Rendszeradminisztráció

Harsáczki András

MÉDIAINFORMATIKAI KIADVÁNYOK

Rendszeradminisztráció

Harsáczki András

Eger, 2013

Korszerű információtechnológiai szakok magyarországi adaptációja

TÁMOP-4.1.2-A/1-11/1-2011-0021

Lektorálta:
Nyugat-magyarországi Egyetem Regionális Pedagógiai Szolgáltató és Kutató Központ

Felelős kiadó: dr. Kis-Tóth Lajos
Készült: az Eszterházy Károly Főiskola nyomdájában, Egerben
Vezető: Kérészy László
Műszaki szerkesztő: Nagy Sándorné

Tartalom

1 BEVEZETÉS

1.1 CÉLKITŰZÉSEK, KOMPETENCIÁK A TANTÁRGY TELJESÍTÉSÉNEK FELTÉTELEI

1.1.1 Célkitűzés

A tananyag a rendszeradminisztráció tantárgy tematikájával összhangban tárgyalja a Microsoft Windows Server 2008 R2 kiszolgáló és a Windows 7 kliens operációs rendszer vállalati szintű informatikai rendszerek tervezésében és építésében nyújtott számos lehetőségének alkalmazását, valamint ezen lehetőségek mind elméleti, mind gyakorlati ismereteinek megfelelő mélységű elsajátítására tesz kísérletet.

A tantárgy célja, hogy a hallgató a legmodernebb hálózati operációs rendszerek telepítését, beállításait, üzemeltetését és karbantartását kellő mélységben megismerje, valamint ezeket a tevékenységeket megfelelő biztonsággal végre is tudja hajtani. Fontos, hogy átlássa egy rendszer felépítését és működését, továbbá maga is képes legyen önállóan rendszerek tervezésére, valamint ezeknek a rendszereknek a telepítésére, beállítására, kivitelezésére. Meg kell ismernie a különböző rendszerek migrációját és ezeket tudnia kell alkalmazni is. Képesnek kell lennie a különböző típusú problémák, hibák felismerésére, megfelelő kezelésére (illetve ha szükséges és lehetséges, akkor javítására), mind a szoftver, mind a hardver vonatkozásában. A szakterületéhez kapcsolódóan legyen képes az információk hatékony keresésére, sokoldalú hálózati kommunikációra, adatok, információk elektronikus kezelésére, valamint mindig legyen kész a legújabb technológiák, szoftverek befogadására és kipróbálására, valamint azok megfelelő alkalmazására.

1.1.2 Kompetenciák

- Az élethosszig tartó tanulást megalapozó kompetenciák fejlesztése
- Modern rendszerek és eszközök teljes körű használata és az erre való nyitottság
- Fejlődőképesség, önfejlesztés, új ötletek, megoldások kipróbálása
- Készségek és képességek fejlesztése az informatikai rendszerek üzemeltetéshez szükséges tudásbázis felhasználásával

- A megszerzett ismeretek használata modern oktatási környezetben

Tudás:

- Ismerni fogja a legelterjedtebb és legmodernebb hálózati operációs rendszereket, azoknak működését, valamint a kliens-szerver architektúrát
- Képes lesz a különböző címtár alapú rendszereket tervezni, üzemeltetni és karbantartani
- Át tud tekinteni egy vállalati rendszert, és ezen keresztül megérti a vállalati felépítését.
- Tudja hasznosítani megszerzett ismereteit a mindennapi élete és a későbbi tanulmányai, munkája során

Attitűdök/nézetek:

- A rendszerek tervezéséhez, kialakításához, működtetéséhez és továbbfejlesztéséhez szükséges kompetenciák kialakulása.
- Fel kell ismernie a problémákat és képesnek kell lennie ezeknek a problémáknak a megoldására.

Képességek:

- A személyes kompetenciái közül kiemelt szerepet kap a szervezőkészség, az önállóság és a döntésképesség.
- A kognitív kompetencia területén fejlesztenie kell az információfeldolgozó-képességét
- El kell sajátítania a különböző, a témakörhöz kapcsolódó hardverek és szoftverek kezelését.

1.1.1 A tantárgy teljesítésének feltételei

A képzés végén a hallgató képes lesz kisebb cégek, szervezetek informatikai rendszerének megtervezésére és megépítésére, különös tekintettel a címtár infrastruktúra megfelelő alkalmazására, valamint az azt használó kiszolgáló-alkalmazások telepítésére és működtetésére. Megismeri az üzemeltetés és a karbantartás legfontosabb összetevőit, és megfelelően tudja alkalmazni azokat az egész szervezetet lefedő felhasználói adminisztrációtól a hozzáférésvezérlésen keresztül egészen a csoportházirend szerkesztésig.

Jól el tud igazodni a virtualizációs technológia nyújtotta lehetőségek között és megfelelően tudja majd alkalmazni azokat a tervezés és kivitelezés folyamatában.

A tantárgy gyakorlati jeggyel zárul, melynek megszerzéséhez két projektmunka elkészítése a hozzáférés-vezérlés és biztonság, valamint a címtár témakörből, valamint egy gyakorlati jellegű feladat számítógépen történő órai megoldása is szükséges.

1.2 TANULÁSI TANÁCSOK, TUDNIVALÓK

A tananyag a Microsoft professzionális, a vállalati szférában előszeretettel alkalmazott operációs rendszerein és rendszerszoftverein keresztül mutatja be a hálózat és a címtár-infrastruktúra alkalmazási lehetőségeit. Jó azonban tudni arról, hogy hasonló működésű, funkciójú rendszerek más szoftvertermékekből is építhetők, akár nyílt forráskódú szoftverek segítségével is. Az alapelvek és az alkalmazott szabványok ugyanis több rendszerben is implementálva vannak.

Az informatika ezen területe ugyan igényli az elméleti háttér megfelelő ismeretét, azonban tagadhatatlan, hogy erősen gyakorlatias tudást igényel, továbbá nem nélkülözi a kreativitást és a problémamegoldó készséget sem. Ezen készségek és képességek megfelelő mélységű kifejlesztése, a gyakorlatias gondolkodás elsajátítása, a bonyolultabb rendszerek problémáival való gyakoribb találkozással és a probléma megoldással egyenes arányban nő.

Fontos tisztázni, hogy az itt elsajátított ismeretek gyorsan elavulttá válhatnak, hiszen 4-5 évente újabb operációs rendszer verzió kerül kiadásra, amelyben számos újdonság mellől már több, korábban alkalmazott elem kikerült elavultsága miatt. A tananyag a Windows Server 2008 R2 és a Windows 7 operációs rendszerekre épít, azonban éppen e tananyag születésének napjaiban jelenik meg a Windows 8 és nem sokkal később a Windows Server 2012 is. Ezért nagyon fontos, hogy a hallgató a kurzus elvégzése után is figyeljen ismeretei frissítésére.

2 TELEPÍTÉS, FRISSÍTÉS, MIGRÁCIÓ

2.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Ebben a leckében a Windows operációs rendszerek fejlődésének gyors történeti áttekintése után a Windows Server 2008 és Windows Server 2008 R2 újdonságainak rövid ismertetési következik. A tankönyvben található gyakorlati példák egy speciális virtuális környezetben lesznek létrehozva, ennek megértéséhez ismertetésre kerül a virtualizáció fogalma és az alkalmazandó virtualizációs környezet. Ebben a környezetben történik majd az operációs rendszerek telepítése, frissítése és migrációja.

