtás pedig folytatódik a hibernáláskor megjegyzett ponton.
- Ha nincsen alvó operációs rendszer, akkor az NTLDR beolvassa a gyökérmappában lévő *boot.ini* nevű fájl tartalmát. A *boot.*ini ARC-útvonalak *(Advanced RISC Computing)* formájában tartalmazza a számítógépen található indítható operációs rendszerek helyét. Az NTLDR a *boot.ini* alapján készíti el azt a kis menüt, amiből kiválaszthatjuk az elindítandó operációs rendszert.

A menü csak akkor jelenik meg, ha egynél több bejegyzés van a boot.ini-ben. Egy bejegyzés esetén az NTLDR azt feltételezi (milyen intelligens, nem?), hogy azt az egyet szeretnénk elindítani. Ha egyáltalán nincsen *boot.ini,* akkor az NTLDR azt feltételezi, hogy az operációs rendszer az adott partíció alapértelmezett mappájába *(c:\windows)* van telepítve. Ha ez a mappa nincs a helyén, akkor a következő üzenet jelenik meg: *Windows could not start because the following file is missing or corrupt: \winnt root\system32\ntoskrnl.exe*.

- Miután valamilyen módon sikerült tisztázni, hogy melyik operációs rendszert is kell elindítani (kiválasztottuk a menüből, vagy sikerült az alapértelmezés alapján megtalálni), az NTLDR elindítja az ntdetect.com programot (az ntdetect.com szintén a gyökérmappában található). Az ntdetect listát készít a számítógép hardverkomponenseiről (busztípusok és eszközök, lemezmeghajtók, grafikus kártya, billentyűzet, soros és párhuzamos portok, egér stb.) és az eredményt átadja az NTLDR-nek.

Ezen a ponton, vagyis az indítandó rendszer kiválasztása (automatikusan, vagy a menüből) után az NTLDR törli a képernyőt, és megjelenít egy karakteres „folyamatjelzőt". Sajnos (vagy szerencsére) ez többnyire szinte láthatatlan a gyors betöltődés miatt. A különféle indítási opciók (csökkentett mód, DSRM stb.) elérésére szolgáló indítómenü megjelenítéséhez viszont pontosan akkor kell megnyomnunk az F8 billentyűt, amikor ez a folyamatjelző látható, (illetve nem látható).

- Ezután az NTLDR sorban elkezdi betölteni a memóriába rendszer különböző részeit (de csak betölti, még nem inicializálja, illetve nem indítja el őket). Elsőként betöltődik az *ntoskernel.exe* és a *hal.dll* (mindkét fájlnak a *%systemroot%\System32* mappában kell lennie), majd a registry *HKLM\SYSTEM* ága (a *%systemroot%\System32\Config\System* fájlból, és az ebben tárolt adatok alapján valamennyi szükséges eszközvezérlő. Az eszközvezérlőket tartalmazó fájlok a *%systemroot%\System32\Drivers* mappában találhatók. Az NTLDR a registryben tárolt adatok alapján határozza meg, hogy a betöltődés további részét meghatározó úgynevezett Control Setek közül melyiket kell felhasználnia. Ezen a ponton történik a Last Known Good Configuration *(legutolsó helyes konfiguráció)* betöltése (lásd később), ebben az esetben egy korábban elmentett, a legutolsó módosításokat még nem tartalmazó Control Setet fog felhasználni az NTLDR.
- Utolsó tevékenységeként az NTLDR elindítja a már korábban betöltött ntoskernel.exe programot, a betöltődés további részét már az *ntoskernel.exe* vezérli.

- Az *ntoskernel* indulásakor a képernyő grafikus üzemmódban vált, és a színes Windows logó alatt megjelenik a dísz folyamatjelző, ami nem jelzi ugyan semmiféle folyamat előrehaladását, de legalább kellemes, megnyugtató látványt nyújt. Közben azért fontosabb dolgok is történek, az *ntoskernel* memóriastruktúrákat hoz létre, inicializálja a megszakításkezelőket, elindítja a folyamatkezelőt és létrehozza a System folyamatot. Ezután kerül sor az NTLDR által betöltött eszközkezelők inicializálására. Következő lépésként az *ntoskernel* elindítja a Session Managert (smss.exe), majd a winlogon.exe indításakor megjelenik a Windows bejelentkező ablaka.

Az indítómenü

A Windows indítómenüje lehetővé teszi azt, hogy az operációs rendszert különféle speciális üzemmódokban indítsuk el. A speciális üzemmódokra általában hibakeresés, illetve elhárítás céljából van szükség. Az indítómenüt az NTLDR futása közben lenyomott F8 billentyű segítségével érhetjük el. A következőkben áttekintjük az egyes menüpontok szerepét, és felsorolunk néhány tipikus problémát, amelyek az indítómenü használatával oldhatók meg.

Az indítómenü használata
Ebben a screencastban az operációs rendszer indítómenüjének különféle lehetőségeivel ismerkedhetünk meg.
Fájlnév: II-3-1a-Boot-Menu.avi

Csökkentett módok

Ha a számítógép a szokásos módon nem indítható, illetve a szokásos indításkor olyasmi is elindul, amire egyáltalán nincsen szükség (például különféle kedves spyware programok, vagy egyéb férgek), akkor érdemes megpróbálkozni valamelyik csökkentett módban történő rendszerindítással. Természetesen bármelyik csökkentett módot is választjuk, valamelyik helyi felhasználói fiók használatával be kell jelentkeznünk a rendszerbe.

- **Safe Mode** *(Csökkentett mód)* – Csökkentett módban a Windows az alapértelmezett beállításokat használja (hálózati szolgáltatások betöltésére nem kerül sor). Ebben az esetben az operációs rendszer csak a működéséhez nélkülözhetetlen eszközmeghajtókat (VGA monitorvezérlő, a tárolóeszközök (IDE, SCSI, CD-ROM stb.) kezelőprogramjai, egér és billentyűzet) és a legszükségesebb szolgáltatásokat (Logical Disk Manager, Plug and Play, RPC stb.) indítja el. Nincsen hálózat, nem használhatóak a különféle extra eszközök (USB-memóriák, hangkártya

stb.), és nem indulnak el a szokásos rendszerindításkor automatikusan induló programok sem. Ha a számítógépet ilyen módon sikerül elindítani, akkor megkereshetjük és letilthatjuk, illetve eltávolíthatjuk a problémát okozó eszközillesztőt, szolgáltatást, vagy programot.

- **Safe Mode with Networking** *(Csökkentett mód hálózattal)* – Ez az indítási mód megegyezik a csökkentett móddal, de betöltődnek a hálózati alapszolgáltatások is (DHCP- és DNS-ügyfél, Server, Workstation stb.) vagyis elérhetjük és felhasználhatjuk a hálózati erőforrásokat is. Ebben az esetben használhatunk tartományi felhasználónevet is a bejelentkezéshez.
- **Safe Mode with Command Prompt** *(Csökkentett mód parancssorral)* – ebben az esetben nem indul el a Windows grafikus felhasználói felületét biztosító Windows Explorer (explorer.exe), hanem helyette csak egy parancssort (cmd.exe) kapunk. Akkor lehet szükség erre az indítási módra, ha a számítógép normál módú indítását lehetetlenné tevő problémát maga a Windows Explorer okozza (például hiányzik, vagy sérült az explorer.exe fájl).

A csökkentett módokban elinduló eszközillesztőket és szolgáltatásokat a *HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot* registrykulcs alatt található értékek határozzák meg, a Minimal szakasz mindhárom esetben, a Network szakasz pedig a *Csökkentett mód hálózattal* menüpont választása esetén töltődik be.

Az indítómenü további lehetőségei

A menü további elemei bizonyos speciális problémák esetén használható hibakeresési, illetve helyreállítási lehetőségeket kínálnak:

- **Enable Boot Logging** *(Rendszertöltés naplózásának engedélyezése)* – ha ezt a menüpontot választjuk, akkor indításkor naplófájl készül a betöltött (és a valami miatt be nem töltött) eszközillesztőkről és szolgáltatásokról. A fájl ntbtlog.txt néven a *%systemroot%* mappában található. A rendszer indítása ebben az esetben normál módban történik, de alapértelmezés szerint valamennyi csökkentett mód használata esetén is készül naplófájl. A napló segítségünkre lehet a rendszerindítási hibák pontos okának meghatározásában.
- **Enable VGA Mode** *(VGA mód engedélyezése)* – A számítógép ebben az esetben a grafikus kártya telepített illesztőprogramjának betöltésével, de a lehető legkisebb képernyőfelbontással (640×480) indul. (A csökkentett módokban a rendszer a grafikus kártya illesztőprogramja helyet a Windows beépített VGA-eszközillesztőjét használja.)

- **Last Known Good Configuration** *(Legutolsó helyes konfiguráció)* – A rendszer minden indításkor mentést készít a registrynek a betöltődési folyamatot meghatározó részéről (Control Set). A menüpont kiválasztásakor a rendszer indítása a Windows legutóbbi indításakor elmentett registryadatok alapján történik, vagyis az utolsó bejelentkezés óta módosított illesztőprogram- és rendszerbeállítások el fognak veszni. A Control Set „jó" készletként való megjelölése, a bejelentkezéskor történik, vagyis ekkor az aktuális és a legutolsó helyes Control Set megegyezik. A munkamenet során elvégzett változtatások csak az aktuális registryadatokat érintik, a bejelentkezéskor létrehozott példány megmarad eredeti állapotában, erre térhetünk később vissza (a csökkentett módban való bejelentkezés **nem** szinkronizálja a Control Seteket, vagyis ekkor megmarad a korábbi konfiguráció is). A menüpontot tehát közvetlenül a hibát okozó változtatás után érdemes használni (a következő bejelentkezés előtt), segítségével részlegesen visszaállíthatjuk a registryt (az eszközmeghajtók és szolgáltatások beállításait), de sérült vagy hiányzó fájlok pótlására nem használható.
- **Directory Services Restore Mode** *(Címtárszolgáltatások visszaállítása)* – Az elmentett Active Directory adatbázis mentésből való helyreállításakor van szükség a DSRM üzemmódban történő rendszerindítás használatára (csak tartományvezérlőkön). A DSRM-üzemmód részletei az előző, „Tartományi környezet" című fejezetben találhatók.
- **Debugging mode** *(Hibakeresési mód)* – A rendszer indításkor a soros (COM2), illetve firewire portra küld különféle hibakeresési adatokat.
- **Disable automatic restart on system failure** *(Automatikus újraindítás letiltása rendszerhiba esetén)* – Alapértelmezés szerint rendszerleállás („kék halál") után a számítógép automatikusan újraindul, így nem tudjuk megnézni és felírni a képernyőn látható hibaüzenetet, ami pedig igen fontos lenne a hiba okának megállapításához. Természetesen az alapértelmezett viselkedés a működő rendszer grafikus felületén megváltoztatható, de ha a leállás a Windows indítása közben történik, akkor ez a lehetőség már nem érhető el. A menüpont használatával nem induló rendszer esetében is megváltoztathatjuk ezt a fontos beállítást.

Példák az indítómenü lehetőségeinek használatára

A következőkben felsorolunk néhány, az indítómenü felhasználásával könnyen megoldható tipikus problémát:

- Telepítettünk egy olyan programot a számítógépre, ami hozott magával egy új rendszerszolgáltatást vagy eszközmeghajtót, és beállította ennek automatikus indítását is. Újraindításakor azonban az induló szolgáltatás hibája miatt nem indul el a számítógép („kék halál"). Ebben az esetben csökkentett módban valószínűleg probléma nélkül elindítható a rendszer, és letilthatjuk az újonnan telepített szolgáltatás vagy eszközmeghajtó automatikus indulását, illetve eltávolíthatjuk a programot.
- Telepítettük gépünkre az internetről letöltött rendszerkarbantartó és kávéfőző csodaprogram legfrissebb, 2.43.5f verzióját. Mégsem tetszik azonban a programba integrált e-mailküldési funkció, ami folyamatosan különféle reklámokkal bombázza ismerőseinket, ezért megpróbálunk megszabadulni tőle. Szomorúan tapasztaljuk, hogy a Feladatkezelővel sajnos nem lehet leállítani a folyamatot. Sebaj, töröljük le magát a programfájlt! Amíg azonban a folyamat fut, sajnos a fájlt sem lehet letörölni. Következő lépésként megpróbálhatjuk megkeresni és törölni a registry megfelelő bugyrában *(HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run)* a program automatikus indítását végző bejegyzést. Újraindítás után azonban a csodaprogram.exe újra ott figyel a futó folyamatok között, sőt visszaírta magát a registrybe is. Ekkor következik a csökkentett módban történő indítás, ami már valódi megoldást jelenthet. Csökkentett módban nem indulnak el az egyébként automatikusan induló (csoda)programok, így már törölhetőek a fölösleges fájlok, és véglegesen törölhető a registrybejegyzés is.
- Az egyik számítógéphez új monitort csatlakoztatunk. A gép látszólag elindul, de aztán már csak nem látszólag működik, mivel a bejelentkező ablak helyén csak egy fekete képernyő fogad minket. Ebben az esetben az a helyzet, hogy az új monitor nem képes a régi monitor számára beállított 1746x1398 képpontos felbontás (esetleg a 168 Hz képfrissítési frekvencia) megjelenítésére. Csökkentett, vagy VGA-módban történő indítás esetén a grafikus felület olyan felbontással indul, amelyet minden monitor biztosan meg tud jeleníteni, így már be tudunk jelentkezni, és tetszés szerint átállíthatjuk a képernyő paramétereit.

Helyreállítási konzol

A Helyreállítási konzol *(Recovery Console)* használatára akkor van szükség, ha semmilyen más módon nem tudjuk elindítani a gépre telepített operációs rendszert (csökkentett módban sem). A Helyreállítási konzol teljesen önállóan indítható, használatához nincsen feltétlenül szükség a merevlemezen tárolt információkra.

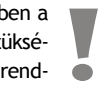
A Helyreállítási konzolnak nincsen grafikus felülete, ez tulajdonképpen egy korlátozott parancskészlettel rendelkező önálló mini operációs rendszer, amelynek használatával hozzáférhetünk a merevlemezeken tárolt adatokhoz, pótolhatunk, kicserélhetünk, vagy lementhetünk fájlokat (NTFS fájlrendszer esetén is). Lehetőségünk van diagnosztikai eszközök futtatására (például *chkdsk* a fájlrendszer ellenőrzéséhez és javításához), és bizonyos mértékig hozzáférhetünk a registryhez is: engedélyezhetjük, illetve letilthatjuk az egyes eszközmeghajtók és rendszerszolgáltatások indítását. További fontos lehetőség a fő rendszertöltő rekord (MBR) és a bootszektor javítása (újraírása) is.

A Helyreállítási konzolt telepíthetjük a gép merevlemezére (de a telepített változat a rendszerindítás korai fázisának hibája esetén nem érhető el), illetve elindíthatjuk közvetlenül az operációs rendszer telepítőlemezéről is. A konzol lefelé kompatibilis, vagyis például a Windows Server 2003 telepítőlemeze használható a Windows 2000, XP stb. rendszerek javításához is.

A Recovery Console telepítése a merevlemezre
Ebben a screencastban feltelepítjük a kiszolgáló merevlemezére a Recovery Console-t.
Fájlnév: *Fájlnév*: *II-3-1b-RC-telepites.avi*

A konzol indítása

A Helyreállítási konzol indításához a számítógépet a Windows telepítő CD-ről kell elindítanunk (mintha csak az operációs rendszert telepítenénk). A merevlemezek eléréséhez esetleg szükséges SCSI- vagy RAID-vezérlőket az F6 billentyű megnyomása után floppyról adagolhatjuk be (éppen úgy, mint telepítés közben).



Lehetőség van arra is, hogy a Helyreállítási konzolt a merevlemezre telepítsük. Ebben az esetben a konzol indításához már nincs szükség a telepítő CD-re, mivel a telepítés során a futtatáshoz szükséges minden fájl a rendszerkötet gyökerében létrejövő *cmdcons* nevű rejtett mappába kerül, a rendszerindításkor megjelenő menübe pedig *(boot.ini)* bekerül a *Windows Server 2003 Recovery Console* sor. A telepítéshez azonban szükség van a Windows CD-re, a következő parancsot kell kiadnunk: *x:\i386\winnt32/cmdcons*, ahol *x* a telepítőlemezt tartalmazó CD-meghajtó betűjele.

6.1. ábra: *Telepítés helyett válasszuk a Recovery Console indítását*

Az eszközmeghajtók betöltése után a telepítés helyett válasszuk a rendszer javítását, majd a telepített operációs rendszerek listája alapján (a szám beírásával) ki kell választanunk azt a Windows példányt, amelyikbe be szeretnénk jelentkezni, és meg kell adnunk a helyi Administrator *(Rendszergazda)* fiókhoz tartozó jelszót (ha a fiók nevét megváltoztattuk, akkor sincs szükség felhasználónévre, mivel azt a biztonsági azonosító (SID) helyettesíti).

```
Microsoft Windows(R) Recovery Console.
The Recovery Console provides system repair and recovery functionality.
Type EXIT to quit the Recovery Console and restart the computer.

1: C:\WINDOWS

Which Windows installation would you like to log onto
(To cancel, press ENTER)? 1
```

6.2. ábra: *A Recovery Console egyetlen lehetőség esetén is kérdez…*

Tartományvezérlő esetén a DSRM-mód jelszavát kell begépelnünk, amelyet a tartományvezérlővé való előléptetéskor állítottunk be. (Ez a jelszó utólag az *ntdsutil* program használatával módosítható, de természetesen csak a működő rendszerben, a helyreállítási konzolban nem.) A jelszó megadásával háromszor próbálkozhatunk, ha a harmadik tipp is helytelen, a számítógépet már csak újraindítani lehet. Ha a helyreállítási konzol nem talált a lemezen telepített Windows-rendszert, akkor természetesen nincs hova bejelentkezni, és a parancssor minden további nélkül megjelenik.

Ha sikerült megadnunk a megfelelő jelszót, akkor a kiválasztott példány *%systemroot%* mappájában (például *c:\windows)* találjuk magunkat, és kezdődhet a küzdelem.

A Helyreállítási konzol parancsai

A Recovery Console indítása és használata
Ebben a screencastban elindítjuk, illetve megmutatjuk a Recovery Console számos lehetőségei közül a legérdekesebbeket, illetve a leghasznosabbakat.
Fájlnév: Fájlnév: II-3-1c-RC-hasznalat.avi

A következőkben áttekintjük a helyreállítási konzol legfontosabb, leggyakrabban használt parancsait, és a parancsok használatával kapcsolatos tudnivalókat.