A hallgató a lecke végén ismerni fogja a virtualizáció fogalmát, képes lesz ilyen környezetek kialakítására az Oracle VirtualBox virtualizációs szoftvere segítségével. Ismerni fogja a legújabb Microsoft Windows operációs rendszereket, és meg tudja különböztetni ezek kiadásait. Képes lesz ezeket a rendszereket telepíteni, illetve régebbi rendszerekről a legújabbra frissíteni, migrálni.

2.2 TANANYAG

2.2.1 Egy kis történelem

A Microsoft Corporation csaknem húsz éve van jelen a szerver operációs rendszerek piacán és ez a húsz év elegendő volt arra, hogy a nagyvállalati rendszerek gyártói között az egyik legnagyobbá nője ki magát. Ez nem is lehetett annyira bonyolult, hiszen az asztali gépek legelterjedtebb operációs rendszere mindig is a Microsoft Windows nevű terméke volt. Egyszerűen készíteni kellett egy olyan szerver operációs rendszert, amelynek szolgáltatásai tökéletesen illeszkedtek a munkaállomások Windows rendszeréhez, illetve kiegészítették, teljesebbé tették azt.

A történet 1988-ban kezdődött, amikor a Microsoft egy új 32 bites operációs rendszer fejlesztésére kérte fel a Digital Equipment Corporation fejlesztő csapatát. Az új rendszer nem az addig is létező MS-DOS és az arra épülő MS Windows aktuális verzióinak továbbfejlesztése akart lenni, hanem egy teljesen új alapokról induló operációs rendszer. Ez tükröződött a rendszer nevében is: Windows NT (New Technology – új technológia). Az áttörést az addigra hihetetlen népszerűségnek örvendő Windows 95 GUI-jával (Graphical User Interface – grafikus felhasználói felület) közel azonos felülettel rendelkező Windows NT 4.0 hozta 1996-ban. A könnyű kezelhetőség és a stabilitás párosítása segített a

rendszernek a nagyvállalati környezetben történő elterjedéséhez, míg az otthoni felhasználók inkább maradtak a megbízhatatlan, ámde rugalmas Windows 95-nél és utódainál (Windows 9x sorozat).[1]

A Windows NT már akkor is kétféle változatban jelent meg: Server és Workstation. Kódbázisuk azonos volt, de amíg a szerver (Server) változattal települő összetevők tartalmazták a különböző kiszolgáló szoftvereket, illetve a rendszer kimondottan kiszolgáló működésre volt „hangolva", addig a kliens (Workstation) változat valóban munkaállomásnak készült.

A következő verzió a Windows 2000 volt (NT 5.0 verzió), amelynek két változata a Server és a Professional. Az utóbbi változat megpróbálta a Windows 9x vonal szerepét átvenni, és ez részben sikerült is neki. A nagy áttörést azonban nem a Windows 2000 Professional hozta a kliens (munkaállomás) operációs rendszereknél, hanem a 2001-ben megjelent Windows XP (eXPerience – élmény, NT 5.1 verzió), amely ezzel a legnépszerűbb asztali operációs rendszerré vált és végképp lezárta a hagyományos Windows 9x vonalat. Ezzel együtt elindította azt a trendet, miszerint a szerver és kliens változatok kiadása időben elvált egymástól. A szerver változat hatalmas újdonsága az Active Directory (AD – aktív címtár) megjelenése volt, amely attól kezdve a Windows kiszolgálók infrastruktúrájának alapját képezi. Innentől jelennek meg a szerverváltozat különböző kiadásai is, amely a különböző licenszek számában és árában, valamint más kiegészítő szolgáltatásokban térnek el egymástól (Server, Advanced Server, Datacenter Server).

Az XP megjelenése után - amely szintén több kiadásban jelent meg (Home Edition, Professional, Mediacenter Edition) - két évvel kijött a szerver változat is, amely a Windows Server 2003 nevet viselte (NT 5.2 verzió) és számos újdonsággal rendelkezett elődjéhez képest. Kiadásait új nevekkel látták el, illetve bővítették a kiadások számát is. Ekkor jelenik meg a Web Server kiadás, valamint a Standard és az Enterprise új elnevezésű kiadások is a már létező Datacenter mellett, amely kiadások azóta is minden verziónál megjelennek. Fontos még szót ejteni az ún. SBS kiadásról is (Small Business Server), amely kisvállalkozásoknak készült és valójában egy Standard kiadás Exchange levelező kiszolgálóval és egyéb apróságokkal. Ez a kiadás is megjelenik a későbbiekben is.[2]

---

[1] Sting: 20 éves a Windows - történelmi áttekintést az elmúlt két évtizedről. Online cikk, PC Fórum, 2005 <http://pcforum.hu/cikkek/115/20+eves+a+Windows-tortenelmi+attekintest+az+elmult+ket+evtizedrol.html>, 2012.09.11

[2] Wikipedia: A Microsoft Windows története. Online enciklopédia, Wikipedia, 2004-2012 <http://hu.wikipedia.org/wiki/A_Microsoft_Windows_t%C3%B6rt%C3%A9nete>, 2012.09.11

A két évvel később megjelenő Windows Server 2003 R2 (Release 2 – második kiadás) több újdonságot is hozott, bár ugyanazon a kódbázison alapul, mint elődje és az NT verziószámozásban ugyanúgy az 5.2-es számot viseli.

A következő kliens verzió nem aratott túl nagy sikert, kvázi megbukott. A felhasználók panaszkodtak a hatalmas erőforrásigényére, és a vállalatok sem akarták egész gépparkjukat lecserélni egy új rendszer bevezetése miatt. Pedig a Windows Vista már a 6.0-ás NT verzió volt, így rengeteg újdonsággal rendelkezett, de úgy tűnt azok még kiforratlanok. A Windows Server 2008 bő 1 év múlva követte a klienst. Kódbázisa a Vista SP1-gyel azonos (Service Pack – szerviz csomag), így automatikusan tartalmazza a Vista SP1 olyan újdonságait, mint az újraírt hálózatkezelés, a lemezkép alapú telepítés, vagy akár az olyan új biztonsági funkciók, mint a Bitlocker meghajtótitkosítás vagy az ASLR (Address Space Layout Randomization), a véletlenszerű címterület-kiosztás.

A 6.1-es verziójú Windows Server 2008 R2 2009 nyarán jelent meg, kódbázisa az ugyanabban az évben ősszel megjelenő Windows 7 asztali gépekre szánt operációs rendszerével egyezik meg, és ezzel sikerült a gyártónak megint szinkronba hozni a szerver és a kliens változatok kiadását.[3]

2.2.2 A Windows Server 2008 és a Windows Server 2008 R2 legfontosabb újdonságai

A Windows Server 2008 az előző Windows 2003 R2 verzióhoz képest óriási változott. A legalapvetőbb hardverkezeléstől a hálózat és a biztonság kezelésén keresztül a felhasználói felületig szinte mindenen változtattak.

Nagy fejlődésen ment keresztül a kiszolgálókezelő (Server Manager), amely a rendszergazda első számú eszköze az üzemeltetésben. Ez tulajdonképpen a rendszerfelügyelet komponenseinek központi kezelő eszköze egy MMC konzolba integrálva, praktikusan, hogy minden megtalálható legyen egy helyen. A Windows Server 2008-ban már a szerepkörök és szolgáltatások telepítését, törlését, konfigurálását illetve ellenőrzését ezen keresztül tehetjük meg, továbbá elérhetjük a diagnosztika több elemét is, mindezt kombinálva akár távoli eléréssel is.