A konzol indítása után kilistázhatjuk a használható parancsokat a help parancs használatával, illetve egyes parancsokhoz is kérhetünk segítséget, ha begépeljük a help <parancsnév> utasítást.

- **Chkdsk** – a parancs segítségével lemezellenőrzést végezhetünk, és kérhetjük a talált hibák automatikus javítását. Ha az ellenőrzendő lemez nincsen inkonzisztensként megjelölve, akkor a *chkdsk* csak a */p* kapcsoló használata esetén végzi el annak ellenőrzését. Ha megadjuk a */r* kapcsolót is, akkor a *chkdsk* megkísérli a hibás szektorokban található adatok helyreállítását. A *chkdsk* működéséhez szükség van az *autocheck.exe* programra, ha nem sikerül automatikusan megtalálnia (a merevlemezen vagy a telepítő CD-n), akkor a *chkdsk* rákérdez annak helyére.
- **Fixmbr** – a parancs újraírja a fő rendszertöltő rekord (MBR) első 446 bájtját, vagyis az MBR-ben található programkódot, de (általában) érintetlenül hagyja a partíciós táblát.

Más a helyzet azonban hibás partíciós tábla (például két aktívként megjelölt partíció) vagy az MBR-t lezáró 0x55AA érték hiánya esetén. Ekkor a *fixmbr* teljesen, és visszavonhatatlanul letörli a partíciós táblánkat. Nem szabad tehát a *fixmbr* parancsot használni, ha az *Operating system not found* vagy az *Invalid partition table* hibaüzenetet látjuk (legalábbis, ha még szükségünk van a lemez partíciós táblájára). Ilyen esetben sajnos az automatizált megoldásokban már nem bízhatunk, vagyis csak a nehéz út járható: a merevlemezt átszereljük egy működő gépbe, és a Resource Kit-ben található *DskProbe.exe* nevű program segítségével manuálisan kijavítjuk a partíciós tábla hibáját (csak erős idegzetűeknek!). Ugyancsak fölösleges a *fixmbr*-rel próbálkozni, ha egyáltalán nincs aktívként megjelölt partíciónk, mivel ekkor a partíciós tábla megmarad ugyan, de aktív partíció továbbra sem lesz benne.

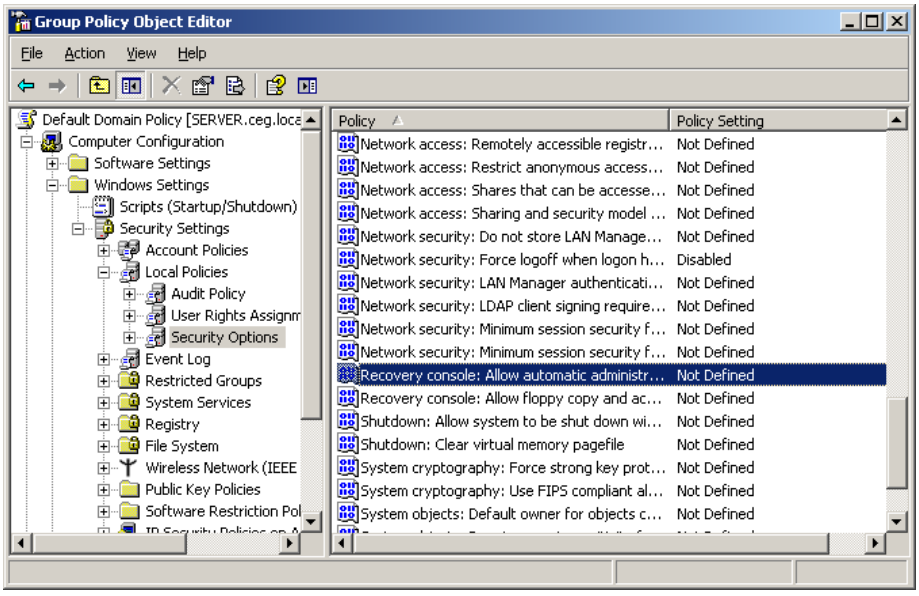
- **Fixboot** – a rendszerpartícióra új bootszektort ír. Ez a művelet nem jár különösebb kockázattal, rontani biztosan nem ront a helyzetünkön.
- **Diskpart** – egyszerű, karakteres felületű partícionálóprogram, megegyezik azzal (csak a színösszeállítás más egy kicsit), amivel a Windows-telepítés elején találkozhatunk. Elsődleges és kiterjesztett partíciók, illetve logikai kötetek létrehozását és törlését végezhetjük el segítségével, illetve meg is formázhatjuk a létrehozott meghajtókat.
- **Map** – a parancs megjeleníti a meghajtó betűjelek és a fizikai eszköznevek összerendeléseit. Erre az információra például a *fixboot* és a *fixmbr* futtatásakor lehet szükség, mivel ekkor a fizikai eszközneveket (például *\Device\HardDisk0\Partition1)* kell megadnunk paraméterként. Az *arc* paraméter használatával a parancs ARC (Advanced RISC Computing) formátumban írja ki az eszközneveket (például *multi(0)disk(0)rdisk(0)partition(1)),* ezeket az értékeket a *boot.ini* szerkesztésekor használhatjuk fel.

- **Set** – a parancs segítségével megjeleníthetjük és beállíthatjuk a konzol környezeti változóit. Mindössze négy környezeti változónk van (értékük *true* vagy *false* lehet), amelyekkel tiltható, illetve engedélyezhető különféle műveletek végrehajtása. Alapértelmezés szerint mind a négy változó értéke *false*, vagyis a hozzájuk tartozó műveletek tiltottak. Sőt alapértelmezés szerint csak akkor állíthatjuk át a változók értékét, ha ezt a számítógép helyi házirendjében (vagy a csoportházirendben) már korábban engedélyeztük (lásd később). A négy változó a következő:
    - **AllowAllPaths** – a változó segítségével engedélyezhetjük a merevlemezeken található valamennyi kötet és mappa elérését. (Alapértelmezés szerint csak a Windows-mappa és a gyökér érhető el.)
    - **AllowRemovableMedia** – engedélyezhetjük az adatok cserélhető meghajtóra való kimásolását. (Alapértelmezés szerint csak befelé másolhatunk.)
    - **AllowWildCards** – engedélyezhetjük a helyettesítő karakterek használatát a fájl és mappakezelő parancsokban (például *copy *.*).*
    - **NoCopyPrompt** – *true* érték esetén a konzol nem kér megerősítést a meglévő fájlok felülírása előtt.
- **Batch** – a parancs paramétereként tetszőleges nevű, a Helyreállítási konzol utasításait tartalmazó szövegfájl nevét adhatjuk meg. A fájlban szereplő utasításokat a konzol úgy hajtja végre, mintha egyesével gépeltük volna be azokat. Második paraméterként megadhatjuk a parancsok kimenetét fogadó fájl nevét is, de ha nem adunk meg nevet, akkor a kimenet a szokásos módon a konzolra kerül.
- **Bootcfg** – a parancs segítségével módosíthatjuk a *boot.ini* tartalmát, megkereshetjük például a lemezre telepített Windows-példányokat és hozzáadhatjuk a megfelelő bejegyzéseket a *boot.ini*-hez.
- **Listsvc** – a parancs megjeleníti a számítógépen elérhető valamennyi eszközillesztő és szolgáltatás listáját.
- **Enable** – a parancsot a paraméterként megadott eszközillesztő vagy szolgáltatás engedélyezésére használhatjuk. Második paraméterként megadható az engedélyezet szolgáltatás indítási típusa is. Az indítási típus a következő értékek valamelyike lehet:
    - SERVICE_BOOT_START
    - SERVICE_SYSTEM_START
    - SERVICE_AUTO_START
    - SERVICE_DEMAND_START

- **Disable** – a parancs letiltja a paraméterként megadott szolgáltatás, vagy eszközillesztő indítását.
- **Logon** – a parancs segítségével átjelentkezhetünk a lemezre telepített másik operációs rendszerbe.
- Használhatók a fájl és mappaműveletekkel kapcsolatos szokásos parancssori utasítások *(cd, dir, copy, delete, md, rd, rename, type)*. Ha a Windows telepítőlemezről másolunk fájlokat a merevlemezre, akkor nincs szükség külön kitömörítésre *(expand)*, a *copy* parancs ezt elintézi helyettünk.
- **Exit** – kilépés a konzolból és a számítógép újraindítása.

Biztonsági beállítások

A Helyreállítási konzol két biztonsági beállítását még a számítógép működőképes állapotában a helyi-, illetve a csoportházirendben kell megadnunk. Tartományhoz nem tartozó számítógépek esetén csak a helyi házirend áll rendelkezésre. A két beállítást ebben az esetben a *gpedit.msc* (vagy a *secpol.msc)* konzolban adhatjuk meg (Security Settings -> Security Options). Természetesen a fenti módszer tartományi számítógépek esetén is működik, de ekkor a csoportházirend esetleges beállításai felülírhatják a helyi házirendet. Tartományi számítógépek esetén célszerű a fenti beállításokat központilag, a csoportházirendben szabályozni.



6.3. ábra: *Recovery Console opciók a csoportházirendben*

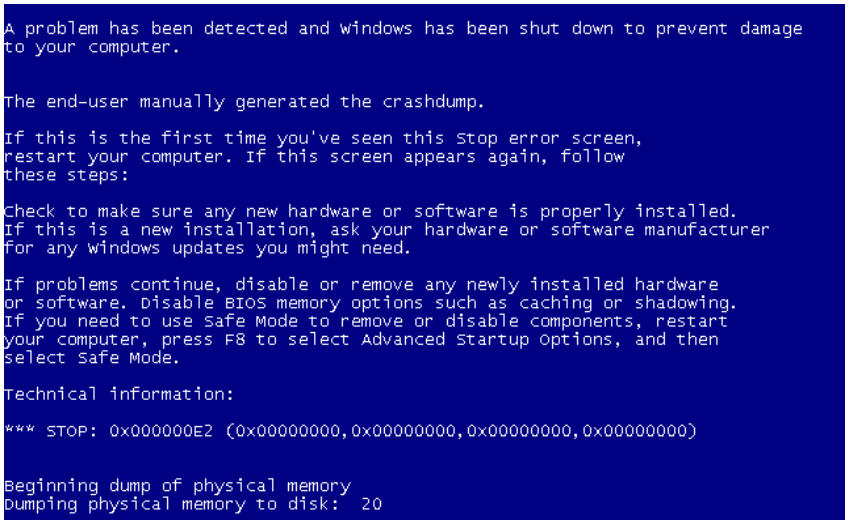
A két opció jelentése a következő:

- **Allow floppy copy and access to all drives and folders** *(Hajlékonylemez másolása és hozzáférés minden meghajtóhoz és mappához)* – ha engedélyezzük ezt az értéket, akkor a korábban említett *set* parancs használatával átállíthatjuk a konzol négy környezeti változóját.
- **Allow automatic administrative logon** *(Automatikus rendszergazdai bejelentkezés)* – ha engedélyezzük az értéket, akkor a konzol indításakor nem kell megadnunk a rendszergazda jelszavát, a bejelentkezés automatikusan megtörténik.

A „kék halál”

Ha a Windows indítása vagy futása során kezelhetetlen hibába ütközik, az adatok megóvásának érdekében leáll, és megjeleníti a hírhedt kék képernyőt (a jelenség neve Blue Screen of Death, vagyis a halál kék képernyője). A kék halál tehát egy megoldhatatlan szituációnak a lehetőségekhez képest korrekt lezárását jelenti.

A kék képernyős rendszerleállásokat az esetek nagyon jelentős részében nem maga az operációs rendszer, hanem valamelyik kernel módban futó eszközmeghajtó, illetve a hardver hibája okozza. A hiba okától függetlenül az információs képernyő megjelenítését, és a rendszer leállítását a *KeBugCheckEx* nevű rendszerfüggvény hajtja végre.

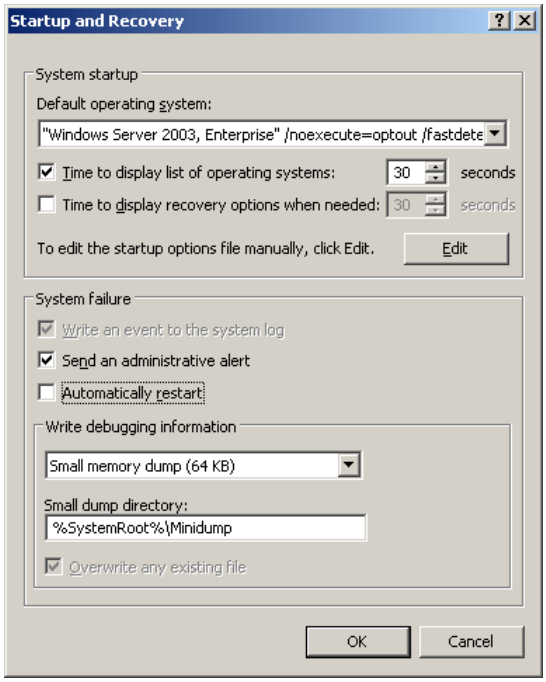


6.4. ábra: *Ha valaki még nem látott volna ilyet…*

A kék képernyő a következő esetekben jelenhet meg:

- Egy eszközmeghajtó, vagy kernel módban futó operációs rendszer függvény kezelhetetlen kivételt generál (például írni próbál a memória írásvédett területére)
- Egy eszközmeghajtó vagy operációs rendszer függvény kifejezetten meghívja a *KeBugCheckEx* függvényt, mert olyan körülményeket észlelt, amelyek lehetetlenné teszik a rendszer további működését.
- Hardver hiba, vagyis nem maszkolható megszakítás *(Non maskable Interrupt, NMI)* esetén.

Természetesen az is megoldható lenne, hogy az operációs rendszer egyszerűen nem vesz tudomást a fenti jelenségekről, és fut tovább, mintha mi sem történt volna, de ebben az esetben később valószínűleg még rosszabb körülmények között kényszerülne leállni a rendszer. A „kék halál" tehát nem feltétlen kényszer, hanem a későbbi súlyosabb problémák megelőzésére szolgáló óvintézkedés, ha nem lenne, ki kellene találni ☺.



6.5. ábra: *Beállíthatjuk, hogy mi történjen rendszerhiba esetén*

A megjelenő információk igen fontosak lehetnek a hiba okának megtalálásához, szerepel köztük egy hibakód, és annak emberi nyelvű megfelelője is (például *IRQ_NOT_LESS_OR_EQUAL).* Bár száznál is több különböző hibakód létezik, a legtöbb közülük csak nagyon ritkán fordul elő. Ha nem vagyunk biztosak a hiba okában és a lehetséges megoldásban, akkor a hibakód alapján további információkat találhatunk a Microsoft Tudásbázisban (http://support. microsoft.com).

Ha a képernyőre kiírt információk alapján nem sikerül azonosítani a hibát, akkor hasznos lehet a rendszerleállás közben fájlba mentett memóriatartalom *(crash dump)* tanulmányozása. Erre a célra számos különféle többékevésbé automatizált analizáló eszköz létezik.

A rendszerhibák kezelésének beállításai
Ebben a screencastban áttekintjük a Startup and Recovery lap beállítási lehetőségeit.
Fájlnév: II-3-1d-Startup-and-Recovery.avi

A rendszerhibák kezelésének különféle paramétereit a Control Panel -> System -> Advanced -> Startup and Recovery lapon (6.6.5. ábra) adhatjuk meg. Talán a legfontosabb beállítás az automatikus újraindítás engedélyezése, illetve tiltása. Alapértelmezés szerint a számítógép újraindul a leállások után, ami nagyon jól jöhet például egy csendes hétvégén, mivel ha a kiszolgáló egyáltalán képes az újraindulásra, akkor a rendszergazda jó esetben hétfőn csak az eseménynaplóból értesül a történtekről. Ha azonban szeretnénk látni a hibaüzenetet, akkor feltétlenül ki kell kapcsolnunk az automatikus újraindítást. Ha ezt elmulasztjuk, akkor – ahogyan már korábban említettük –, az indítómenü használatával utólag is megváltoztatható ezt a beállítás *(Disable automatic restart on system failure).*

A „kék halál" mesterségesen is előidézhető több módon is. Leállíthatunk például olyan szolgáltatásokat, amelyek nélkül a rendszer működésképtelen, illetve használható a „hivatalos", valószínűleg tesztelés céljára szolgáló módszer is. Létre kell hoznunk a *CrashOnCtrlScroll DWord* értéket (1) a *HKLM\System\CurrentControlSet\i8042prt\Parameters* kulcs alatt. Újraindítás után a jobb oldali *Ctrl* nyomva tartása mellett üssük le kétszer a *Scroll Lock* billentyűt…

Grafikus ellenőrző-javító eszközök

Ha sikerült elindítanunk az operációs rendszert (akár csökkentett módban is), akkor a különféle hibák felderítéséhez és elhárításához számos beépített, grafikus felülettel rendelkező eszköz áll rendelkezésünkre, a következőkben ezek közül ismerkedünk meg a legfontosabbakkal.

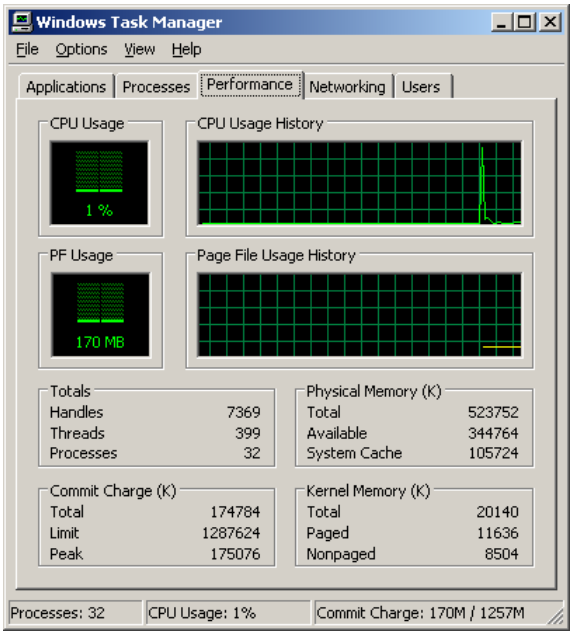
A grafikus felülettel rendelkező ellenőrző- javító eszközök használata
Ebben a screencastban kipróbáljuk a Windows rendszerek beépített ellenőrző és hibajavító eszközei küzöl a legsűrűbben használtakat.
Fájlnév: II-3-2a-GUI-eszkozok.avi

Feladatkezelő *(Task Manager)*

A Windows-rendszerek talán legtöbbet használt ellenőrző eszköze a Feladatkezelő *(Taskmgr.exe)*. Segítségével gyors, de viszonylag átfogó pillanatképet kaphatunk a rendszerben futó alkalmazásokról és folyamatokról, ellenőrizhetjük a számítógép legfontosabb terhelési adatait és megjeleníthetjük a bejelentkezett felhasználókat. Ismerkedjünk meg a Feladatkezelő egyes lapjairól leolvasható adatokkal, illetve az ott elvégezhető műveletekkel:

- **Applications** *(Alkalmazások)* – a lap elnevezése talán kissé félrevezető lehet, mivel a lapon nem a rendszerben futó alkalmazásokat, hanem az adott felhasználó munkaasztalán lévő, látható állapotú ablakok címsorait találhatjuk meg. Egy alkalmazáshoz több megnyitott ablak is tartozhat (tipikusan ilyen például a Windows Explorer), illetve számos olyan alkalmazás is futhat a gépünkön, amelyikhez egyáltalán nem tartozik látható ablak – ezek nem fognak megjelenni az Alkalmazások lapon sem. Szintén nem egészen egyértelműek az egyes ablakok állapotaként megjelenített értékek. Ha az ablak állapota *Fut (Running)*, az azt jelenti, hogy az ablak üzenetkezelő ciklusa (ez fogadja a leütött billentyűket, egérműveleteket, más folyamatoktól érkező üzeneteket stb.) késlekedés nélkül válaszol a kérésekre, vagyis az ablak mögött található alkalmazás üzenetre (bevitelre) vár, tehát nem csinál semmit. Ha az ablak állapota *Not responding (Nem válaszol)*, az jelentheti persze azt is, hogy az ablak mögött álló alkalmazás leállt (lefagyott), de az is lehetséges, hogy csak egyéb sürgős elfoglaltságai miatt éppen nem jut ideje az üzenetkezelő ciklusra. Az egyes „alkalmazásokhoz" (például a jobb gombos helyi menüből) a szokásos ablakkezelő parancsok kiadására van lehetőség [Bring to Front *(Előtérbe hozás)*, Minimize *(Kis méret)*, Maximize *(Teljes méret)* stb.]. Az End Task *(Feladat befejezése)* menüpont szintén nem az alkalmazásra, hanem az ablakra vonatkozik, a kérést első körben az üzenetkezelő ciklusnak kell(ene) fogadnia (ha ez nem sikerül, akkor komolyabb eszközökkel is próbálkozik a Feladatkezelő). Nagyon fontos a Go To Process (*Ugrás folyamatra)* menüpont, ezzel a Feladatkezelő következő lapjára kerülünk, és kijelölhetjük azt a rendszerfolyamatot, amelyikhez az adott ablak tartozik.

- **Processes** *(Folyamatok)* – ezen a lapon már a számítógépen futó összes folyamat látható, megtalálhatjuk köztük az előző oldalon felsorolt alkalmazásokhoz, a többi alkalmazáshoz és az összes rendszerszolgáltatáshoz tartozó folyamatot is. Alapértelmezés szerint itt láthatjuk a folyamathoz tartozó végrehajtható állomány nevét, a futtató felhasználót, valamint itt követhetjük nyomon a pillanatnyi memória- és processzoridő felhasználást. Itt kereshetjük meg például azt a rendszerfolyamatot, amelyik valami miatt túl sok erőforrást használ, és lelassítja a rendszert. Számos más adatot is megjeleníthetünk, ha a View *(Nézet)* menü Select Columns *(Oszlopok kiválasztása)* pontjára kattintunk. Fontos információ lehet például a folyamat azonosítója *(Process Identifier, PID)*, ezt a hibakeresés során, több helyen is felhasználhatjuk majd. A jobb gombos helyi menüben beállíthatjuk az egyes folyamatok prioritását (de csak óvatosan, mert ha egy processzt nagyon „kiemelünk" pl. a Realtime lehetőséget választva, akkor minden más folyamat iszonyúan lelassulhat), és itt közvetlenül is leállíthatjuk a nem válaszoló alkalmazásokhoz tartozó folyamatokat.
- **Performance** *(Teljesítmény)* – a Teljesítmény lapon a számítógép teljesítményével, vagyis a processzor(ok) és a memória kihasználtságával kapcsolatos információk jelennek meg. A memória kihasználtságával kapcsolatos adatok között is találhatunk néhány félreérthető nevű mezőt, így tekintsük át egyenként az adatok tartalmát.



6.6. ábra: *Az operációs rendszer legfontosabb teljesítményadatai a Feladatkezelőben*

- A **CPU Usage** *(CPU-használat)* mezővel semmi probléma nincs, százalékos érték formájában megjeleníti a processzor pillanatnyi terheltségét.
- A **PF Usage** *(Lapozófájl)* érték (és a hozzá tartozó grafikon) viszont nem a lapozófájl használatát mutatja, hanem a rendszer által lefoglalt összes memóriaterület (a fizikai memóriában és a lapozófájlban együttesen) nagyságát.
- A **Totals** *(Összesítés)* szakaszban a rendszerben futó folyamatok, programszálak és a leírók (a programok által használt erőforrások, például fájlok, registrykulcsok stb.) számát találhatjuk.
- A **Commit Charge** *(Lefoglalt memória)* szakasz három értékének jelentése a következő: a Total *(Összes)* érték a rendszer által a fizikai memóriában és a lapozófájlban lefoglalt összes memóriát jelenti (megegyezik az PF Usage kijelzőn látható értékkel). A Limit *(Korlát)* a fizikai memória és valamennyi lapozófájl összesített mérete, maximálisan ennyi memóriát foglalhatnak a folyamatok. A Peak *(Csúcsérték)* a számítógép bekapcsolása óta lefoglalt legtöbb memóriát jelenti.
- A **Physical Memory** *(Fizikai memória)* szakaszban a számítógépben lévő fizikai memória (RAM) méretét láthatjuk. Az Available *(Rendelkezésre álló)* érték a szabad memória mennyiségét jelenti, a System Cache *(Rendszergyorsítótár)* mezőről pedig a megnyitott fájlok leképezéséhez igénybe vett fizikai memória mennyiségét olvashatjuk le.
- A **Kernel Memory** *(Kernelmemória)* szakaszban az operációs rendszer magja és az eszközillesztők által használt memóriára vonatkozó adatokat találhatjuk meg. A Paged *(Lapozható)* érték a kernel által használt memória kilapozható részét jelenti, a Nonpaged *(Nem lapozható)* mező pedig az a rész, amelynek mindenképpen a fizikai memóriában kell maradnia.

- **Networking** *(Hálózat)* – ezen a lapon a számítógép engedélyezett hálózati csatolóira vonatkozó adatokat tekinthetünk meg. A grafikonok a pillanatnyi terhelés alakulását mutatják, alul pedig az alapértelmezett készleten kívül még számos további adatot is megjeleníthetünk (View menü Select Columns pontja).
- **Users** *(Felhasználók)* – a lapon láthatók a számítógépre bejelentkezett felhasználók, az egyes munkamenetek állapota és neve. A bejelentkezet felhasználóknak küldhetünk üzenetet, és szükség esetén meg is szakíthatjuk a kiválasztott munkamenetet.

Computer Management MMC

Az első fejezetben már megismerkedtünk a Vista legfontosabb MMC-alapú felügyeleti eszközeivel, és az ezzel kapcsolatos újdonságokkal, most csak azokra az elemekre fogunk koncentrálni, amelyek a Windows kiszolgálókon is megtalálhatók, és a hibakeresésben is jól felhasználhatók.

A rendszerszolgáltatások

A rendszerszolgáltatás olyan program, vagy folyamat, amely a rendszer egy meghatározott, más programok támogatására szolgáló funkcióját valósítja meg, általában alacsony, hardver közeli szinten. Minden szolgáltatás egy meghatározott felhasználói fiók használatával bejelentkezve éri el az operációs rendszer erőforrásait és objektumait. Windows Server 2003 esetén a szolgáltatások nagy többsége alapértelmezés szerint a Helyi rendszer *(Local System)* fiók használatával jelentkezik be, ami gyakorlatilag korlátlan hozzáférést biztosít a teljes rendszerhez.

A SYSTEM fiók sok esetben még az Administrators csoport tagjainál is kiterjedtebb jogokkal rendelkezik, a rendszerleíró adatbázis néhány területéhez például csak a SYSTEM fióknak van jogosultsága, az *administrator* még csak be sem nézhet oda. Bár a SYSTEM fiókkal természetesen nem lehet közvetlenül bejelentkezni, egy egyszerű trükk segítségével mégis elindíthatunk a SYSTEM nevében futó programokat; ha egy tetszőleges programot a SYSTEM fiókkal bejelentkező Feladatütemező szolgáltatás indít el, az természetesen szintén a SYSTEM fiók nevében fog futni. Ha tehát például kiadjuk a következő parancsot: *C:\>at 21:00:00 /interactive cmd*, akkor (majd este kilenckor) kapunk egy SYSTEM jogokkal futó parancssort, ahonnan már bármilyen más programot is ugyanilyen jogosultsági szinttel indíthatunk el.

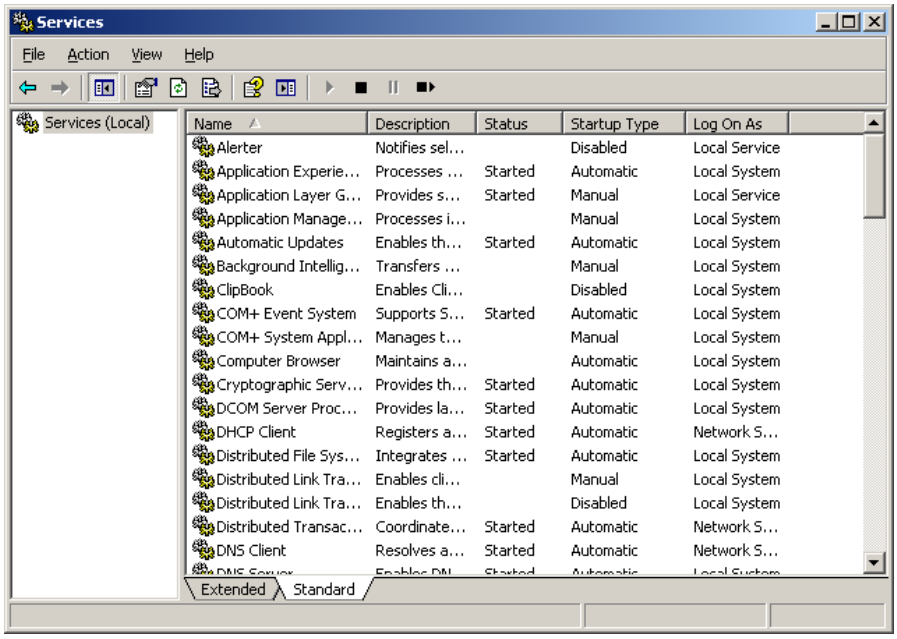
Ha a SYSTEM fiókkal bejelentkező szolgáltatás tartományvezérlőn fut, akkor nemcsak magához a számítógéphez, hanem a teljes tartományhoz is korlátlan hozzáféréssel rendelkezik.

Más, korlátozott jogosultsági szinttel is megelégedő szolgáltatások a Network Service *(Hálózati szolgáltatás),* vagy a Local Service *(Helyi szolgáltatás)* fiók használatával jelentkezhetnek be, amelyek jelentősen kevesebb jogosultsággal (és veszéllyel) járnak. Az előbbi esetben (Network Service) a szolgáltatás csak a hálózaton, míg a Local Service használata esetén csak a helyi gépen kap jogosultságokat. A szolgáltatások hozzáférési szintjének korlátozása a rendszer védelmét szolgálja az adott szolgáltatás hibás működése, vagy egy ellene irányuló külső támadás esetén. Ahogyan már korábban is említettük, a Vista operációs rendszerben drasztikusan csökkent a SYSTEM fiók nevében futó szolgáltatások száma, éppen a biztonsággal kapcsolatos megfontolások következtében.

A szolgáltatások három különböző indítási típusba tartozhatnak. Az automatikus indításúak a rendszer indításával együtt elindulnak és többségük folyamatosan aktív marad a teljes rendszer, vagy az adott szolgáltatás leállításáig. A kézi indítású szolgáltatásokat szükség esetén a felhasználó, illetve különféle programok vagy más szolgáltatások indíthatják el, a tiltott szolgáltatások pedig sem automatikusan, sem manuálisan nem indíthatók el.

A Services *(Szolgáltatások)* MMC-modul segítségével (meglepetés!) a rendszerben futó szolgáltatások állapotáról kaphatunk információt, illetve beállíthatjuk a futtatásukkal kapcsolatos különféle paramétereket. Amint a 6.7. ábrán látható, a listában megtalálhatjuk a szolgáltatások nevét, rövid leírását, aktuális állapotát, indítási típusát és azt a felhasználónevet, amelynek használatával a szolgáltatás bejelentkezik a rendszerbe.

A szolgáltatásokkal kapcsolatos hibák gyors felmérése jól felhasználható, ha a sorokat az indítási típus szerinti sorrendbe rendezzük. Ekkor az automatikus típus kerül a lista elejére, így könnyen észrevehetjük, ha egy ilyen szolgáltatás valami miatt nem indult el. (Néhány automatikusan induló szolgáltatásnak nem kell folyamatosan futnia, de ezekből meglehetősen kevés van.)



6.7. ábra: *A Szolgáltatások kezelésére szolgáló MMC-modul*

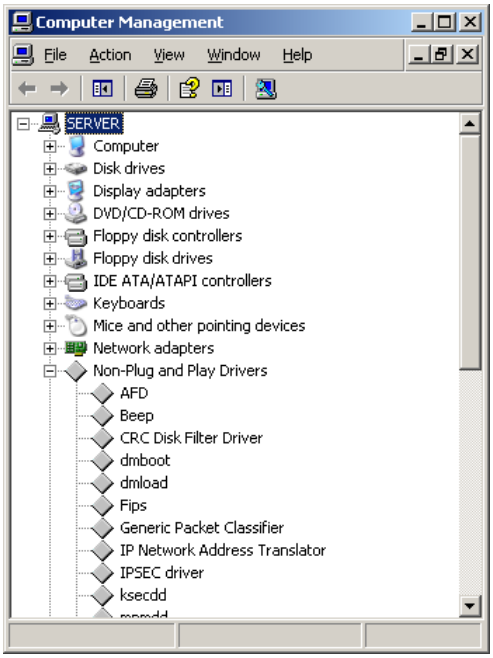
A további adatokat megjelenítő, illetve bizonyos paraméterek beállítását is lehetővé tévő párbeszédablak megjelenítéséhez duplán kell kattintanunk az adott szolgáltatást reprezentáló sorra. A párbeszédablak lapjain megadhatjuk a

szolgáltatás indítási típusát, és a futtató felhasználói fiókot (le is állíthatjuk, illetve elindíthatjuk a szolgáltatást). A Recovery *(Helyreállítás)* lapon megadhatjuk, hogy mi történjen, ha a szolgáltatás leáll az első, második, illetve harmadik alkalommal. Újraindítható az adott szolgáltatás, maga a számítógép, illetve lefuttathatunk egy tetszőleges programot is. Ezek a lehetőségek számos esetben nagyon hasznosak lehetnek, hiszen egy szolgáltatás leállása komoly problémát okozhat, de ezt a szolgáltatás, vagy a számítógép újraindítása a legtöbb esetben megoldja (hacsak nincs nagyobb baj), az elindított program pedig értesítheti például a rendszergazdát, vagy a felhasználókat.

A hibakeresés szempontjából talán a Dependencies *(Függőségek)* lap tartalma lehet a legfontosabb. Innen azt olvashatjuk le, hogy az adott szolgáltatás mely más szolgáltatásoktól függ (vagyis minek kell futnia, hogy ő elindulhasson), és mely szolgáltatások függenek tőle (vagyis mi minden fog leállni az adott szolgáltatással együtt).

Az Eszközkezelő

Az Eszközkezelő *(Device Manager)* a számítógépre telepített hardvereszközök grafikus nézetét biztosítja; segítségével frissíthetjük a hardvereszközök illesztőprogramjait, módosíthatjuk a hardverelemekkel kapcsolatos különféle beállításokat, és felderíthetjük, illetve elháríthatjuk a hibákat.



6.8. ábra: *Az Eszközkezelő a rejtett (nem Plug and Play) eszközök megjelenítésére és eltávolítására is képes*

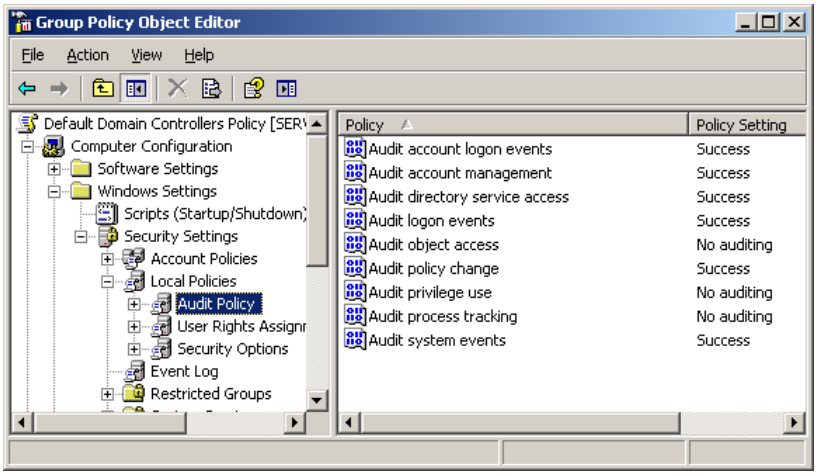
Az Eszközkezelő segítségével gyors, áttekintő képet kaphatunk a számítógép hardvereszközeiről, ellenőrizhetjük azok megfelelő működését, illetve módosíthatjuk a hardverelemek erőforrásokkal (megszakítás, I/O tartomány stb.) kapcsolatos beállításait.

Ugyancsak az Eszközkezelő ad lehetőséget a hardvereszközök illesztőprogramjainak frissítésére, illetve a korábban már megtárgyalt Árnyékmásolat szolgáltatás segítségével rosszul sikerült frissítés esetén vissza is térhetünk az előző verzióra (Driver Rollback).