A címtárszolgáltatás fejlesztése 2003-ban sem állt le, hiszen a Windows szervereken alapuló hálózatok megkerülhetetlen alapja. Az erőforrások (felhasználók, számítógépek stb.) megbízható tárolásán és kezelésén kívül a fontosabb szerveralkalmazások is erre épülnek (pl. csoportházirend). A Windows Server 2008-ban olyan újdonságok jelentek meg, mint a csak olvasható tarto-

3 GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

mányvezérlő (RODC – Read-Only Domain Controller), vagy az újraindítható címtárszolgáltatás, valamint sokat fejlődött a csoportházirend is.

A telepítő indulásakor látható, hogy minden kiadáshoz létezik egy Server Core változat is, amely úgy telepíti a kiválasztott kiadást, hogy csak a szükséges összetevőket tartalmazza GUI, azaz grafikus felület nélkül. Ez azért nagyon jó dolog, mert a GUI futtatása sok erőforrást emészt fel fölöslegesen és természetesen több a hibalehetőség is. A Server Core változatok kezelése kizárólag parancssoros környezetben történik. Itt kell megemlíteni a Power Shell (v1.0) nevű parancsértelmezőt, amely biztosítja azokat az eszközöket, melyek segítségével egy Server Core változat is könnyen kezelhetővé válik.

Ha Windows szerverekről beszélünk, egy rendszergazdának mindig eszébe jut a hálózati biztonság kérdése. A NAP (Network Access Protection) olyan megoldás, amely csak a biztonságosnak tekinthető számítógépeket engedi a hálózathoz csatlakozni, ezáltal próbálja megakadályozni, hogy a nem megbízható klienseken keresztül illetéktelenek hozzáférhessenek a szerverhez.

Ha új Windows szerver, akkor új webkiszolgáló. Ez a trend itt sem szakadt meg. Az IIS 7-ről (Internet Information Services 7.0) mindenkinek csak egy webkiszolgáló jut eszébe, pedig sokkal több annál, hiszen olyan jól konfigurálható, egyszerűen felügyelhető, biztonságos modularizált platform, amely webalkalmazások és webszolgáltatások üzemeltetésére és fejlesztésére is használható.

További újdonságok jelentek meg a terminálszolgáltatások és a virtualizáció területén is. A terminálszolgáltatások között olyan új fejlesztések találhatók meg, mint a Web Access, a Terminal Service Gateway, az Easy Printing vagy a RemoteApp. A virtualizáció ebben az esetben Hyper-V hypervisort jelenti, mely integráltan található meg a Windows Server 2008-ban és segítségével jobban kihasználhatók a hardver erőforrásai.[4]

A Windows Server 2008 R2 verzióban a hardveres támogatástól a címtáron keresztül a felügyeletig minden területen hatalmas fejlesztések történtek. A hardveres támogatásnál talán a legfontosabb, hogy csak kizárólag 64 bites változat készült, de megemlítendő a legfeljebb 256 logikai processzor vagy a SLAT (Second Level Address Translation) támogatás. Ez utóbbi a virtualizációnál használatos és a CPU kihasználtság optimalizációján alapul. A szerverekre nem igen jellemző az energiatakarékos jelző, hiszen folyamatos működést igényelnek, azonban a Windows Server 2008 R2-be sikerült olyan újításokat meglépni, mint pl. a processzor magok ki és bekapcsolása attól függően, hogy szükség van-e rájuk.

[4] GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

Az újonnan megjelenő címtárszolgáltatások közül talán az Active Directory felügyeleti központ (Active Directory Administrative Center – ADAC) a legfontosabb, amely egy teljesen önálló webszolgáltatás (tehát nem az IIS része), és rajta keresztül gyakorlatilag minden címtár funkció elérhető. Meg kell említeni továbbá a kliensek offline beléptetését a tartományba, vagy az AD lomtárat, illetve a csoportházirend fejlesztéseit.

A felügyeleti eszközök közül a kiszolgálókezelő újdonságait érdemes megemlíteni, valamint a Power Shell 2.0-t, amely a Windows Server 2008 R2-től kezdve már olyan összetevőket is támogat, mint az AD vagy az IIS.

Ezenkívül a hálózati szolgáltatások fejlesztése illetve a terminálszolgáltatások (Terminal Services) átnevezése távoli asztali szolgáltatásokra (Remote Desktop Services – RD) érdemel figyelmet. Utóbbi olyan új megoldással is rendelkezik, mint a Hyper-V-vel és az Active Directoryval együttműködő VDI (Virtual Desktop Infrastructure) támogatása. A VDI központi szervereken található virtuális számítógépek futtatását és felügyeletét teszi lehetővé olyan eszközökön keresztül, mint pl. a RD Web Access).

Látszik, hogy a Windows Server 2008 R2 nem csak egy javítócsomaggal ellátott második kiadás, hanem annál sokkal több. Mivel azonban mindent tud, amit az elődje, a továbbiakban csak ez a változat kerül ismertetésre.[5]

2.2.3 Az alkalmazott virtualizációs technológia

Manapság már alig akad olyan informatikai fogalom, amely ne állna valamilyen kapcsolatban a virtualizációval. Az emberek virtuális valóságról beszélgetnek virtuális barátaikkal egy virtuális közösségben, amelyet egy olyan alkalmazás működtet, amely egy virtuális számítógépen fut, és virtuális tárhelyeken tárolja el azokat a fényképeket, amelyeket mások virtuális hálózatokon keresztül érhetnek el és tölthetnek le, és teszik mindezt egy virtuális térben.

Virtualizáció

A tananyagban a virtualizáció elsősorban a virtuális számítógépek, röviden virtuális gépek (Virtual Machine – VM), és az azokat összekötő virtuális hálózatok használatát jelenti. A virtuális gépen futó operációs rendszer természetesen virtuális lemezekről (Virtual Disk) indul, és ha a sok alkalmazás túl lassan fut rajta, akkor gombnyomásra még több virtuális memóriával és virtuális processzorral lehet bővíteni a rendszert. Nem nehéz belátni, hogy a virtualizációnak számtalan előnye van, de ki kell emelni, hogy az oktatás szempontjából, azon belül is az operációs rendszerek, a hálózatok, valamint a fejlesztés szempontjá-

[5] GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

ból ez az előny kimagasló. A virtualizáció segítségével ugyanis lehetségessé válik olyan tanulási és teszt környezetek megalkotása, amelyhez régen rengeteg hardvert kellett volna megvásárolni. Egy egyszerűbb kliens - szerver hálózati architektúra az ember saját közepes kategóriájú számítógépén is lemodellezhető. Talán meg sem kell említeni, hogy ez mekkora előrelépés az ezredfordulói állapotokhoz képest.

Számítógép a számítógépben

A virtualizációnak számos definíciója létezik. Attól függően, hogy a virtualizáció mely területe fontosabb valamilyen szempontból valakinek, definíciójában azt a területet állítja előtérbe. Ebben a tankönyvben elsősorban a platformvirtualizáció (annak is kétféle megközelítése) kerül ismertetésre. Az első megközelítés - amely valahol a második speciális esete is egyben - a virtualizációnak a tananyagban elfoglalt segítő szerepére utal:

> **A virtualizáció szűkebb értelemben egy adott fizikai számítógépen (hardveren) futó egy vagy több emulált számítógépet jelent.**

Ezt egyébként teljes virtualizációnak is nevezhetjük, mivel a módszer az egész számítógépet emulálja, nem csak egy részét. A másik definíció a platformvirtualizáció egy jóval általánosabb megfogalmazása:

> **A virtualizáció egy olyan rendszer vagy köztes réteg, amelynek segítségével az egy helyre koncentrált erőforrás elemek szabadon, tetszés és igény szerint újraoszthatók a réteg felett létrehozott logikai rendszer entitások között.**

Ez gyakorlatilag azt jelenti, hogy a különböző hardvererőforrásokat, pl. számítógépeket, processzorokat, merevlemezeket, memóriát össze lehet úgy fogni egy **készletbe** (Pool), hogy azokat egy köztes réteggel elrejtve (amely réteg maga a virtualizációs rendszer), azok transzparens módon újraoszthatóak legyenek a réteg felett elhelyezkedő virtuális gépek számára. Tulajdonképpen a virtualizáció lényege nem más, mint az absztrakció.