Fontos lehetőség, hogy az eszközkezelő a nem Plug and Play hardvereszközök megjelenítésére (és eltávolítására) is lehetőséget ad. Az ilyen eszközök esetében ugyanis nemcsak a telepítés, hanem az eltávolítás sem mindig automatikus, ha az eltávolítást végző program nem fut le tökéletesen, akkor az illesztőprogram a hardvereszköz fizikai eltávolítása után is aktív maradhat, foglalhatja a rendszer erőforrásait, és esetleg más problémákat is okozhat. A rejtett eszközök megjelenítéséhez kapcsoljuk be a View → Show hidden devices *(Nézet → Rejtett eszközök megjelenítése)* opciót.

Az Eseménynapló

Az Eseménynapló szolgáltatás által készített naplók segítségével nyomon követhetjük a számítógép egyes komponenseinek működését, és gyorsan értesülhetünk a különféle problémákról. Természetesen lehetőségünk van az események különféle tulajdonságai (típus, forrás, dátum stb.) szerinti szűrésre és keresésre is. A Windows Server 2003 családba tartozó operációs rendszerek alapértelmezés szerint háromféle naplóban rögzítik az eseményeket:



6.9. ábra: *A tartományvezérlők naplórendje*

- Az **alkalmazásnapló** *(Application log)* a különféle alkalmazások által naplózott eseményeket tartalmazza. Ide jegyzi be a futása közben történt eseményeket valamennyi Microsoft program, de számos más forrásból származó alkalmazás üzeneteit is megtalálhatjuk itt. Az alkalmazásnaplóba kerülő üzenetek tartalma és mennyisége teljes mértékben az egyes alkalmazások fejlesztőinek hatáskörébe tartozik, bármelyik program felkészíthető az Eseménynapló használatára.
- A **biztonsági napló** *(Security log)* az érvényes és érvénytelen bejelentkezési kísérleteket, valamint a különféle erőforrások (például fájlok) létrehozását, megnyitását vagy törlését tartalmazza. A biztonsági naplóba kerülő események körét a csoportházirend, (illetve a helyi házirend) beállításai határozzák meg.
- A **rendszernapló** *(System log)* a Windows rendszerösszetevői által naplózott eseményeket tartalmazza. Ide kerülnek a különféle illesztőprogramokkal és más rendszerösszetevőkkel kapcsolatos események, például a sikertelen betöltés, leállás stb.

A tartományvezérlőkön a fentieken kívül még legalább két másik naplót is találhatunk:

- A **címtár-szolgáltatási napló** *(Directory Service log)* az Active Directory-szolgáltatás által naplózott eseményeket tartalmazza, ide kerülnek például a címtáradatbázis replikációjával kapcsolatos különféle bejegyzések.
- A **Fájlreplikációs szolgáltatás naplója** *(File Replication Service log)* a Fájlreplikációs szolgáltatása által naplózott eseményeket tartalmazza. A rendszer ebben a naplóban rögzíti például a tartományvezérlők SYSVOL-mappáinak szinkronizálásakor bekövetkező hibákat.
- Ha a tartományvezérlő egyben DNS-kiszolgáló is, akkor egy további naplót is találhatunk rajta. A **DNS-kiszolgálónapló** *(DNS Server log)* a DNS-szolgáltatás által naplózott eseményeket tartalmazza.

Az egyes naplók méretére, illetve a maximális méret elérésekor bekövetkező eseményekre vonatkozó beállításokat az egyes naplók tulajdonságlapján, illetve a csoportházirend segítségével határozhatjuk meg. Valamennyi napló esetében lehetőség van a bejegyzések fájlba mentésére, az így elkészült fájlt pedig akár egy másik számítógépen is importálhatjuk.

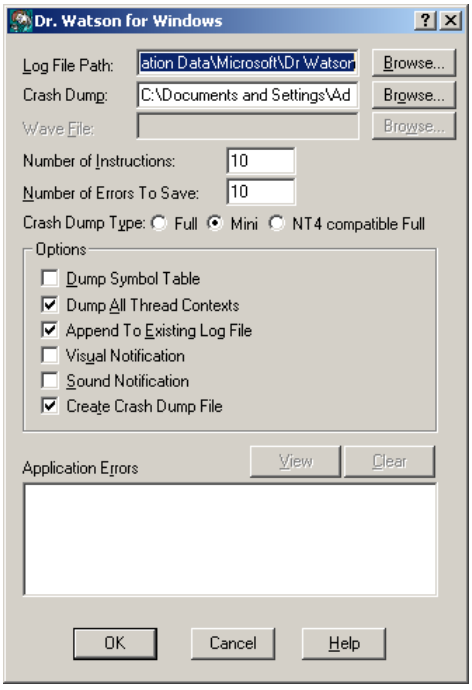
A naplókba kerülő bejegyzések a következő öt típus valamelyikébe tartoznak:

- **Hiba** *(Error)* – Jelentős, már bekövetkezett probléma, például egy szolgáltatás sikertelen indítási kísérlete, vagy leállása, egy alkalmazás „lefagyása" stb.
- **Figyelmezetés** *(Warning)* – Nem feltétlenül jelentős, de a jövőben könnyen súlyosabb problémába torkolló esemény. Figyelmeztetés kerül például a naplóba, ha a rendszerköteten (vagy máshol) lecsökken a szabad lemezterület, ha nem törődünk a figyelmeztetéssel, az a legtöbb hibánál is súlyosabb következményekkel járhat. Nem érdemes tehát csak a hibákra szűrve olvasgatni a naplókat, mert így nem kerülnek a szemünk elé azok a bejegyzések, amelyek előre jelezhetnék a későbbi komolyabb problémákat.
- **Információ** *(Information)* – Egy alkalmazás, illesztőprogram vagy szolgáltatás sikeres működését leíró esemény. Amikor például betöltődik egy hálózati csatoló illesztőprogramja a naplóba Információ típusú bejegyzés kerül.
- **Sikeres események naplózása** *(Success Audit)* – Ilyen típusú bejegyzésekkel a biztonsági naplóban találkozhatunk. Sikeres eseménynek minősül például, ha egy felhasználónak sikerül bejelentkeznie a rendszerbe.
- **Sikertelen események naplózása** *(Failure Audit)* – Szintén csak a biztonsági naplóba kerülhetnek ezek az események, ilyen bejegyzés készül például egy hálózati meghajtóhoz való sikertelen hozzáférési kísérlet esetén.

Az Eseménynaplóba kerülő hibák (és sok esetben a figyelmeztetések is) mindenképpen törődést érdemelnek, bár gyakran előfordul az is, hogy semmi különös teendőnk nincs, mert például egyszerűen a számítógép újraindítása megoldja a problémát. Ebben az esetben sem árt azonban, ha a naplóbejegyzésben található eseményazonosító alapján rákeresünk a hibaüzenetre a Microsoft Tudásbázisban *(http://support.microsoft.com),* ahol gyakorlatilag minden elképzelhető bejegyzéssel kapcsolatban részletes, megbízható forrásból származó információt kapunk (a legtöbb esetben persze angolul, bár van néhány magyarított cikk is). Megtudhatjuk, hogy mi okozhatja a jelenséget, és mi lehet a megoldás (például javítócsomag letöltése és telepítése, beállítások módosítása stb.). Szintén jól használható forrás lehet a *http://eventid.net* webhely, ahová akár mi magunk is feltölthetjük egy adott problémával kapcsolatos kérdésünket, illetve válaszolhatunk mások kérdéseire is. Természetesen sok esetben jól használhatók az általános keresők is.

Dr. Watson

Dr. Watson egy hibakereső/nyomkövető alkalmazás, ami összegyűjti a különféle programhibákkal kapcsolatos tényeket, hogy aztán ezek alapján Sherlock Holmes (a rendszergazda) rendkívül éles elméjével levonhassa a megfelelő következtetéseket.



6.10. ábra: *Dr. Watson megkapja az instrukciókat*

Programhiba, illetve kezeletlen kivétel esetén Dr. Watson automatikusan akcióba lendül, hozzákapcsolódik a hibás alkalmazáshoz vagy szolgáltatáshoz, megvizsgálja a hibát és a DRWTSN32.LOG nevű szöveges naplófájlba írja a vizsgálat eredményét (és bejegyzést készít az Eseménynaplóba is). Dr. Watson segítségével létrehozhatunk a memória tartalmát tároló bináris fájlt is, amely aztán speciális hibakereső alkalmazás segítségével elemezhető.

Dr. Watson beállításainak (például a naplófájl és a memóriakép tárolómappája) megadásához a *drwtsn32.exe* programot kell elindítanunk.

Hálózati gondok megoldása

A következőkben a hálózati hibák felderítésére szolgáló legfontosabb eszközökkel fogunk megismerkedni. Számos kisebb-nagyobb program használható erre a célra, először néhány egyszerű parancssori eszközzel, majd egy komolyabb, egészen mély vizsgálatot és elemzést is lehetővé tevő alkalmazással foglalkozunk.

A hálózat diagnosztikai eszközei
Ebben a mini bemutatóban megmutatjuk a hálózati hibák felderítéséhez használható eszközöket.
Fájlnév: II-3-2b-Halozat-eszkozok.avi

Az ***ipconfig*** parancs segítségével megjeleníthetjük a hálózati csatolókhoz tartozó TCP/IP-paramétereket, frissíthetjük a csatolók a DHCP-beállításait és bejegyeztethetjük a paramétereket a DNS-kiszolgáló adatbázisába. Ha paraméter nélkül adjuk ki az *ipconfig* parancsot, akkor megjeleníthetjük az összes adapter IPv6- vagy IPv4-címét, alhálózati maszkját és alapértelmezett átjáróját. Ha a parancsot az */all* kapcsolóval indítjuk el, akkor igen részletes adatokat kapunk valamennyi csatolóról, így könnyen áttekinthetjük a beállításokat, és gyorsan megtalálhatjuk az esetleg elgépelt, vagy más ok miatt hibás értékeket.

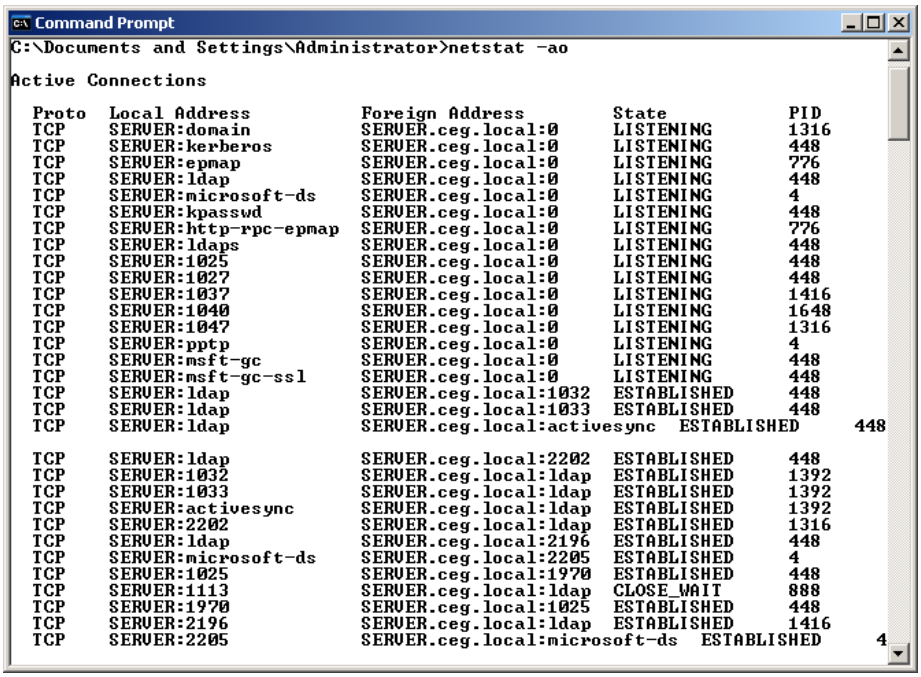
A ***NetStat*** paranccsal protokollstatisztikát és az aktív TCP/IP-kapcsolatokat jeleníthetjük meg. A *-r* kapcsoló használatával kilistázhatjuk a számítógép útválasztási táblázatát, a *-e* kapcsolóval pedig a küldött és fogadott Ethernet keretekre vonatkozó statisztikai adatokat jeleníthetjük meg. A *-s* kapcsoló segítségével protokollonkénti bontásban kapunk statisztikát a számítógép TCP/IP-forgalmáról.

A ***netstat –a*** parancs segítségével az aktív kapcsolatokat listázhatjuk ki, megjelenik használt protokoll, a nyitott port száma, és a kapcsolat állapota. Fontos információt kaphatunk a *netstat –ao* parancs használatával, mivel ekkor az előző lista kiegészül az egyes kapcsolatokat nyitva tartó folyamat azonosítójával (PID) is. A PID-et felhasználva a Feladatkezelő segítségével gyorsan beazonosítható az adott kapcsolatot nyitva tartó rendszerfolyamat.

Az ***Nbtstat*** parancs hasznos eszköz a NetBIOS-alapú név-hozzárendelési problémák hibakeresésében. Az *nbtstat* paranccsal megjeleníthetjük az aktív NetBIOS-munkamenetek listáját, azok állapotát, és a munkamenetekre vonatkozó statisztikai adatokat, illetve kilistázhatjuk vagy megújíthatjuk a gyorsítótárakban és a WINS-kiszolgálón regisztrált névhozzárendeléseket.

Az ***Arp*** parancs segítségével a címfeloldási protokoll *(Address Resolution Protocol, ARP)* által a hálózati forgalom csökkentéséhez használt címfordítási táblázat, vagyis az ARP-gyorsítótár tartalmát jeleníthetjük meg. Az ARP végzi a

kimenő Ethernet-keretekbe kerülő MAC-címek meghatározását az IP-címek alapján. Az ARP-gyorsítótár tartalmát az *arp –a* paranccsal jeleníthetjük meg, az *arp –s* használatával pedig új statikus bejegyzéseket adhatunk a táblázathoz.



6.11. ábra: *A tartományvezérlő igen sok ponton kapcsolódik a hálózathoz*

A ***NetDiag***-program a kiszolgáló operációs rendszerek telepítőlemezén, a Support Tools csomagban található, a csomag telepítésével kerül fel a gépre *(\support\tools\suptools.msi)*. A parancs segítségével a különféle hálózati komponensek részletes vizsgálatát végezhetjük el. A program megvizsgálja valamennyi fontos hálózati elem működését (TCP/IP-paraméterek, NetBIOS, tartományvezérlők, különféle szolgáltatások elérhetősége stb.).

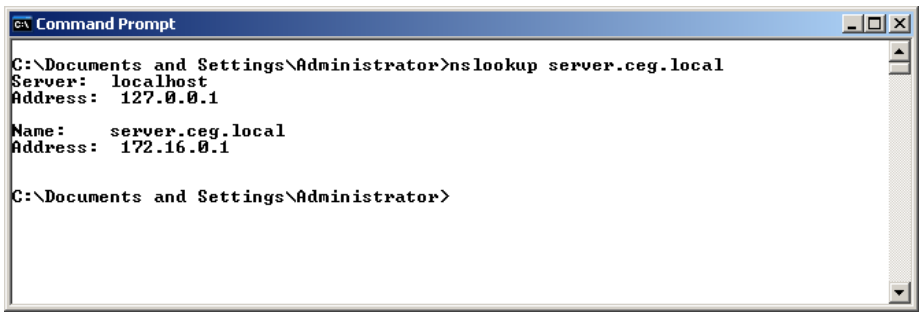
A ***Tracert*** nevű nyomkövető segédprogram a hálózati csomagok útvonalának meghatározására használható, segítségével listát készíthetünk azokról az útválasztókról, amelyeken egy megadott cél felé tartó csomagok áthaladnak. A *tracert* a következők szerint működik: A program ICMP *Echo* üzeneteket küld a cél IP-cím felé, amelyeknek TTL (Time to Live) értéke folyamatosan növekszik. A TTL érték 1-gyel indul, vagyis az első kiküldött csomag csak az első útválasztóig jut el, itt a TTL nullára csökken. Az útválasztó ilyenkor nem küldi tovább a csomagot, hanem ICMP Time Exceeded – TTL Exceeded in Transit hibaüzenetben értesíti a küldőt az eseményről. A *Tracert*-program feljegyzi a hibaüzenetet, (amely természetesen tartalmazza a feladó, vagyis

az első útválasztó címét is) és új csomagot küld a célcím felé, egyel nagyobb TTL-értékkel. Ez a csomag a második útválasztón fog hibaüzenetet generálni, így a *tracert* már ennek a címét is feljegyezheti. Mire a csomag eljut a címzetthez, a *tracert* az összes útválasztó címét ismerni fogja, amelyeken a csomag áthaladt. Ezután a *tracert* listát készít a hibaüzenetekből kinyert útválasztó-címekből, és a címhez DNS-lekérdezés segítségével meghatározott nevekből. Ha használjuk a *-d* opciót, a program nem hajt végre DNS-lekérdezést, ilyenkor csak az útválasztók IP-címei jelennek meg. A *tracert* parancs felhasználható annak a meghatározására, hogy egy adott csomag továbbítása a hálózat mely pontján lett leállítva.

A ***ping*** parancssori segédprogram a megadott célállomás működőképességének ellenőrzésére szolgál. A ping ICMP *Echo* üzeneteket küld a megadott IP-cím felé, majd várakozni kezd a címzettől érkező ICMP *Echo Reply* üzenetekre. A program kiírja a beérkezett válaszüzenetek számát, valamint a kérés elküldése és a válasz megérkezése között eltelt időt.

A ***pathping*** nevű parancssori eszköz a *ping* és a *tracert* funkcionalitásának kombinációját nyújtja, és néhány további szolgáltatással is rendelkezik. Az útvonal feltérképezése mellett a *pathping* minden egyes útválasztót többször is pingel, és megjeleníti a késleltetéssel és elveszett csomagokkal kapcsolatos információkat. Ilyen módon felmérhetjük az útvonalon elhelyezkedő rossz átvivő képességű vonalakat és útválasztókat.

Az ***nslookup*** program a DNS-infrastruktúra hibakereséséhez használható adatok megjelenítésére alkalmas. Segítségével lekérdezhetjük a megadott DNS-kiszolgáló adatbázisában tárolt értékeket (számítógépnév megadásával IP-címet és fordítva). A parancs első paramétereként a lekérdezendő nevet, vagy IP-címet kell megadnunk, második paraméterként pedig megadhatjuk annak a DNS-kiszolgálónak a nevét (vagy IP-címét), amelynek a lekérdezését el kell küldeni. Ha nem adunk meg második paramétert, akkor a számítógépen beállított alapértelmezett DNS-kiszolgáló fog válaszolni. Az *nslookup* nagyon jól használható a névfeloldással kapcsolatos egyszerűbb hibák gyors felderítésére, ha ilyen problémára gyanakszunk érdemes mindig ezzel kezdeni a hibakeresést.



6.12. ábra: *A kiszolgáló saját magától kérdezi meg az IP-címét*

Network Monitor

Az eddigiekkel szemben a Network Monitor már egyáltalán nem nevezhető egyszerű eszköznek, de szakértő kézben gyakorlatilag bármire képes; segítségével a hálózati működés legmélyebb rétegeibe is betekintést nyerhetünk. A program segítségével rögzíthetjük és megvizsgálhatjuk a gépünkhöz érkező vagy kimenő valamennyi hálózati csomagot, ezeket a Network Monitor a hálózati architektúra NDIS rétegének megcsapolásával gyűjti össze számunkra. Mivel az NDIS meghajtó a hierarchia legalacsonyabb szoftveres rétege (alatta már csak a hálózati adapter hardvere található), a Network Monitor segítségével minden olyan csomagot láthatunk, amit a hálózati adapter továbbküld az operációs rendszer felé.

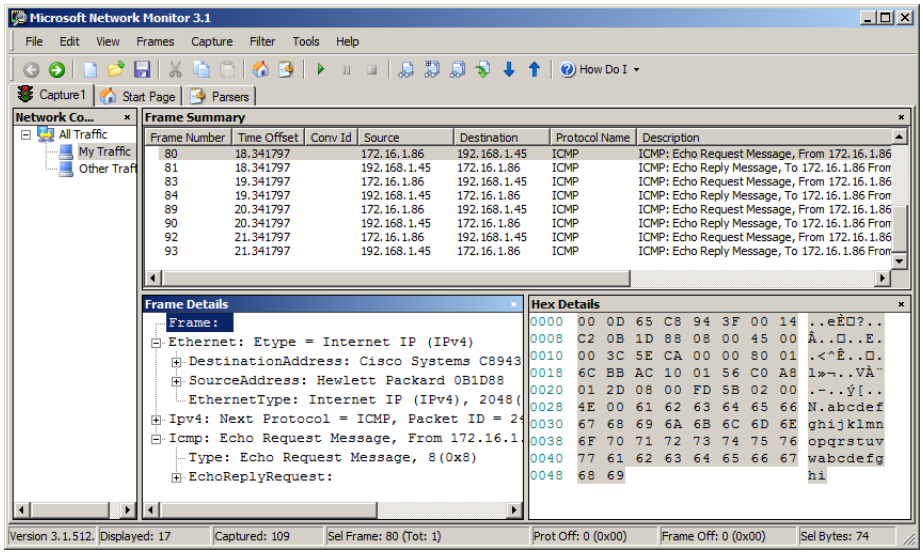
Az üzenetszórásos hálózat működési elve szerint (a switchekkel összekapcsolt hálózattal most nem foglalkozunk), minden egyes csomagot a hálózatra kapcsolt valamennyi gép megkap. Ezután a hálózati adapter hardveresen összehasonlítja az Ethernet csomagban lévő cél MAC-címet a sajátjával, és csak a neki szánt csomagokat küldi tovább a feljebb lévő szoftveres rétegek felé. A Network Monitor driver ezt a hardveres szűrést kapcsolja ki (promiszkusz mód), így megjelenítheti a hálózaton elérhető valamennyi csomag tartalmát.

A promiszkusz mód korábban csak a SMS részeként beszerezhető Network Monitor Gold verzióban volt használható (a kiszolgáló operációs rendszerek részeként kapott alapváltozatban nem), de a legújabb, 3.1-es verzióban már nincs ilyen megkülönböztetés, a p-módnak elnevezett üzemmód egyszerűen ki- és bekapcsolható a grafikus felületen.

Egyetlen esetben nem jelenik meg a hálózati csomag a Network Monitorban; ha az Ethernet keret CRC-je hibás, a hálózati adapter semmiképpen nem küldi tovább a csomagot. A Network Monitor használatával összegyűjthetjük azokat az információkat, amelyek segítségünkre lehetnek a hálózat hibátlan működésének fenntartásában, és az esetleges hibák gyors kiküszöbölésében.

A Network Monitor programot beállíthatjuk úgy, hogy csak azokat az adatokat jelenítse meg, amelyekre az adott helyzetben éppen szükségünk van. Szűrők segítségével szabályozhatjuk a csomagok megjelenítését és elrejtését, például a csomag típusa (protokoll), vagy forrás-, illetve célcíme alapján. Beállíthatjuk azt is, hogy a Network Monitor bizonyos feltétel, vagy feltételek teljesülése esetén automatikusan elindítsa, vagy leállítsa a csomagok gyűjtését. Természetesen lehetőségünk van a megjelenítés paramétereinek beállítására is, például a különböző csomagtípusokat különböző színnel jeleníthetjük meg.

A Network Monitor segítségével az összegyűjtött adatokat fájlba is menthetjük későbbi vizsgálat és elemzés céljából.

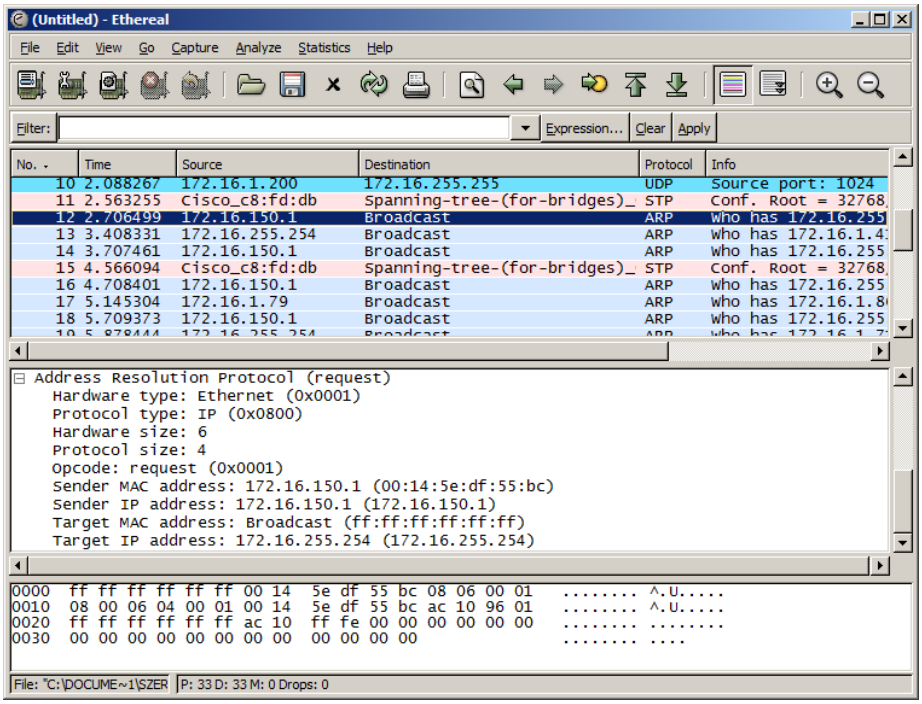


6.13. ábra: *A ping program hálózati forgalma a Network Monitorban*

A Network Monitor régebbi verzióit a Windows kiszolgáló operációs rendszerek beépítetten tartalmazzák (az Add or Remove Programs *(Programok telepítése és törlése)* segítségével telepíthető), a legújabb, 3.1-es verzió pedig szabadon letölthető a Microsoft webhelyről. Az új verzió számos új funkcióval rendelkezik, képes például a vezeték nélküli hálózatok forgalmának megfigyelésére, a Vista RAS-kapcsolatainak (beleértve a VPN-kapcsolatokat is) ellenőrzésére. Az új Network Monitor a szokásos módon a Microsoft Update, (illetve a vállalat saját WSUS-kiszolgálója) segítségével frissíthető.

Ethereal

Az Ethereal egy másik hálózatmonitorozó program, amelynek funkciói nagyjából megegyeznek a Network Monitor lehetőségeivel, de számos beállítása valamivel egyszerűbben adható meg, ezért kezdésnek talán jobban ajánlható. Az Ethereal számos platformra (Windows, MAC, különféle Linux és UNIX verziók) ingyenesen letölthető a *http://www.ethereal.com/download.html* címről.



6.14. ábra: *Broadcast ARP-lekérdezés megjelenítése az Ethereal programban*

Adataink biztonsága

A biztonsági mentés és visszaállítás beállításai és időzítése
Ebben a screencastban az NTBackup programé a főszerep, megmutatjuk a különféle beállítási lehetőségeit, biztonsági mentést készítünk néhány fájlról, majd visszaállítjuk azokat.
Fájlnév: II-3-3a-NTBackup.avi

A biztonsági mentés a hibaelhárítás utolsó védelmi vonala, segítségével még a legsúlyosabb esetekben is elkerülhető értékes adataink teljes elvesztése. Természetesen csak akkor szabad ehhez az eszközhöz nyúlnunk (persze nem a mentésről, hanem a helyreállításról van szó), ha más módszertől már nem remélhetünk eredményt, hiszen a biztonsági mentésből való helyreállítás szükségszerűen adatvesztéssel jár; a mentések ütemezése határozza meg az elveszíthető adatok maximális mennyiségét.

Meg kell jegyeznünk, hogy a redundáns lemez-alrendszerek (hardveres RAID) semmiképpen nem helyettesíthetik a rendszeres biztonsági mentéseket, hiszen nem nyújtanak védelmet az adatok szándékos vagy véletlen (például figyelmetlenség, vagy szoftverhiba miatt) törlése ellen, illetve a hardverrel kapcsolatos katasztrófa (több lemez egyidejű meghibásodása, tűzeset stb.) esetén is elveszíthetjük adatainkat. A redundáns alrendszerek alapvetően nem az adatbiztonságot (részben persze azt is), hanem a rendelkezésre állást növelik.

Nagyon fontos, hogy két fogalmat pontosan megkülönböztessünk egymástól:

- **Biztonsági mentés** – adatok másolása egy alternatív médiára, az adatvesztés elkerülése (csökkentése) miatt. A mentett állományok hosszú távú megőrzése általában nem szükséges.
- **Archiválás** – az adatok áthelyezése olyan médiára, mely biztosítja a hosszú távú megőrzést (ezt általában különféle előírások szabályozzák) és többnyire keresési lehetőséget is nyújt.

A mentési rendszer megtervezésével kapcsolatban számos olyan szempontot kell figyelembe vennünk, amelyek teljes mértékben a helyi, egyedi adottságoktól függenek, így sajnos nem létezik általánosan használható recept. A következőkben azokat a kérdéseket tekintjük át, amelyekre választ kell találnunk a tervezés során:

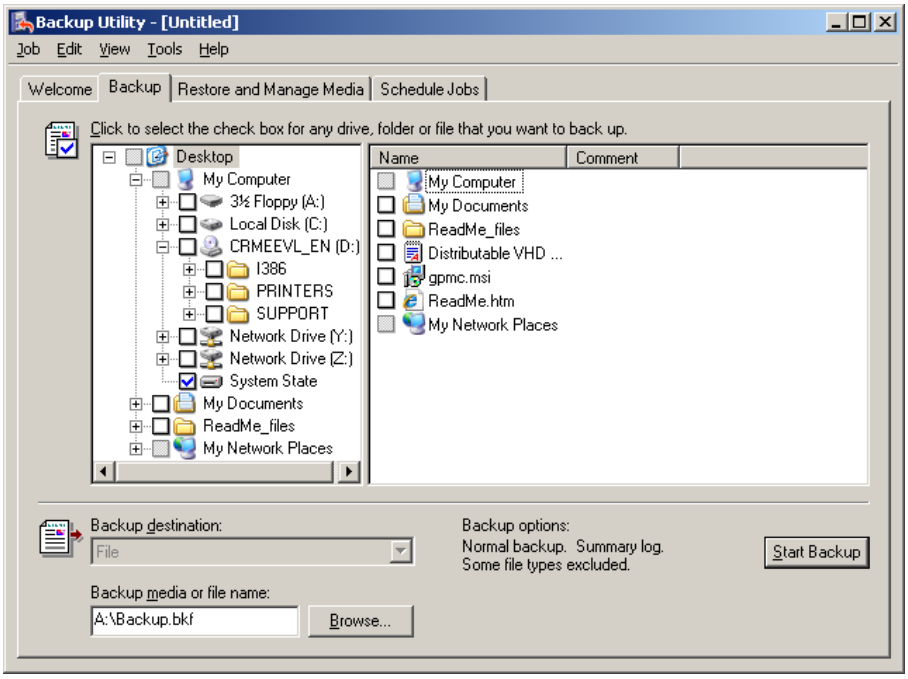
- **Mit mentsünk?** (És mit ne?) – Mentsünk rendszeresen minden olyan adatot, amelynek elvesztése problémát okoz, és más módon való helyreállítása nem lehetséges, illetve több munkával jár, mint a mentési fájl visszatöltése. Semmiképpen nem érdemes azonban lementeni tehát azokat az adatokat, amelyek helyreállítására biztosan nem lesz szükség, illetve azokat sem, amelyek más módon is könnyen helyreállíthatóak. Fölösleges adatra jó példa a TEMP könyvtár és teljes tartalma, a felhasználók profiljába az Internet Explorer által lementet weblaptöredékek stb. Könnyen helyreállítható adatnak minősülhet például az Office programcsomag, és más alkalmazások. Bár az NTBackup képes a megnyitott fájlok mentésére is, mégsem érdemes a rendszerhez tartozó nyitott fájlokkal próbálkozni. Teljesen fölösleges például bevenni a mentésbe a Windows lapozófájlját *(pagefile.sys),* vagy az Active Directory-adatbázisfájljait *(ntds.dit)* stb. (az Active Directory mentése a System State mentés része, a fájlok közvetlen mentésére nincs szükség).
- **Milyen sűrűn mentsünk?** – Amint már említettük, a mentések sűrűségét az elveszíthető adatok maximális mennyiségének kell meghatároznia. Minél kevesebb (rövidebb idő alatt keletkező) adat elvesztését képes különösebb probléma nélkül elviselni a vállalat, annál gyakrab-

ban kell mentéseket végeznünk. Természetesen a mentések gyakoriságának meghatározásakor figyelembe kell vennünk a tárolt (és mentendő) adatok közötti különbségeket is: a gyakran változó, értékes állományokat sűrűbben, a ritkábban módosított adatokat pedig ritkábban kell menteni (esetleg elegendő az egyszeri archiválás is).

- **Mire mentsünk?** – Nagyon fontos kérdés a biztonsági mentéseket tároló eszközök és a média (merevlemez, szalag, optikai lemezek stb.) kiválasztása is. A kiszolgálóban lévő második merevlemeztől, a különféle szalagos meghajtókon keresztül az önálló, automatizált tárolóegységekig számtalan megoldás közül választhatunk, az optimális megoldás megtalálásához figyelembe kell vennünk a szükséges kapacitást, a sebességet, a megbízhatóságot, tartósságot, és a fajlagos költséget is. A mentéseket tartalmazó média tárolására lehetőség szerint válasszunk olyan megoldást, ami komolyabb katasztrófa esetén is megfelelő biztonságot nyújt: szükséges lehet a kiszolgálótól fizikailag is elkülönített (akár különálló telephelyen lévő) tároló hely, tűzbiztos kazetta stb.
- **Mikor mentsünk?** – Az adatok mentését célszerű olyan időpontra időzíteni, amikor várhatóan nincsen sok megnyitott fájl (bár ezek korábbi verzióit az árnyékmásolat technológia segítségével az NTBackup képes lementeni), és a mentés által lefoglalt erőforrások hiánya nem zavarja a felhasználókat. Szokásos irodai környezetben ez azt jelenti, hogy a mentéseket az éjszakai órákra és a hétvégére kell időzítenünk. Ebből következően a mentések elvégzésére korlátozott időintervallum áll rendelkezésre, ezt figyelembe kell vennünk a mentendő adatok körének (mennyiségének) meghatározásakor, és ennek megfelelően kell kiválasztanunk a mentés típusát (a mentés különféle típusairól később még szót ejtünk) és a felhasználandó eszközöket is.
- **Mennyi ideig fog tartani a visszaállítás?** – Természetesen már a mentések megtervezésekor figyelembe kell vennünk a visszaállítással kapcsolatos szempontokat. Hogy maximálisan mennyi időt vehet igénybe a visszaállítás, azt alapvetően a vállalat működése határozza meg, az elvárt szintidőnek megfelelően kell megvalósítanunk és beállítanunk a mentési rendszert.
- **Ki fogja elvégezni a mentést?** – A fájlok mentését azok tulajdonosai és a legalább olvasási joggal rendelkező felhasználók végezhetik el, ennek megfelelően kell beállítanunk az időzített mentésekhez tartozó felhasználói fiókot. Az Administrators, Backup operators és Server operators csoportok tagjai még olyan fájlok mentésére is képesek, amelyekhez egyébként semmiféle jogosultsággal nem rendelkeznek.

Az NTBackup

A biztonsági mentések elvégzésére a Windows-rendszerek beépített NTBackup programját használhatjuk. Természetesen a megfelelő pénzösszeg ellenében választhatunk más megoldást is – számos kifinomultabb, több lehetőséggel rendelkező rendszer van a piacon –, de kisvállalati környezetben az NTBackup gyakorlatilag mindent tud, amire szükségünk lehet.



6.15. ábra: *Az NTBackup grafikus felülete*

Az NTBackup segítségével a következő feladatokat végezhetjük el:

- Kiválasztott fájlok és mappák mentése és visszatöltése.
- Megnyitott fájlok mentése az árnyékmásolat technika segítségével. Az árnyékmásolatokról *(Shadow Copies)* és a kapcsolódó beállítási lehetőségekről a negyedik, **Kiszolgáló a hálózatban** című fejezetben részletes leírás található.
- Másolat készítése a számítógép rendszerállapotáról (System State mentés).

Az NTBackup program a csak a helyi rendszerállapot adatok mentésére képes, távoli számítógépek rendszerállapotának mentésére nincs lehetőség.

- Automatikus rendszer-helyreállításhoz (*Automated System Recovery, ASR)* szükséges fájlok és konfigurációs beállítások mentése és helyreállítása.
- A távtárolókon és felcsatolt hálózati meghajtókon található adatok mentése.
- Naplófájl készítése a biztonsági mentés folyamatáról.
- Másolat készítése a rendszerpartícióról, a rendszerindító partícióról és rendszerindításhoz szükséges fájlokról.
- A biztonsági másolatok automatikus elkészítésének időzítése.
- A mentéshez felhasznált média alapszintű kezelése (például formázás). Az NTBackup gyakorlatilag bármilyen médiára képes mentést készíteni.
- Online adatbázist használó Microsoft termékek adatainak mentése.