A platform virtualizáción belül sokféle létezik, amelyek legfőképp a virtualizációt megvalósító technikában különböznek:

- **Szoftveres:** amelynél az utasítások vizsgálata után a problémás utasításokat a rendszer transzformálja más utasításokra, a nem problémásokat pedig közvetlenül végrehajtatja a processzorral. (Az x86-os architektúránál ezt bináris fordításnak (Binary Translation) nevezik. Itt kell megemlíteni a tiszta emulációt is, amikor minden utasítás transzformálásra

kerül. Ebben az esetben azonban különböző platformokat is emulálhat a rendszer.).

- **Para-virtualizáció:** amely a virtuális gépen futó operációs rendszer olyan módosításán alapul, hogy az már eleve ne is akarjon problémás utasításokat futtatni. A problémás utasításokat tartalmazó függvényhívások helyett módosított függvényeket hívjon meg, amelyet a virtualizációt megvalósító szoftver hajt majd végre.
- **Hardveresen támogatott virtualizáció:** ahol a processzor támogatja a virtualizációt, megoldást adva a problémás utasítások és azok következményeinek kezelésére.

Arra lehetne gondolni, hogy a hardveres megoldás nyújthatja a legjobb teljesítményt, de ezt jelenleg egyértelműen nem lehet kijelenteni, hiszen egyrészt ez függ a terheléstől és a környezettől, valamint nem szabad elfelejteni, hogy több éves lemaradásban van a másik két technológiához képest. Éppen ezért a különböző virtualizációs szoftverek ezeknek valamilyen keverékét használják. A jövőben azonban valószínűleg a helyére fog kerülni a hardveres támogatás technikája is.

A platform virtualizációs szoftvereknek, a virtuális gépeket kezelő rendszernek (Virtual Machine Monitor – VMM) alapvetően kétféle megvalósítása létezik. Az egyiket hosted („gazdagépes”), míg a másikat bare-metal („csupasz vas”) virtualizációnak nevezzük. A kettő közötti lényeges különbség, hogy míg a hosted virtualizáció esetében a hardver erőforrásokat a gazdagépen (Host) futó operációs rendszer (Host OS) kezeli, addig a bare-metal virtualizációs esetében ez a VMM feladata. Bare-metal virtualizáció esetén a VMM-et, amely gyakorlatilag egy speciális operációs rendszer gyakran hypervisornak neveznek. A hosted virtualizációnál a VM-et Guest-nek (vendég) is hívják az azon futó operációs rendszert pedig vendég operációs rendszernek (Guest OS).

Hosted rendszerek például olyan VMware rendszerek, mint a Workstation, Server és a Player, de ide soroljuk az Oracle (Sun) VirtualBox-ot, MS VirtualPC-t, a KVM-et (Kernel Based Virtual Machine), és az UML-t (User Mode Linux).

Bare-metal rendszerek közül a legfontosabbak a VMWare ESXi, a Xen, és az MS Hyper-V.

VirtualBox

A VirtualBox fejlesztését a német Innotek GmbH kezdte el, amelyet 2008-ban vásárolt fel a Sun Microsystem Inc. Két évvel később, 2010-ben az Oracle felvásárolta a Sun-t innentől kezdve Oracle Virtualbox a neve a terméknek, amely egy szabad szoftver. Ahogy már említésre került a VirtualBox egy hosted

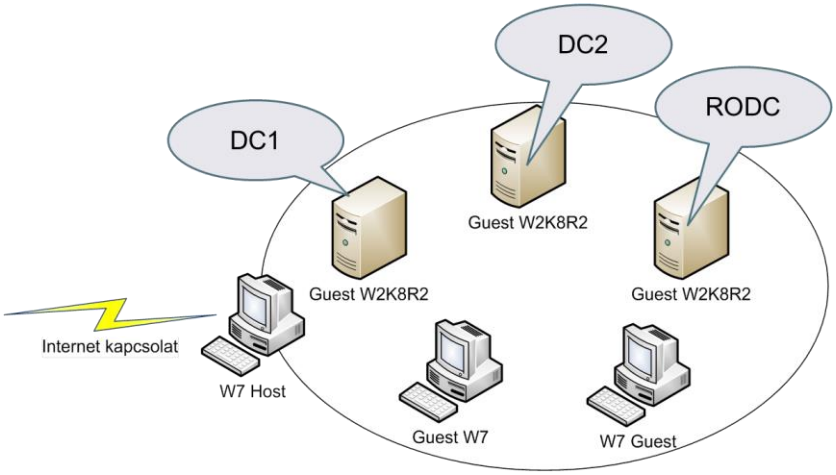
típusú VMM, amely szoftveres és hardveres virtualizációt is használ, és Windows, Mac, Linux és Solaris operációs rendszereken tud futni. Vendég operációs rendszer szinte bármi lehet az x86-as platformon Windows, Linux, Mac, BSD, vagy akár DOS vagy OS/2 is, a lista nem teljes.[6]

Fontos tudni a VirtualBox esetében (és a legtöbb virtualizációs rendszernél is), hogy x64 (vagy amd64) architektúra (azaz az Intel x86 64 bites tovább fejlesztését) virtualizációja csak hardveresen megoldott, azaz ha nem áll rendelkezésre olyan számítógép, amely processzora 64 bites és támogatja a virtualizációt (Intel VT-x, AMD-V), akkor 64 bites operációs rendszereket nem lehet rá telepíteni. (Ebben az esetben ez azért fontos, mert a Windows Server 2008 R2-ből már csak 64 bites verzió létezik.)

A létrehozandó virtualizált környezet és feltételei

A tankönyvben bemutatott példák gyakorlati kivitelezéséhez először létre kell hozni egy olyan virtuális környezetet, amely alkalmas egy kis cég hálózatának szimulálásához. Ehhez először is szükség van egy hardveres virtualizációt támogató processzorral ellátott számítógépre, amelyen legalább 64 bites Windows 7 van telepítve. (Elméletileg megengedhető lenne más gazda operációs rendszer is, de a tankönyv példái, feladatai a fent említett környezetben lettek kipróbálva, más rendszerben nem lehet garantálni működésüket.) Szükséges még, hogy a gazdaszámítógép lehetőleg legalább 4GB memóriával, valamint legalább 100GB szabad hellyel rendelkezzen a virtuális lemezek számára, hiszen egyszerre egy időben több virtuális gépnek is futnia kell. A kialakítandó hálózati infrastruktúra internetkapcsolatot és egy virtuális helyi hálózatot feltételez, amelyet a VirtualBox Host-Only Network virtuális hálózat fog szimulálni, amely átjárójának szerepét a gazda Windows 7 fogja ellátni a fizikai Ethernet interfészével az internet és egy virtuális, ún. VirtualBox Host-Only Ethernet Adapter hálózati interfésszel a belső, virtuális, helyi hálózat felé.