Az NTBackup nemcsak a grafikus felület, hanem parancssori paraméterek segítségével is teljeskörűen vezérelhető, így lehetőség van a parancsfájlból, vagy különféle szkriptnyelvekből való használatára is.

System State mentés

A tartományvezérlőkön elvégezhető rendszerállapot mentésről az előző, **Tartományi környezet** című fejezetben már volt szó, most csak röviden áttekintjük, hogy a számítógép funkciójától függően milyen adatok kerülnek bele ebbe a körbe:

- Regisztrációs adatbázis – minden esetben
- Indítófájlok, rendszerfájlok – minden esetben
- A WFP érvényessége alatt lévő rendszerfájlok – minden esetben
- Tanúsítványtár – ha a számítógép Tanúsítványtár kiszolgáló
- Címtár-adatbázis *(Active Directory)* – ha a számítógép tartományvezérlő
- SYSVOL-mappa – ha a számítógép tartományvezérlő
- Klaszter szolgáltatásra vonatkozó adatok – ha a számítógép egy klaszter része
- IIS metadirectory – ha telepítve van

A mentés típusa

Az NTBackup több különböző típusú mentés elvégzésére képes, a következőkben ezekkel fogunk megismerkedni. A különböző típusú mentések közben az NTBackup a mentendő fájlok két tulajdonságát veszi figyelembe. Az egyik természetesen az utolsó módosítás dátuma, a másik pedig egy speciális fájl, illetve mappatulajdonság, az archiválandó attribútum. Az attribútumot minden olyan művelet köteles bekapcsolni, ami a fájl tartalmának módosításával jár (ebből tudja majd az NTBackup, hogy a fájl megváltozott, tehát menteni kell). A sikeres mentés után általában (a mentés típusától függően) az NTBackup törli az attribútumot. A fájlok és mappák tulajdonságlapján az archiválandó attribútum az Advanced *(Speciális)* szakaszban File is ready for archiving *(A fájl archiválásra kész*) néven szerepel.

Az NTBackup program segítségével a következő mentési típusokat használhatjuk:

- **Copy backup** *(Másolat)* – A másolás lementi az összes kijelölt fájlt, de nem jelöli meg a fájlokon a biztonsági mentés elvégzését (vagyis nem törli az archiválandó attribútumot). A másolás akkor lehet hasznos, ha például az ütemezett normál és növekményes biztonsági mentések között egy extra másolatot is szeretnénk készíteni adatainkról, mivel a másolás semmiképpen nem befolyásolja a szokásos mentéseket.
- **Daily Backup** *(Napi mentés)* – a kijelölt fájlok közül csak azokról készít mentést, melyek a mentés futtatásának napján módosultak. A biztonsági mentést az NTBackup nem jelöli a fájlokon (más szóval nem törli az archiválandó attribútumot).
- **Differential Backup** *(Különbségi mentés)* – a különbségi mentés a legutolsó normál vagy növekményes mentés óta létrehozott vagy módosított fájlokról készít biztonsági másolatot. A különbségi mentés nem törli az archiválandó attribútumot. A normál és különbségi biztonsági mentés kombinációjának (például hetente normál, naponta pedig különbségi mentés) használatakor a visszaállításhoz a legutolsó normál és a legutolsó különbségi másolatra lesz szükség.
- **Incremental Backup** *(Növekményes mentés)* – A növekményes mentés a legutolsó normál vagy növekményes biztonsági mentés óta létrehozott vagy módosított fájlokról készít másolatot. A mentés végrehajtását a rendszer megjelöli a fájlokon, vagyis ebben az esetben törlődni fog az archiválandó attribútum. A normál és a növekményes biztonsági mentés kombinációjának használatakor a visszaállításhoz a legutolsó normál és az azóta létrehozott valamennyi növekményes biztonságimásolat-készletre szükség lesz.

- **Normal Backup** *(Normál mentés)* – A normál biztonsági mentés az összes kijelölt fájlt lementi, és törli rajtuk az archiválandó attribútumot. Normál biztonsági másolat esetén valamennyi fájlt egyetlen biztonságimásolat-készlet használatával visszaállíthatjuk. A legelső biztonságimásolat-készlet létrehozásakor általában normál biztonsági másolatot kell készítenünk.

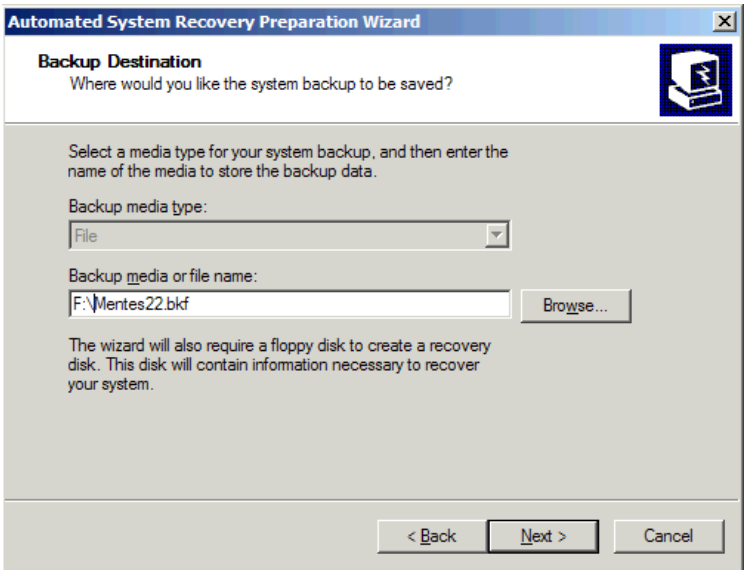
Adataink biztonsági mentéséhez a normál és a növekményes mentés kombinációjának használatával van szükség a legkisebb tárolókapacitásra, és a növekményes mentések végrehajtásához viszonylag kevés idő is elegendő lehet. A fájlok visszaállítása azonban ezzel a módszerrel időigényes és bonyolult lehet, mivel több biztonságimásolat-készletet kell használnunk, amelyek akár több lemezen vagy szalagon is lehetnek. Ha például hétvégén végezzük el a normál mentést (ekkor viszonylag sok idő állhat rendelkezésre), éjszakánként pedig a növekményes mentéseket, akkor egy pénteki visszaállítás esetén szükségünk lesz az előző hétvégén készült normál mentésre és minden azóta készült növekményes mentésre is.

Ha a normál és a különbségi biztonsági mentés kombinációját használjuk, akkor a különbségi mentések több időt vehetnek igénybe (különösen gyakran módosuló adatok esetén), de egyszerűbb lesz az adatok visszaállítása, mivel csak az utolsó normál, és az utolsó különbségi készletre lesz szükségünk.

Automatikus rendszer-helyreállítás

Az Automatikus rendszer-helyreállítás *(Automated System Recovery, ASR)* segítségével egy hajlékonylemezből és egy mentési fájlból álló készletet lehet létrehozni, amelynek segítségével visszaállítható a sérült rendszer mentéskori állapota. Természetesen mielőtt ezt a módszert használnánk érdemes megpróbálkozni más lehetőségekkel is (csökkentett mód, Last Known Good Configuration, Helyreállítási konzol stb.).

Az automatikus rendszer-helyreállítás két részből áll: elsőként a működő rendszeren az NTBackup program Automatikus rendszer-helyreállító varázslójának *(Automated System Recovery Wizard)* segítségével létre kell hoznunk a megfelelő helyreállító készletet. A készlet egyik eleme egy mentési fájl, ami tartalmazza a rendszerállapot adatokat, a rendszerszolgáltatásokat és az operációs rendszerhez tartozó valamennyi kötet adatait. A varázsló a mentési fájl mellé egy hajlékonylemezt is készít, amelyen megtalálhatjuk a biztonsági másolatra és a lemezbeállításokra (alap- és dinamikus kötetek), valamint a visszaállítás menetére vonatkozó információkat.



6.16. ábra: *ASR-készlet létrehozása az NTBackup használatával. Szükség lesz egy floppylemezre is (és nem árt egy floppymeghajtó sem)*

Időzített mentés

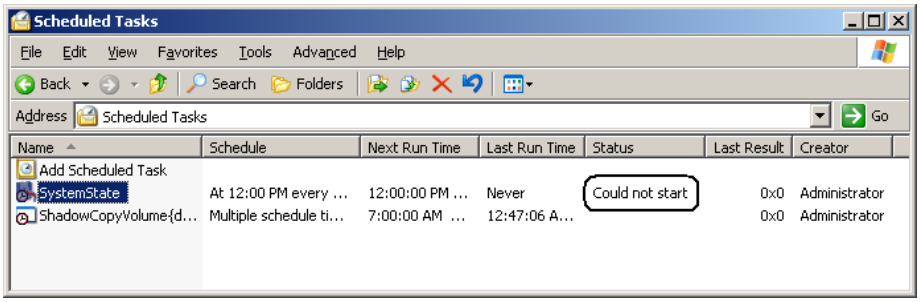
Az NTBackup segítségével összeállított mentési feladatokat végrehajthatjuk közvetlenül a felületről történő indítással, illetve (a mentési beállítások fájlba írása után) a beállítható időzítésnek megfelelő időpontokban automatikusan. A mentések ütemezéséhez az összeállított beállításokat fájlba kell mentenünk, és meg kell adnunk egy felhasználónevet (és jelszót), akinek nevében az ütemezetten induló feladatok futni fognak.

A következő időzítések beállítására van lehetőségünk:

- **Egyszer** *(Once)* – A feladat egyetlen egyszer, a megadott időpontban fog lefutni.
- **Napi** *(Daily)* – A feladat naponta egyszer, a megadott időpontban fog lefutni.
- **Heti** *(Weekly)* – a feladat hetenként ismétlődve a megadott napok megadott időpontjában fog lefutni.
- **Havi** *(Monthly)* – a feladat havonta egyszer, a megadott időpontban fog lefutni.
- **Rendszerindításkor** *(At System Startup)* – A következő rendszerindítás alkalmával.

- **Belépéskor** *(At Logon)* – A következő belépés alkalmával (a mentést időzítő felhasználó belépésről van szó).
- **Üresjárati időben** *(When idle)* – A feladat akkor fog elindulni, amikor a rendszer a megadott idő óta nyugalmi állapotban van.

Az ütemezett feladatok (így a beállított biztonsági mentések) végrehajtásáért a Windows-rendszerek beépített Feladatütemező szolgáltatása *(Task Scheduler)* a felelős. A Control Panel → Scheduled Tasks elemének használatával ellenőrizhetjük mentési feladataink végrehajtásának eredményét, és szükség esetén itt is módosíthatjuk a beállításokat (időzítés, futtató felhasználó stb.).



6.17. ábra: *A mentési feladatok futásának eredményét a Feladatütemezőben nézhetjük meg*

A visszaállítás

A visszaállítás az a lépés, amit soha senki nem szokott előre kipróbálni, éles helyzetben meg úgysem sikerül. Nagyon fontos, hogy a mentési feladatok beállítása után teszteljük a visszaállítást is. A következőkben végigkövetjük a mentésből való helyreállítás lépéseit. Tételezzük fel, hogy az egyik tartományvezérlőnk rendszerlemeze meghibásodott, a gép nem indítható, és semmi esély nincs rá, hogy más módon üzemképessé tehetjük. A gépben lévő második merevlemezen (vagy szalagon, ez tulajdonképpen lényegtelen) van egy előző nap készített normál mentés (d:\mentes\backup.bkf) ezt szeretnénk visszaállítani. Mi a teendő?

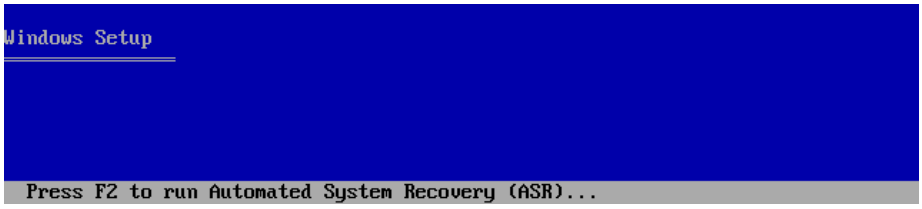
A mentési fájl beolvasásához és a visszaállításához szükségünk van az NTBackup-programra, mégpedig éppen azon a gépen, amelyre a rendszerállapot adatokat vissza szeretnénk állítani. A hibás merevlemez cseréje után tehát telepítenünk kell a gépre egy Windows Server 2003 rendszert, hogy legnagyobb részét azonnal felülírhassuk a korábbi mentésünkkel. A következő lépéseket kell tehát elvégeznünk:

- Telepítünk egy üres Windows Server 2003-at a telepítőlemezről.
- Az új rendszerben elindítjuk az NTBackup-programot, és a mentési fájlból visszatöltjük a rendszerállapot adatokat.
- Végül újratelepítjük a szükséges alkalmazásokat, és megint az NTBackup segítségével visszamásoljuk a mentett adatokat is.

A visszaállítás (csak a megfelelő jogosultság birtokában végezhető el) értelemszerűen felülírja mentésben szereplő fájlokat és mappákat, illetve a rendszerállapot adatokat is. A mentett fájlok és mappák nem csak az eredeti helyükre, hanem bárhová visszaállíthatók, de a rendszerállapot adatok csak az NTBackup programot futtató számítógép aktuális beállításainak helyére kerülhetnek, vagyis mindenképpen felülírják azokat

Visszaállítás ASR-készlet alapján

Az Automatikus rendszer-helyreállítási készletek segítségével történő helyreállítás a Windows telepítőprogramjának futtatása közben érhető el (CD-ről való rendszerindításkor). A telepítési folyamat elején az F2 billentyű lenyomásával indíthatjuk el a helyreállítási folyamatot.



6.18. ábra: *Az automatikus rendszer helyreállítást a telepítőlemezről bootolva indíthatjuk el*

Az ASR a készlet részeként létrehozott hajlékonylemez alapján helyreállítja a számítógép indulásához szükséges lemezek összes kötetét és partícióját, és a Windows néhány másik létfontosságú összetevőjét, majd a mentési fájl alapján visszaállítja a korábban elmentett fájlokat és adatokat. Az ASR visszaállítás tehát a következő műveleteket végzi el:

- Beolvassa a lemezkonfigurációt
- Visszaállítja a bootlemez szignatúrákat, a köteteket és a partíciókat
- Telepíti a Windows lementett verzióját
- Az NTBackup segítségével visszaállítja a rendszerállapotot és a mentett fájlokat

Külső eszközök

A Windows operációs rendszerek beépített hibakereső eszközein kívül számos külső program is rendelkezésünkre áll erre a célra. A következőkben a Sysinternals által jegyzett eszközök közül tekintünk át néhányat, amelyek igen jól használhatók szinte bármilyen hibakeresési feladat során, illetve némelyikkel az operációs rendszer működésének olyan mélységeibe láthatunk bele, ami semmiféle más eszközzel nem lehetséges. Az eszközöket világszerte rengetegen használják, így azok megbízhatóságához és hasznosságához nem férhet kétség.

Sysinternals segédprogramok

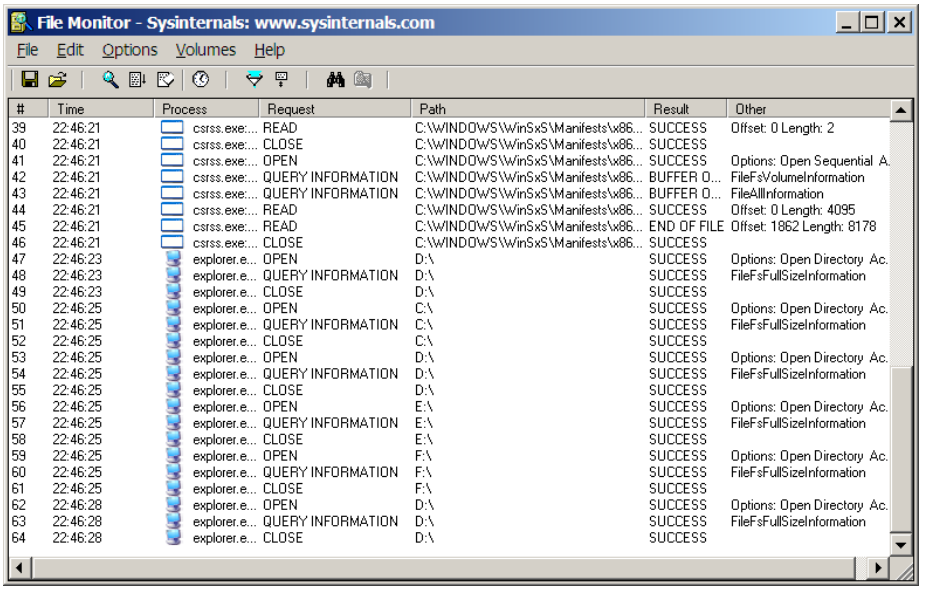
A Sysinternals által készített eszközök tulajdonképpen az operációs rendszer beépített eszközeinek többé-kevésbé (általában inkább többé) felokosított változatai, amelyeknek funkciói és kezelése kifejezetten a rendszergazdák szemléletmódját tükrözi. A Sysinternals cég számtalan ilyen eszközt készített, ezen felül pedig több igen érdekes és fontos könyv (Inside Windows-sorozat), előadás és oktatóanyag fűződik nevükhöz. A vállalatot 2006-ban a Microsoft megvásárolta (a cég alapítói azóta a Microsoft alkalmazásában állnak), de az eszközök továbbra is rendszeresen frissülnek (sőt újak is készülnek), és a http://www.microsoft.com/technet/sysinternals/default.mspx címről valamennyi ingyenesen, bárki számára letölthető.

Valamennyi eszköz futtatásához rendszergazda-jogosultság szükséges (Vista alatt *Run as Administrator)*, viszont telepítésre egyáltalán nincs szükség, a letöltött exe fájl minden további nélkül futtatható. A legfontosabb eszközök egyetlen csomagban is letölthetők a *http://tinyurl.com/ybce37* címről (Sysinternals Suite).

A Sysinternals eszközök
Ebben a screencastban kipróbáljuk a legfontosabb és a legérdekesebb Sysinternals eszközöket.
Fájlnév: II-3-2b-Sysinternals.avi

FileMon (File Monitor)

A FileMon segítségével megfigyelhetjük és naplózhatjuk valamennyi a fájlrendszerrel kapcsolatos műveletet (fájlok megnyitása, olvasás, írás stb.). A valós időben listázott adatok között megtalálhatjuk valamennyi fájlművelet pontos időpontját és típusát, a műveletet kezdeményező folyamat és az érintett fájl nevét, valamint a művelet eredményét is.



6.19. ábra: *Valamennyi fájlműveletet megfigyelhetjük a FileMon segítségével*

A FileMon kiválóan felhasználható a rendszer működésnek megfigyelésére (eléggé megdöbbentő mennyiségű fájlművelet történik egy érintetlen, semmi különöset nem csináló rendszerben is, nem beszélve mondjuk egy Word, vagy Outlook indításáról…), de talán a legfontosabb felhasználási területe a fájlrendszerbeli jogosultsághiányok „kimérése”.

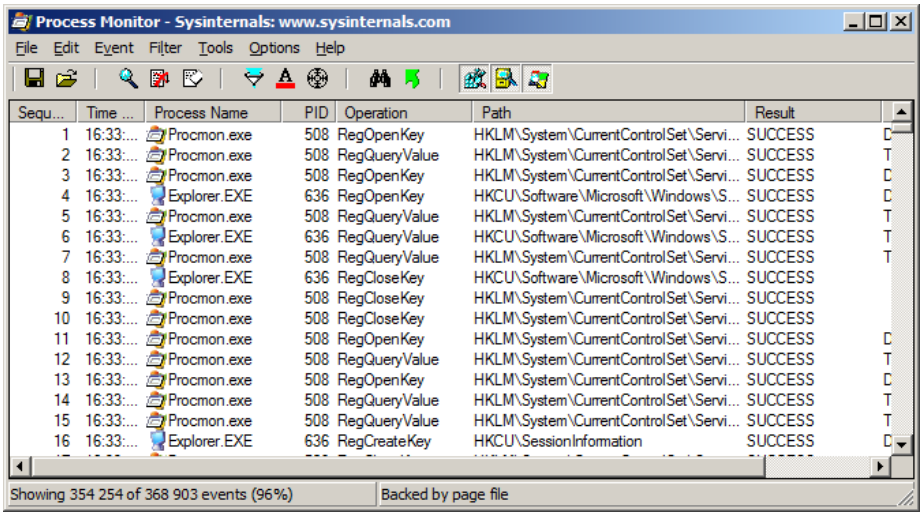
Ha egy rosszul megírt felhasználói alkalmazás nem hajlandó felhasználói jogosultságokkal elindulni, akkor a FileMon segítségével könnyen megtalálhatjuk a sikertelen műveletben szereplő fájlt vagy mappát, és így csak arra az egy elemre kell megadnunk a program futásához szükséges jogosultságot. A listába kerülő adatokat szűrhetjük például a műveletet kezdeményező folyamat neve szerint, és lehetőség van részletes keresésre és fájlba mentésre is.

RegMon (Registry Monitor)

A Regmon a registry-műveletek megfigyelésére használható, működése és felülete is erősen hasonlít a FileMon-ra. Hasonló a felhasználási terület is; megtudhatjuk, hogy a hibát generáló alkalmazás pontosan milyen registry-érték olvasása vagy írása közben adta meg magát (például egy hiányzó kulcs, vagy jogosultsághiány miatt), és így könnyen megoldhatjuk a problémát.

A FileMon és a RegMon helyét a Process Monitor vette át, ami viszont csak Windows 2000 SP4, Windows XP SP2, Windows Server 2003 SP1, és Windows Vista rendszereken futtatható. A régebbi rendszerek támogatása miatt azonban megmaradt az önálló FileMon és RegMon is (ezek még a Windows 9x rendszereken is elindulnak).

Process Monitor



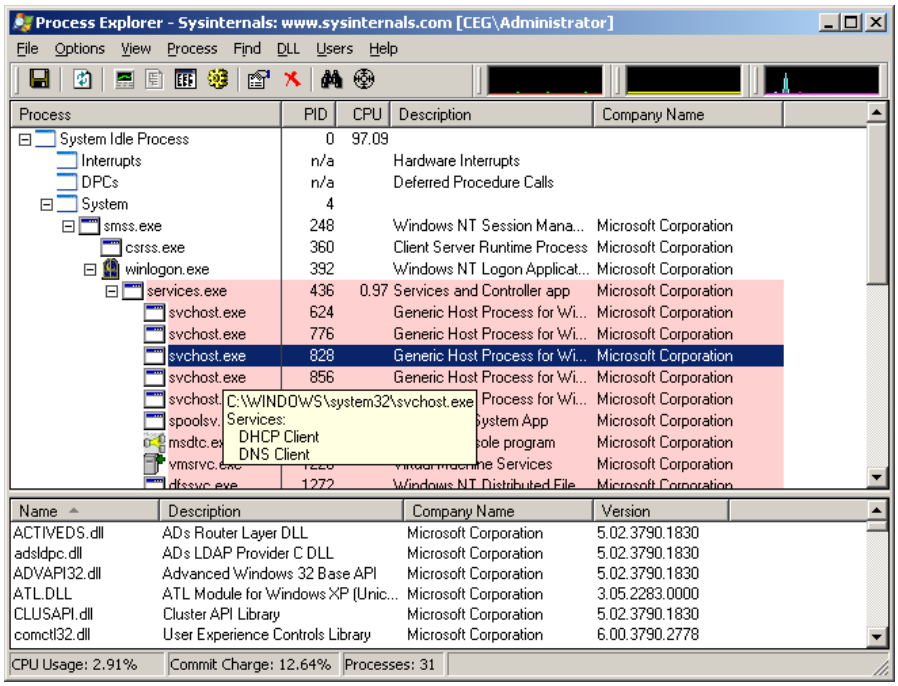
6.20. ábra: *A Process Monitor a fájlrendszer és registry mellett a folyamatok és programszálak monitorozására is képes*

A Process Monitor egy összetett rendszermonitorozó eszköz, amely képes a fájl- és registryműveletek, valamint a folyamatok és szálak valós idejű megfigyelésére (külön-külön és párhuzamosan is). Az eszköz egyben valósítja meg a FileMon és a RegMon képességeit, és számos új lehetőséget is nyújt.

DiskMon (Disk Monitor)

A DiskMon a lemezműveletek közvetlen megfigyelésére ad lehetőséget. Segítségével nyomon követhetjük, és fájlba menthetjük a lemezműveletekre vonatkozó különböző adatokat (időpont, időtartam, művelet fajtája, érintett szektor sorszáma stb.). A DiskMon elhelyezhető a tálcán is, ekkor zöld színnel jelzi az olvasási, pirossal pedig az írási műveleteket.

Process Explorer



6.21. ábra: *Process Explorer, a szuperokos Task Manager*

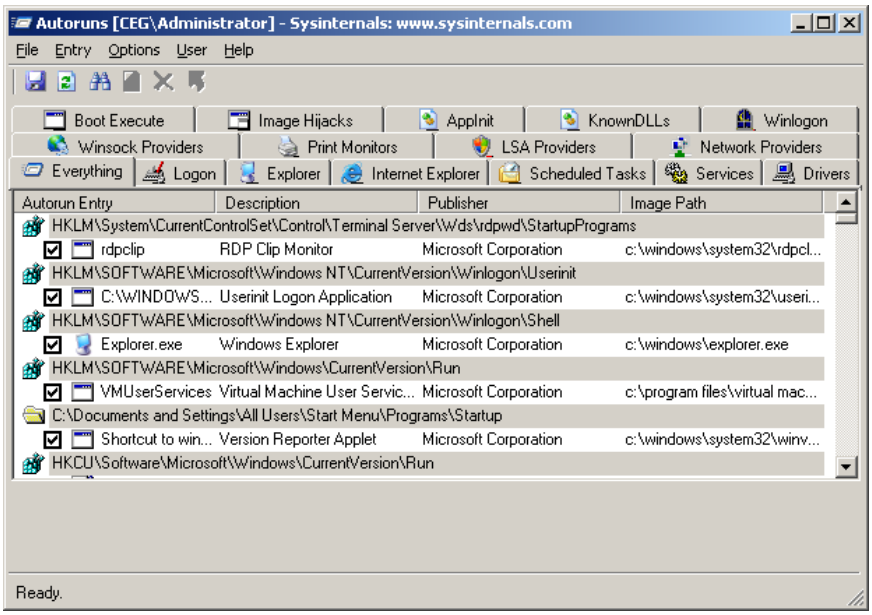
A Process Explorer képes a számítógépen futó folyamatok szinte minden tulajdonságának megjelenítésre. Funkcióinak egy része megtalálható a Feladatkezelőben is, de segítségével rengeteg olyan információhoz is hozzájuthatunk, amelyek megjelenítésére a Feladatkezelő nem képes.

A folyamatok a szülő-gyermek kapcsolatoknak megfelelő fastruktúrában jelennek meg, és valamennyi folyamathoz megjeleníthetjük a használt rendszererőforrások és a nyitva tartott dll-ek listáját is. A Process Explorer igen kifinomult keresési lehetőségekkel rendelkezik, így pillanatok alatt megtalálhatjuk például azt a rendszerfolyamatot, amelyik egy adott erőforrást vagy dll-t megnyitva tart.

AutoRuns

Az AutoRuns segédprogram megkeresi és megjeleníti a rendszerindításkor automatikusan induló valamennyi programot, szolgáltatást stb., vagyis mindent, amit az operációs rendszer automatikusan elindít. A listába kerülnek az indítópultban és a különféle registrykulcsokban *(Run, RunOnce* stb.) szereplő bejegyzések, az Explorer shellbővítmények, a betöltődő eszköztárak és még sok minden más is.

A programhoz tartozik egy parancssori felülettel rendelkező eszköz is *(AutoRunsc.exe),* amellyel lehetőségünk van a kimenet *csv* fájlba való elmentésére is.

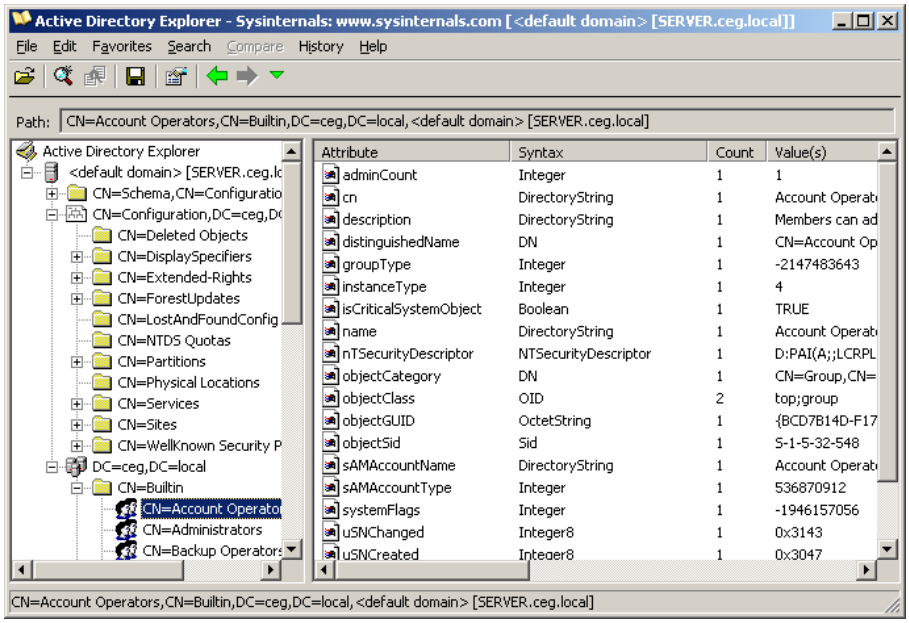


6.22. ábra: *Minden (de tényleg), ami elindul rendszerünkben*

AD Explorer

Az AD Explorer képes a címtáradatbázis nyers formájának megjelenítésére, segítségével elérhetjük valamennyi címtárpartíciót és megjeleníthetjük, illetve szerkeszthetjük az egyes objektumokhoz tartozó tulajdonságértékeket. Az ADExplorer nagyon kifinomult keresési lehetőségekkel rendelkezik, és lehetőségünk van a keresések elmentésére és későbbi újrafelhasználására is.

Teljesen egyedülálló lehetőség az, hogy offline megjelenítésre és összehasonlításra alkalmas pillanatképeket készíthetünk az Active Directory adatbázisról. A mentett adatbázis bármikor újra felcsatolható, vagyis az „élő" adatbázissal megegyező módon jeleníthető meg. A különböző időpontokban készült pillanatképek összehasonlításával azonosíthatjuk a megváltozott objektumokat, tulajdonságokat és jogosultági listákat.



6.23. ábra: *Active Directory-objektumok tulajdonságai az AD Explorerben*

AD Restore

Az ADRestore a törölt címtárobjektumok megkeresésére és visszaállítására képes. A program használata nagyon egyszerű, a címtár online állapotában indíthatjuk el és paraméterként (nem kötelező) csak a törölt objektumok között válogató szűrőt kell megadnunk.

PsTools – csomag a csomagon belül

A PSTools apró parancssori programokból álló gyűjtemény. A programok segítségével egyszerű műveleteket végezhetünk el, viszont érdekes lehetőség, hogy valamennyi parancs távoli gépre is használható.

A PSTools a következő elemekből áll:

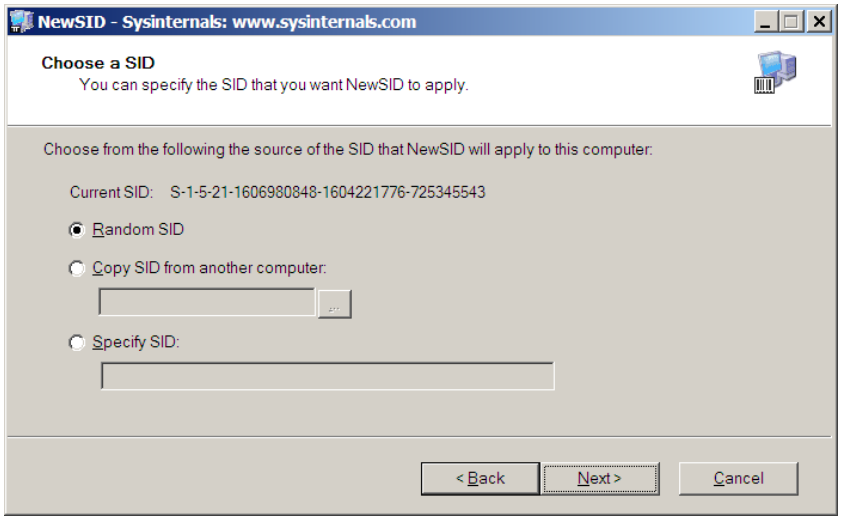
- **PsExec** – segítségével megadott nevű folyamatot indíthatjuk el (távoli gépen is).
- **PsFile** – a parancs a megnyitott fájlok listáját jeleníti meg.
- **PsGetSid** – a számítógép, illetve felhasználó biztonsági azonosítóját *(Security Identifier, SID)* írja ki.
- **PsInfo** – a program listázza az alapvető rendszerinformációkat.
- **PsKill** – a parancs segítségével lehetőségünk van a számítógépen (távoli gépeken is) futó folyamatok „könyörtelen” lezárására.

- **PsList** – a futó folyamatok listáját és az egyes folyamatok legfontosabb adatait jeleníti meg.
- **PsLoggedOn** – a parancs a számítógépre bejelentkezett felhasználókat listázza (a helyi bejelentkezéseket és a megosztott erőforrásokra vonatkozó kapcsolatokat is).
- **PsLogList** – a parancs az Eseménynapló bejegyzéseit listázza.
- **PsPasswd** – a parancs segítségével megváltoztathatjuk a felhasználói fiókokhoz tartozó jelszavakat.
- **PsService** – a parancs segítségével kilistázhatjuk a szolgáltatásokat, és elvégezhetjük a kezelésükkel kapcsolatos legfontosabb műveleteket.
- **PsShutdown** – a parancs használatával leállíthatjuk, illetve újraindíthatjuk a számítógépet (távolról is).
- **PsSuspend** – a parancs segítségével felfüggeszthetjük, illetve újraindíthatjuk a megadott szolgáltatást.

TCPView

A TCPView segítségével a TCP és UDP végpontok listáját jeleníthetjük meg. A program felületéről leolvasható az adott kapcsolathoz tartozó folyamat neve, a helyi és a távoli port száma, és a kapcsolódás állapota is. A program parancssori változatban is használható, ennek neve tcpvcon.exe.

NewSID



6.24. ábra: *A NewSID segítségével grafikus felületen változtathatjuk meg a biztonsági azonosítót*

A NewSID-program segítségével a számítógép egyedi biztonsági azonosítóját *(Security Identifier, SID)* változtathatjuk meg. A SID megváltoztatására a lemezkép alapú klónozás segítségével telepített számítógépek esetén van szükség, mivel a hálózati működés során különféle problémákat okozhat az egyforma biztonsági azonosítók használata.

BGInfo

Bár nem kapcsolódik szorosan a hibakereséshez, mindenképpen figyelmet érdemel ez az egyszerű, de nagyon ötletes program. A BGInfo segítségével egyszerűen az Asztal háttérképét állíthatjuk be, de olyan módon, hogy a képen megjelenjenek a számítógép különféle adatai (neve, IP-címe, operációs rendszere stb.). Ha a programot az Indítópultból, vagy logon szkriptből minden bejelentkezéskor lefuttatjuk, akkor a háttérkép mindig az éppen aktuális adatokat fogja tartalmazni. A program az automatikus indítás esetén sem marad a memóriában, csak elkészíti az aktuális háttérképet, és már véget is ér, vagyis biztosan nem foglalja a rendszer erőforrásait, és nem okoz semmiféle problémát a rendszer működésében.

FÜGGELÉK

Munka a virtuális gépekkel

A fejezet tartalma:

E könyv olvasóiban bizonyosan felmerül majd a fejezetek és a DVD-n található kisebb-nagyobb demók és előadások (screencastok) megtekintése után a különböző technológiák, eszközök és szolgáltatások kipróbálásának igénye. Mivel mi – azaz a könyv szerzői és a Microsoft „Informatika Tisztán" csapata – valóban meg vagyunk erről győződve ennek szükségességéről, szeretnénk ebben a tapasztalatszerzésben a lehető legtöbbet segíteni a kedves Olvasónak.

Véleményünk szerint a legegyszerűbb módszer a gyakorlati ismeretszerzésre a virtuális gépek használata, hiszen ekkor – a megfelelő hardver birtokában – kényelmesen és biztonságosan, akár a saját otthoni gépünkön is képesek leszünk letesztelni, hogy mit tud a Vista, hogyan építünk tartományt, hogyan működik a WSUS, és még sorolhatnánk a jobbnál jobb példákat. Ezért aztán a könyvet kísérő DVD-n elhelyeztünk két, még teljesen érintetlen, tömörített virtuális gépet, magát a virtualizáló alkalmazást, és a gördülékeny teszteléshez szükséges további komponenseket.