[6] Wikipedia: VirtualBox. Online enciklopédia, Wikipédia, 2007-2012 <http://en.wikipedia.org/wiki/VirtualBox>, 2012.09.13



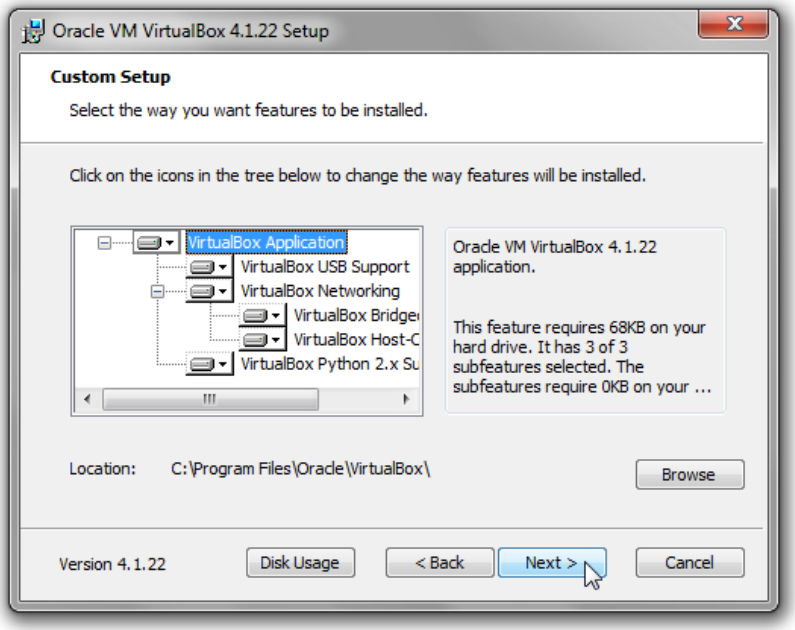
1. ábra: A kialakítandó virtuális környezet

A VirtualBox telepítése

A telepítő csomag letölthető a VirtualBox weboldaláról a Downloads menüből (https://www.virtualbox.org/wiki/Downloads). Itt a VirtualBox 4.1.22 for Windows hosts **x86/amd64** linkre kattintva a telepítő csomag letöltődik. A telepítő csomag megnyitása után a **futtatás** (Run) gombra kell kattintani mire a telepítő elindul.

2. ábra: Indulhat a telepítés

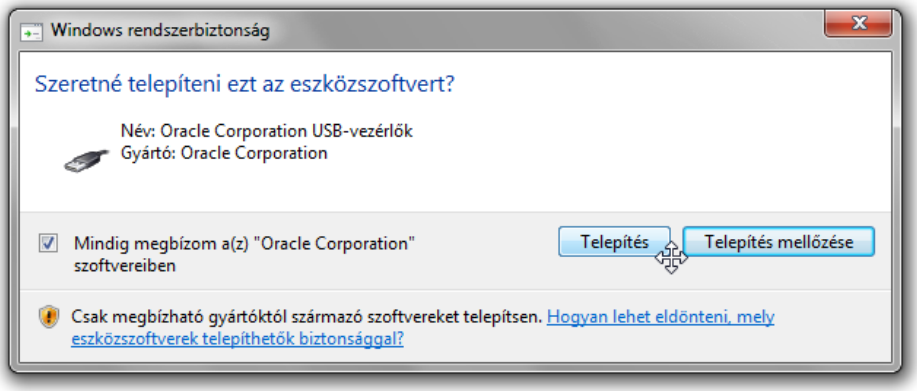
Az üdvözlő képernyőn a **Next** (következő) gombra kell kattintva megjelennek a **telepítendő összetevők** (features will be installed), illetve a telepítés **helye** (Location). Az alapértelmezett beállításokat meghagyva a **Next** (következő) gombra kattintva a parancsikonok létrehozásáról lehet dönteni. Itt is maradhatnak az előre beállított értékek, csak a **következő** (Next) gombra kell kattintani.



3. ábra: Alapértelmezett beállításokkal folytatódik a telepítés

A következő ablakon egy figyelmeztető üzenet olvasható, amely szerint a VirtualBox hálózati összetevőinek telepítése közben a hálózati kapcsolat ideiglenesen megszakadhat. Abban az esetben, ha a hálózati kapcsolat megszakadása kritikus lenne, érdemes lehet a folytatásra a **nem** (No) gombot választani, majd egy későbbi időpontban újra megpróbálni a telepítést. Természetesen az esetek nagy többségében nem szokott gondot okozni, ha pár másodpercre megszakad a hálózati kapcsolat, ilyen esetben az **igent** (Yes) kell választani.

A megjelenő ablakon még van lehetőség visszalépni, ha valamit módosítani kell, de általában ilyenkor az **telepít** (Install) a megfelelő választás. Ezután megkezdődik a VirtualBox telepítése, amely 1-2 percig eltarthat, függően a gép sebességétől.



4. ábra: Megbízható szoftver?

A telepítés közben felugrik egy **Windows rendszerbiztonság** ablak, amely az Oracle Corporation által készített eszközillesztő szoftver telepítésére kérdez rá. Érdemes itt kipipálni a mindig megbízom az Oracle Corporation szoftvereiben kapcsolót, majd a **telepítés** (Install) gombra kell kattintani. Ezt a „megbízást" azért is érdemes bekapcsolni, mert lesz a telepítés során egy pár illesztőprogram, amelynek telepítésekor hasonló ablak ugrik fel, ha ez a lépés kimaradt.

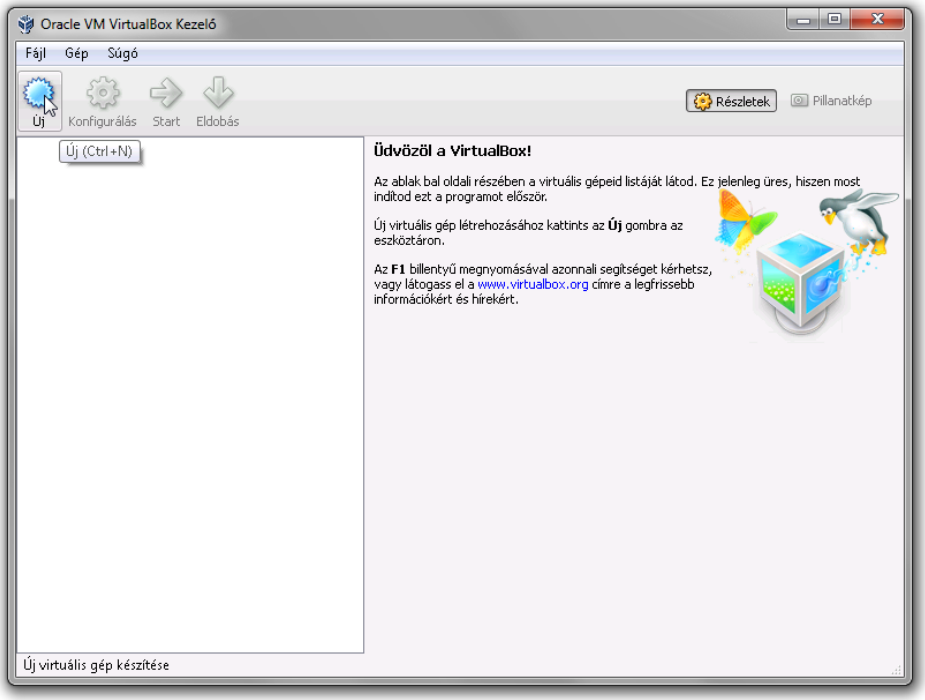
5. ábra: A telepítés vége

A telepítés utolsó lépéseként választható, hogy a telepítő bezárásával egyidejűleg elinduljon-e a VirtualBox. Ha ez nem lenne bekapcsolva, a Start menüből, vagy az elhelyezett parancsikonoktól függően akár az asztalról is elindítható lesz később a VirtualBox.

1.1.2 A virtualizációs környezet

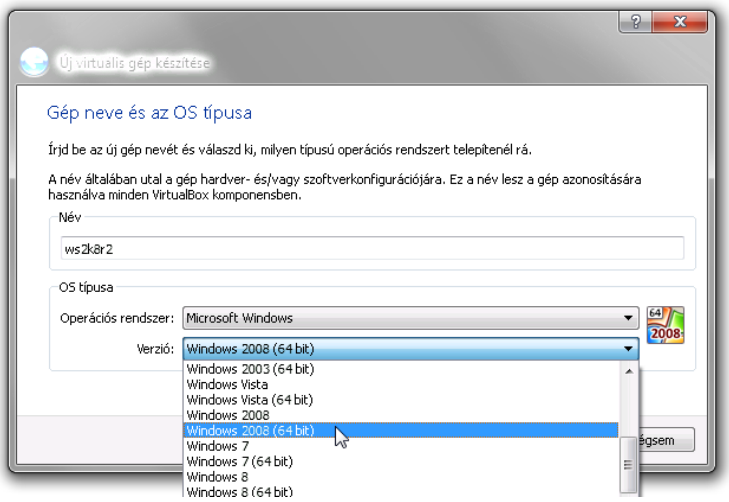
VM létrehozása a VirtualBox kezelőben

A megjelenő ablak **Oracle VM VirtualBox Kezelőként** aposztrofálja magát, a tankönyvben azonban az elkövetkezendőben csak virtuális gépkezelőnek, VM-kezelőnek, vagy röviden VMM-nek lesz nevezve.



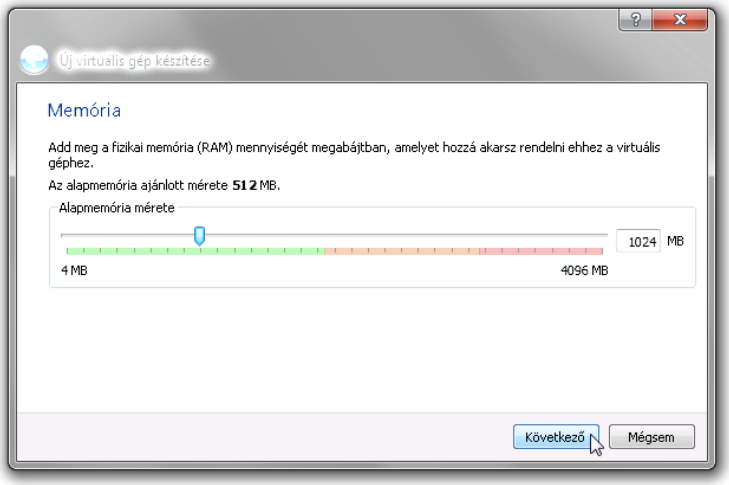
6. ábra: Új VM létrehozása

Új virtuális gép létrehozásához az **új** (New) gombra kell kattintani az eszköztárban, melynek hatására elindul az új virtuális gép varázsló, melynek **következő** (Next) gombjára kattintva meg lehet adni a virtuális gép nevét, illetve ki lehet választani a vendég operációs rendszer típusát és verzióját. (Itt a gép neve ws2k8r2, az operációs rendszer Microsoft Windows, a verzió pedig Windows 2008 (64 bit).)



7. ábra: A VM neve és típusa

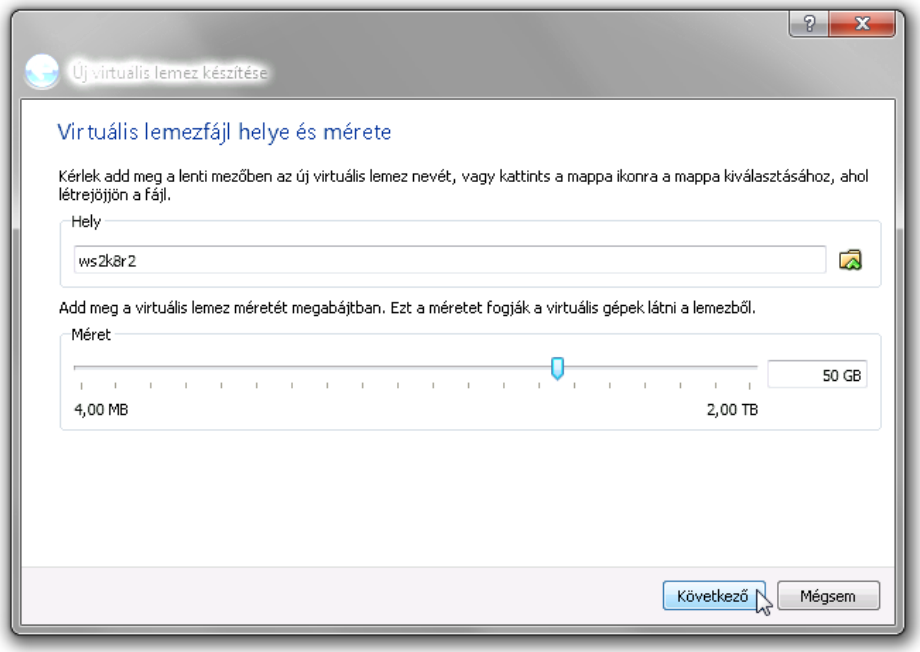
A **következő** (Next) gombra kattintva a virtuális gép memóriájának mennyiségét lehet beállítani egy csuszka segítségével, de akár be is írható számokkal a csuszka jobb oldalán elhelyezkedő mezőbe. A megfelelő érték beállítása utána a **következő** (Next) gombra kell kattintani. (Windows Server 2008 R2 esetén a minimális érték 1024MB, itt is ez van beállítva. Figyelembe kell továbbá venni természetesen a gazdagépben található RAM mennyiségét is.)



8. ábra: A memória mennyisége

A következő párbeszédablakban a virtuális merevlemez beállításait lehet megadni. Ha a VM több virtuális lemezzel is fog rendelkezni, akkor is legalább az egyiknek **indítólemeznek** (Boot Disk) kell lennie, ugyanúgy, mint valós környezetben is. Új virtuális merevlemez létrehozása helyett választható már létező virtuális merevlemez is. Több olyan eset is előfordulhat, amikor ilyesmire van szükség. (A tananyagban használt virtuális gépek mind csak egy virtuális merevlemezzel rendelkeznek, amelyek egyben természetesen indító lemezek is.)