Ezzel az útmutatóval pedig a virtuális gépek területen teljesen járatlan Olvasónak szeretnénk egyfajta támaszt adni, illetve javaslatokat teszünk a demókörnyezet konkrét kialakítására is.

Alapozás a virtualizáció megismeréséhez

Egy-egy virtuális számítógép általában két állományból áll: az egyik egy *.vhd* fájl (ami gyakorlatilag a virtuális gép merevlemeze), a másik pedig egy *.vmc* fájl, amely pedig a virtuális gép beállításait tartalmazza. A Microsoft a *Run IT on a Virtual Hard Disk* jelszóval fenntart egy ún. VHD-könyvtárat, ahonnan bárki (regisztráció után) letöltheti az előretelepített, „konzerv" virtuális gépeket. Ezek közül kettőt helyeztünk el tehát a DVD-n, egy angol nyelvű Vista Enterprise, illetve egy szintén angol nyelvű Windows Server 2003 Enterprise R2 változatot.

A virtuális környezet használatához tehát egyrészt a speciális állományokat kell merevlemezre másolni, valamint fel kell telepíteni egy olyan virtualizációt megvalósító szoftvert, amely képes lesz dolgozni ezekkel a fájlokkal. Ezek a szoftverek jelenleg a következők: Microsoft Virtual PC 2007, Microsoft Virtual Server 2005 R2 SP1 és a System Center Virtual Machine Manager.

Otthoni környezetben, vagy egy szimpla munkaállomáson elsősorban az első szoftvert ajánljuk – és ebben az ismertetőben is csak ezzel foglalkozunk részletesen (az egyébként is ingyenesen letölthető Virtual PC 2007 telepítője DVD-n, a *Telepitocsomagok\VPC2007* nevű mappában található). A haladóknak, az összetettebb környezetre vágyóknak illetve a sok gépet futtatóknak viszont valószínűleg a Virtual Server fog jobban beválni. Természetesen, a friss és igazán professzionális, elsősorban a nagyvállalati környezetet megcélzó eszköz, a System Center Virtual Machine Manager „alatt" is működnek ezek a virtuális gépek, de ez már tényleg „ágyúval a verébre" módszer lenne a mi esetünkben.

Az említett haladó virtualizációs eszközökről további információt találhatunk a http://www.microsoft.com/virtualization weboldalon (a VPC 2007-et is innen tölthetjük le), a konzerv virtuális gépek pedig (sok más termék .vhd-ja mellett) letölthetőek http://www.microsoft.com/vhd oldalról.

A Virtual PC 2007 és a virtuális gép telepítése

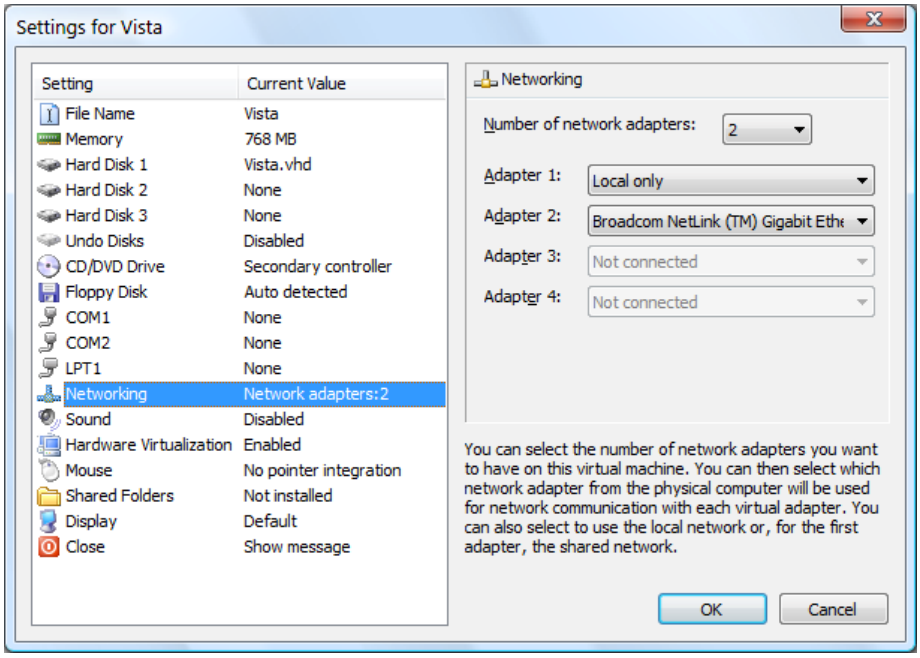
1. Indítsuk el a Virtual PC 2007 telepítőjét *(setup.exe)* a DVD-ről! A telepítés teljesen értelemszerű.

2. Futtassuk a DVD *Gepek\VistaEnt* mappájában lévő *Vista.part01.exe* állományt! Válasszunk ki egy célmappát a merevlemezünkön, majd tömörítsük ki a virtuális gép háttértárát *(.vhd)* és konfigurációs állományát *(.vmc)* és az egyéb információs fájlokat.
3. Tegyük meg ugyanezt a Windows Server 2003 R2 esetén is *(Gepek\W2K3R2* mappa > *WIN2K3R2EE.part1.exe).*

Legyünk türelmesek, a kicsomagolás eltart egy ideig. A két virtuális gép háttértár igénye viszonylag nagy, összesen kb. 7,3 GB.

Fontos tudnivaló az is, hogy mindkét gép az első indítás után maximum 30 napig működik csak. Tehát bármikor indíthatjuk a DVD-ről (pontosabban 2008. június 30-ig), de ha már megy, maximum 30 napig használható. Annak, hogy újra kicsomagoljuk és elindítsunk egy 30 napos periódust, semmi akadálya nincs.

A virtuális gépek elindítása



A virtuális környezet elindításához elegendő a virtuális gép telepítésekor megadott célkönyvtárban duplán kattintani (futtatni) az ott található *.vmc* fájlra, de – az első indítás előtt, a beállítások miatt – alternatív megoldásként használhatjuk a feltelepített Virtual PC 2007 konzolját is, amelyet a Start menüben, a Microsoft Virtual PC ikonjára kattintva tudunk indítani.

Ha ezt az utat választjuk, akkor a megjelent ablakban a *New…* gombra kattintva, majd az *Add existing virtual machine* opciót választva meg kell adnunk azt a könyvtárat, ahová a virtuális környezetet telepítettük, illetve konkrétan az adott *.vmc* elérhetőségét. Ezt követően a Virtual PC konzoljából a megjelent virtuális gépen duplán kattintva, vagy a kiválasztása után a *Start* gombra kattintva indíthatjuk el. De még ne tegyük, ismerkedjünk meg először a gépek finomhangolási lehetőségeivel.

A virtuális gépek beállításai

Az alábbiakat a Virtual PC 2007 konzoljában lehet beállítani gépenként külön-külön, a Settings gombra kattintva. Ezek a beállítások természetesen bekerülnek a *.vmc* állományokba is, azaz automatikusan mentésre kerülnek. Az itt felsorolt paraméterek egy része már be is van állítva, így ezekhez csak akkor szükséges nyúlni, ha változtatni szeretnénk rajtuk.

A Vista virtuális gép számára alapesetben 768 MB RAM van lefoglalva. Ezt az értéket nem célszerű kisebbre állítani (512 MB alá pedig semmiképpen sem), nagyobbra viszont – a lehetőségeink szerint – igen. A Windows Server 2003 R2 alapértelmezett memóriafoglalása 512 MB. Ezzel bőven be is éri, sőt, akár a felére is levehetjük, persze mikor már tartományvezérlőként használjuk érdemes lesz ezt az értéket újra kicsit megnövelni.

A virtuális gépek hálózatikártya-beállítása alapesetben *Not Connected*, ezt célszerű rögtön *Local Only*-ra átállítani mindkét gépnél. Az ilyen beállítással rendelkező virtuális gépek csak egymást érzékelik „fizikailag” a hálózaton, a külvilágot egyáltalán nem, sőt az ún. hostgépet, (amelyen a Virtual PC alkalmazás fut, azaz amely a virtuális gépeknek otthont ad) sem fogják hálózati szempontból elérni. Ez a beállítás ahhoz szükséges, hogy a Windows Server 2003 R2 és a Vista virtuális gépek „lássák” egymást – együtt egy belső hálózatott alkotnak majd –, de ne érintkezzenek sem az internettel, sem a hostgéppel. Ha erre az érintkezésre mégis szükség lesz (pl. WSUS-frissítések letöltése, RRAS stb.), akkor vegyünk fel egy második hálózati kártyát az adott virtuális gép leállított állapotában, és állítsuk be az „igazi” hálókártyánkat ehhez az interfészhez.

Ha a processzorunk megfelelő, akkor minden virtuális gépnél érdemes beállítani a hardveres támogatást, a *Hardware-assisted Virtualization* pontban.

Érdekes és fontos opció a hostgép mappáinak használata is. A beállítások között, a *Shared Folders* pontban van arra lehetőségünk, hogy egy betűvel jelölt meghajtóként felvegyük a futtató gép egy adott mappáját. Ha pl. majd bármilyen külső szoftvert kell telepíteni, akkor ezen a felcsatolt mappán (az-az a hostgépen) keresztül ezt egyszerűen meg tudjuk majd tenni.

Esetleg fontos lehet tudni azt is, hogy az összes virtuális gépre vonatkozó közös beállítás a VPC konzol *File/Options* menüpontja alól érhető el.

Ha viszont az eddig felsorolt fontos és az esetleges további, egyéni paraméterek beállításán túlvagyunk, akkor már elindíthatjuk a virtuális gépeket.

Elképzelhető, hogy a gépek indítása után kapunk egy üzenetet, amelyben arra figyelmeztet bennünket a VPC 2007, hogy a gépek *.vhd* fájlai Virtual Server alá passzolnak inkább. Nyugtázzuk, a működésben nem okoz problémát.

A Windows Server 2003 R2 virtuális gép indítása után először az ún. „mini setup", azaz az előtelepítés utolsó fázisa fut le, amely egy automatikus újraindításba torkollik. Várjuk ki türelemmel.

A Vistánál egy kicsit másképp történik az indítás. Itt is megjelenik a telepítés utolsó fázisa, amelyben viszont nekünk kell megadni először a regionális paramétereket, aztán az óhajtott saját felhasználónevet, jelszót, és ikont. Ezután jöhet a háttérkép, majd a hálózat beállítása (a Work profilt válasszuk, ez fog passzolni a feladatainkhoz). Már csak az idő és dátum beállítása marad, illetve egy automatikus teljesítmény vizsgálat kivárása.

Belépés és az első tennivaló

Miután (egy új ablakban) elindult virtuális operációs rendszerünk, hamarosan elérkezünk a bejelentkezési képernyőhöz.

A bejelentkezési képernyő megjelenése után kattintsunk bele a virtuális gép ablakába, hogy aktív legyen, majd a belépéshez nyomjuk meg az alapértelmezett *host key*-t, ami *ALT Gr + Delete*.

Abban az esetben van ez így, ha ezt korábban nem változtattuk meg. Megváltoztatni a Virtual PC 2007 konzolján lehet a *File* > *Options* > *Keyboard* menüpontra navigálva.

A Windows Server 2003 R2 gyári felhasználója az Administrator fiók**,** melynek jelszava: *Evaluation1.* Természetesen az első belépés után bátran létrehozhatunk saját fiókot, saját jelszóval, vagy megváltoztathatjuk az Administrator fiókét is.

A Vista gép esetén az általunk megadott helyi felhasználói fiókot használjuk.

Virtuális gépek esetén a belépés utáni első teendő a *Virtual Machine Additions* telepítés szokott lenni (a gép ablakának *Action* menüjéből). Ezzel a bővítménnyel általában plusz teljesítményhez és kényelmi szolgáltatásokhoz jutunk. Viszont erre most nem lesz szükség, mindkét virtuális gép esetén ez a komponens előtelepítésre került.

A virtuális gépet teljes képernyőn is használhatjuk, ehhez a *host key* + *Enter* gombok együttes lenyomása szükséges. Az ablakos megjelenítéshez ugyanezzel a billentyűkombinációval lehet visszaváltani.

Javaslat a demókörnyezet beállítására

Vista virtuális gép (az ügyfél):

- NetBIOS név: pl. *Vista, Gep1, PC1* stb.
- Fix IP célszerű: 172.16.0.2, Network mask: 255.255.0.0, Default Gateway: 172.16.0.1, DNS: 172.16.0.1 (mindezt azért fontos ennyire részletesen, mert később beléptetjük a tartományba)
- Amikor a *Network and Sharing Center*-t vizsgáljuk, vagy amikor a kiszolgálóból majd DHCP-kiszolgálót faragunk, érdemes lesz egy másik (szintén *Local Only)* hálózati kártyát felvenni a jól látható eredmény kedvéért.

W2K3 virtuális gép (a kiszolgáló):

- NetBIOS név: W2K3, Server stb.
- Fix IP szükséges: 172.16.0.1, Network mask: 255.255.0.0, Default Gateway: nincs, DNS: 172.16.0.1

Későbbi feladatkörei (a screencastokban mindent bemutatunk):

- FSMO DC, tartomány név nev: pl. ceg.local
- AD integralt DNS (pl. ceg.local)
- DFS, FSRM, PMC
- DHCP
- WINS
- RRAS, VPN
- WSUS 3.0, IIS, WSS

Amikor a Windows Server 2003 R2 alatt egy integrált Windows-komponenst szeretnénk feltelepíteni az *Add/Remove Programs* ablakból, akkor hivatkozzunk a virtuális gép *C:\WindowsInstallationFiles\i386* mappájára, ugyanis ezt szerencsére integrálta a Microsoft, az eredeti *.vhd* fájlba.

A gépek leállítása

A virtuális gépek leállítását a szokásos módon is végezhetjük, ilyenkor az operációs rendszer kikapcsol, de előtte lemezre ment minden módosítást, majd végül teljesen leáll.

Alternatív megoldásként megpróbálhatjuk bezárni a virtuális gép ablakát is. Ekkor választhatunk, hogy az előbb leírt, hagyományos leállítást szeretnénk kérni, vagy egyszerűen „megöljük" a gépet, mintha kihúznánk az elektromos hálózatból, vagy fizikailag kikapcsolnánk. Ez csakúgy, mint valódi gépek esetében csak végszükségben javasolható, mivel adatvesztést okoz.

Az előbbi listában a harmadik opció a *Save state*, amely lementi a virtuális gép teljes memóriáját, majd kikapcsolja azt. Ez nagyban hasonlít a hibernáláshoz, azonban ezt nem a virtuális operációs rendszer, hanem a Virtual PC 2007 végzi el a futtatott virtuális gépen. Az ilyen módon leállított gépeket később elindítva pontosan ugyanabban az állapotban kapjuk vissza, mint ahogy leállítottuk, még akkor is, ha a Virtual PC 2007-et futtató (host-) számítógépet újraindítjuk a leállítás után.

Tárgymutató

A, Á

B

C

Cs

D

E, É

F

G

Gy

H

I, Í

J

K

L

M

N

Ny

O, Ó

Ö, Ő

P

Q

R

S

Sz

T

U, Ú

Ü, Ű

V

W

X

Z

A szerzőkről

Gál Tamás

1996 óta üzemeltet Windows szervereket, vállalkozása több cég informatikai rendszerének gazdája, illetve konzultánsa. Rendszergazda, informatikai vezető, tréner, illetve 2007 januárja óta, a Microsoft Magyarország állományában, a TechNet program szakmai tanácsadójaként is tevékenykedik. Ebben a minőségében a hazai Microsoft konferenciák, események, webcastok rendszeres előadója, offline és online szakmai anyagok szerzője.

Szakvizsgáit tekintve MCSA/MCSE/MCTS, Security és Messaging pluszképesítésekkel is rendelkezik, illetve okleveles Microsoft tréner (MCT). 2004. január óta – Magyarországon az első körben és immár negyedszer újraválasztva – MVP *(Most Valuable Professional)*, azaz a Microsoft Corporation szakmai díjazottja.

Kedvenc szakterületei közé tartozik az ISA Server, a WSUS, a Vista és a Windows Server 2008, valamint a béta szoftverek.

Nős, angol-történelem szakos pedagógus feleségével valamint öt gyermekével Cegléden él.

Szabó Levente

Szakmai gyakorlatát az IBM Magyarországnál szerezte, majd 2000-től egy pénzügyi részvénytársaság rendszergazdája és informatikai vezetője, valamint ellátja a holdinghoz tartozó több cég informatikai teendőit is.

A 2004 végén indult Windows Portal (http://winportal.net) internetes szakmai lap alapítója és főszerkesztője, melynek kapcsán, az online közösségért végzett munkájáért a Microsoft 2007 áprilisától MVP *(Most Valuable Professional)* címmel jutalmazta.

Szakterülete az asztali PC-ken és mobileszközökben használt Windows operációs rendszerek beható tanulmányozása, valamint a legújabb béta szoftverek tesztelése. Kedvencei közé tartozik a Vista és a rendszer biztonsági megoldásaival kapcsolatos témák.

Szerényi László

1995 óta foglalkozik Windows kiszolgálók és ügyfélgépek üzemeltetésével. Jelenleg az Országos Meteorológiai Szolgálatnál dolgozik, mint Windows rendszerekért felelős rendszergazda. Számtalan fordítás fűződik a nevéhez [szakcikkek, tanulmányok, a Neumann János: Számítógép és az agy című könyve (NetAcademia, 2006) stb.], és rendszeresen publikál különféle témájú szakmai írásokat, elsősorban a rendszerfelügyelet automatizálásnak lehetőségeivel kapcsolatban. Társszerzője a Small Business Server 2003 című nagy sikerű szakkönyvnek.

Kedvenc szakterületei közé tartoznak a különféle rendszerfelügyeleti feladatok automatizálásával kapcsolatos eszközök (VBScript, PowerShell, .NET Framework, WMI, ADSI, stb.).

Nős, feleségével és tízéves lányával Budapesten él.

Felelős kiadó: a SZAK Kiadó Kft. ügyvezetője
Felelős szerkesztő: Kis Ádám
Tördelő: Mamira György
Borítóterv: Flórián Gábor (Typoézis Kft.)
Terjedelem 27 (B5) ív.
Készült az OOK Press Nyomdában (Veszprém)
Felelős vezető: Szathmáry Attila