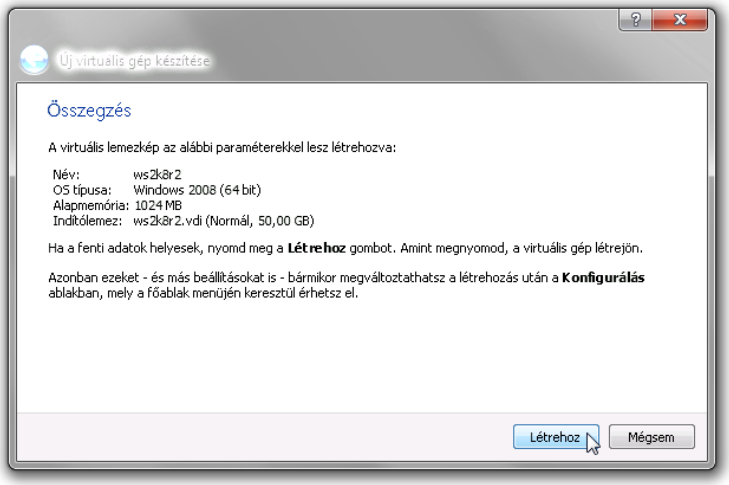
A **következő** (Next) gombra kattintva a megjelenő párbeszédablakon a virtuális lemez típusát lehet megadni. Itt érdemes a VirtualBox lemezkép típust választani, majd a **következő** (Next) gombra kell kattintani.



9. ábra: Virtuális lemezképfájl és helye

A megjelenő ablakban a virtuális lemezfájl méretét és helyét lehet megadni. A hely alapértelmezetten a felhasználó saját mappájában található „VirtualBox VMs” mappa egy a virtuális gép előzőleg megadott nevével azonos nevű almappája. Ebben a mappában fognak tárolódni a VM-hez tartozó más fájlok is. Az alapértelmezett értékek elfogadása után a **következő** (Next) gombra kell kattintani.

A létrehozás utolsó két lépésében két összegző panel látható. Az első a létrehozandó virtuális merevlemezre, a második pedig az egész VM-re vonatkozik. Mindkét panelen a **létrehozás** (Create) gombbal lehet nyugtázni a műveleteket.



10. ábra: Kész.

A VMM-ben megjelenik a bal oldali sávban az új VM ikonja és neve, valamint állapota, amelynek értéke jelenleg **kikapcsolva** (Powered Off). Az új VM indítása előtt érdemes pár dolgot megnézni a beállítások között, arról nem is beszélve, hogy a megfelelő hálózati környezet létrehozásához az alapértelmezett hálózati konfigurációt is módosítani kell.

VM konfigurálása a VirtualBox kezelőben

Ha a VM ki van jelölve, akkor a jobb oldalon láthatóvá válnak a különböző beállítások több szakaszra bontva. Az **általános** beállítások között a VM neve és az operációs rendszer típusa látható.

A **rendszer** szakaszban látszik a memória mennyisége, az indítási sorrend, hogy melyik eszközről induljon a virtuális gép, illetve a különböző gyorsítási hardvertámogatások.

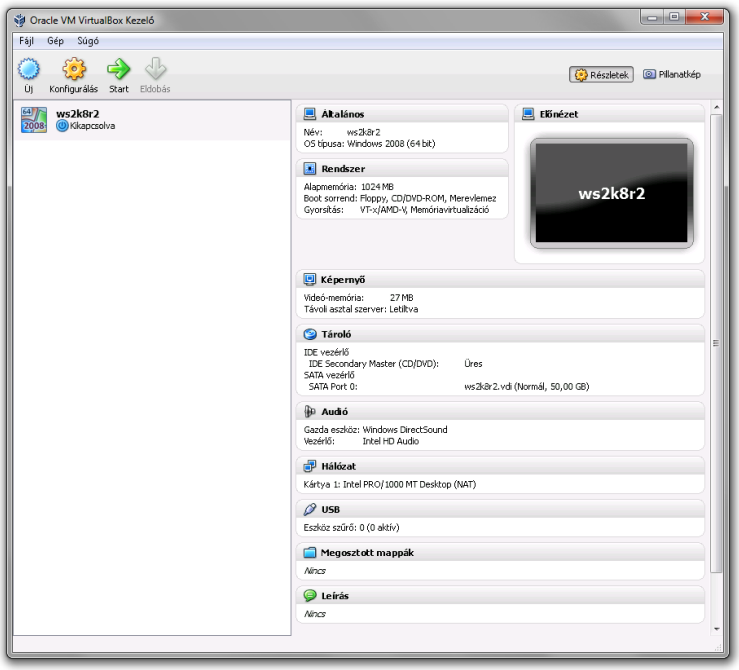
A **képernyő** szakaszban a videomemória mérete és a távoli asztal szerver állapota látszik. Ez utóbbi egy VNC (Virtual Network Computing) szerver segítségével grafikusan is elérhetővé teszi távolról a virtuális gépet.

A **tároló** szekcióban láthatók a virtuális IDE és SATA vezérlők, amelyekhez olyan különböző eszközök csatlakoztathatók, mint a virtuális CD/DVD meghajtó, amelyhez egy CD/DVD ISO képfájlt csatolható, de lehetőség van a gazda gép

CD/DVD meghajtóit is csatolni az eszközhöz. Természetesen ide csatlakoznak a virtuális merevlemezek is, itt lehet látni azt is, hogy melyik és milyen vezérlőhöz vannak csatolva.

Az **audió** szakaszban a gazda és a vendég hangeszközök látszanak. A hálózat szakaszban a használt virtuális hálózati kártyák (interfészek) és azok típusai és működési módjai láthatók. Az USB szakaszban látható, hogy a vendég géphez hány USB eszköz csatlakozik Ezeket az USB eszközöket a gazdagépre csatlakozó USB eszközök közül lehet kiválasztani, de nagy körültekintést igényel, mert abban az esetben ha a VM aktiválódik az USB eszköz a gazdagépről leválasztásra kerül és ez akár adatvesztést is okozhat pl. egy pendrive, vagy usb-s merevlemez esetén.

A **megosztott mappák** szakaszban látszik a megosztott mappák száma. Ezek a mappák olyan mappák a gazdagép fájlrendszerében, amelyek a vendég operációs rendszerből is látszanak, ha a vendég operációs rendszer támogatja az SMB megosztások csatlakoztatását. Ez Windows vendég esetében a Microsoft Networks ügyfél meglétét jelenti, amely alapértelmezetten az operációs rendszer része.



11. ábra: A VM beállításai

A **konfigurálás** (Settings) gombra, vagy a jobb oldalon a konfigurálandó szekció nevére kattintva megjelenik a **beállítások** (Settings) ablak. A teljesség igénye nélkül, csak a tananyagban előforduló konfigurációs módosítások beállításait tekintve az első a **rendszer** szakasz. Ebben a tananyag szempontjából fontos beállítási lehetőség az alaplap adatlapon található memória mennyiség csuszka, illetve az **indítási** (Boot) sorrend. Ez utóbbinál csak a kipipált eszközök vehetnek részt az indítási folyamatban méghozzá olyan sorrendben, ahogyan látszanak. A sorrend a kerettől jobbra található le és fel nyilas gombokkal állítható be úgy, hogy a kijelölt eszköz mozgatható le és fel a nyilas gombok segítségével. A processzor és gyorsítás adatlapokon a processzorok számát illetve a különböző hardvertámogatásokat lehet beállítani.

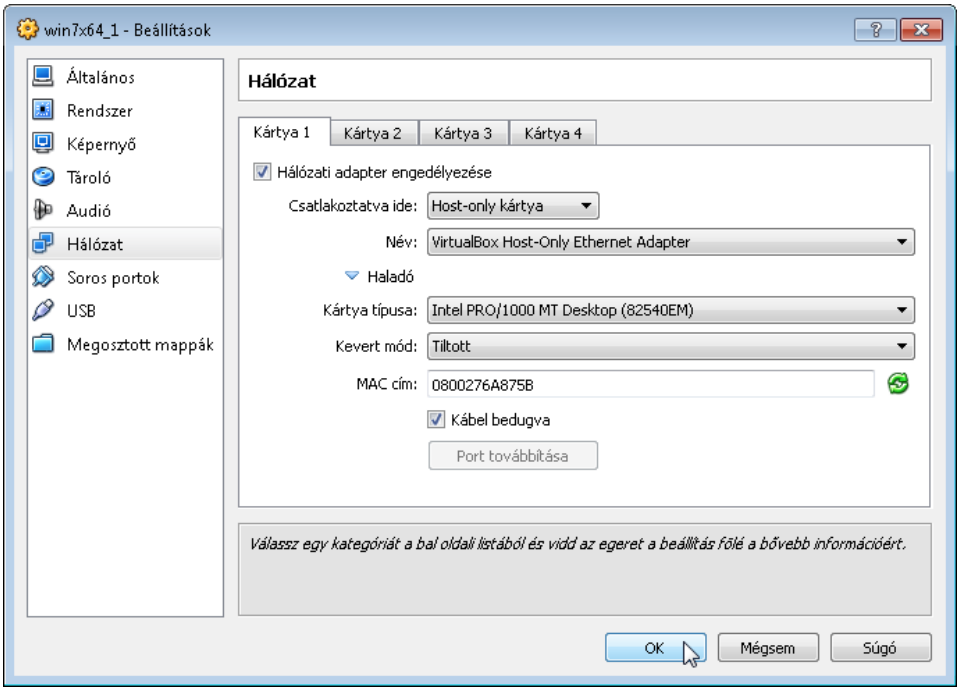
A **tároló** szakaszban állítható, hogy mely CD/DVD lemezkép legyen a virtuális CD/DVD meghajtóhoz csatlakoztatva. Ehhez ki kell jelölni a CD lemez ikonját, majd a bal oldalon, a paraméterek résznél a CD/DVD meghajtó mellett található CD ikonra kell kattintani. A megjelenő listából a már egyszer használt ISO lemezképek választhatók ki, de lehet újabbakat tallózni, a gazda meghajtóit csatolni, vagy a jelenleg felcsatolt lemezt vagy lemezképet leválasztani. Ebben a szakaszban lehet továbbá új virtuális lemezeket csatolni, létrehozni, akár új és más típusú virtuális merevlemez-vezérlő segítségével.

A **hálózat** szakaszban a tananyagban kialakítandó virtuális hálózat szempontjából igen fontos konfigurációs lépéseket kell megtenni. A VirtualBox legfeljebb 8 virtuális hálózati kártyát (interfészt, adapter) tud kezelni virtuális gépenként, bár első ránézésre csak 4 kártyának látjuk a tulajdonságlapját. A tankönyvben leírt VM-ek csak egyet használnak, és ez az esetek legnagyobb részében elegendő is.

Az első kártya beállításai közül megemlítendő a hálózati adapter engedélyezése jelölő négyzet, amellyel engedélyezni vagy letiltani lehet a kártyát a VM-ben. A hálózati csatlakozás helye már több állítási lehetőséget kínál. Itt azt lehet megadni, hogy a hálózati interfész milyen hálózathoz csatlakozzon.

A **hálózati címfordítás** (Network Address Translation – NAT) az alapértelmezett érték minden engedélyezett hálózati interfész esetén. Ez azt jelenti, hogy a gazdagép és a vendég gépek között egy virtuális router foglal helyet, amely egyben egy NAT képes eszköz is, és elvégzi a címfordítást. A vendég operációs rendszerek ebben az esetben biztonsági okokból el vannak szeparálva egymástól. Az IP konfiguráció azonban teljesen automatikus, melyet egy **beépitett dinamikus host konfigurációs protokoll** (Dynamic Host Configuration Protocol – DHCP) kiszolgáló végez. Előnye, hogy az automatikus konfiguráció és a NAT router funkció miatt a vendég rendszeren azonnal használható hálózati kapcsolata (valamint ha a gazdagépnek van internetkapcsolata, akkor internet-

kapcsolata is) lesz. Nem véletlen, hogy ez az alapértelmezett. Azonban ha a cél valamilyen kiszolgáló építése virtualizált környezetben, akkor probléma lehet a VM külső hálózatokból (vagy akár az internet felől) történő elérésével. Ezen valamelyest segíthet a porttovábbítás (port forwarding) technika, de ez különböző okok miatt nem minden esetben kivitelezhető.



12. ábra: Host Only beállítása a VM konfigurációjában

A külső elérést a legkönnyebben a **bridge-elt kártya** (Bridged Adapter) típusú interfésszel lehet elérni, hiszen ilyenkor ugyanabban a hálózatban lesz a virtuális interfész, mint a gazdagép hálózati kártyája. Ezt valahogy úgy kell elképzelni, mintha a VMM-ben egy virtuális **híd** vagy **kapcsoló** eszköz (bridge/switch) került volna be a gazda fizikai kártyája és a gazda OS hálózati kártyája közé, amihez mind a fizikai kártya, mind a gazda és mind vendég rendszer kártyája is csatlakozna. Előnye, hogy mind a gazdagépről, mind külső hálózatokból (akár az internetről is) elérhetővé válik a VM. Hátránya, viszont, hogy ha a hálózatban nincs DHCP kiszolgáló, akkor az IP konfigurációt kézzel kell beállítani.

Nem csak a könyvben alkalmazott technológia miatt fontos, de amiatt mindenképp tárgyalandó a **Host-Only kártya** (Host-Only Adapter) csatlakozási típus, amelynek segítségével egy virtuális helyi hálózatot lehet létrehozni,

amelyhez az összes VM ugyanilyen csatlakozású interfésszel csatlakozhat, ráadásul még a gazdagép is kap egy ilyen interfészt, azaz a VM-ek és a gazda operációs rendszere is láthatják egymást. Előnye, hogy ebben a hálózatban is működik a VMM DHCP kiszolgálója, amit mellesleg akár ki is lehet kapcsolni, mint ahogy erre a későbbiekben szükség is lesz. Hátránya, hogy alapból ezek a VM-ek nem érhetők el a külső hálózatból (vagy az internet felől), és ők sem érnek el semmit a gazdagépen túli hálózatokból. Az erre vonatkozó megoldást a 3. fejezetben tárgyalja a tankönyv.

2.2.4 A telepítés előtt

A telepítés megkezdése előtt több kérdés is felvetődhet. Az első talán az, hogy a telepítendő számítógép hardverelemeit támogatja-e az új operációs rendszer. Ez legkönnyebben Microsoft hardver kompatibilitási listájának (Hardware Compatibility List – HCL)[7] weboldalán deríthető ki, ahol egy kereső funkcióval közvetlenül az eszköz nevét megadva, vagy akár eszköz kategóriánként keresve megtudható, hogy az adott hardverelem támogatott-e, vagy sem.

A következő kérdés, hogy teljesen új rendszert kell-e üzembe helyezni, vagy egy már létező rendszer egy részét vagy egészét kell telepíteni, frissíteni illetve migrálni. A legegyszerűbb eset, amikor teljesen új rendszert kell építeni, és elég egy, esetleg két szervert üzembe helyezni. Természetesen egy új rendszer építése esetén a helyzetet nagyban bonyolítja, ha nem csak egy-két szerver lesz üzembe állítva, hanem jóval több, mert például a vállalat több telephellyel is rendelkezik, amelyek valamilyen hálózati, gyakran internetkapcsolaton keresztül vannak összekötve egymással. Ezért a tervezés általában megelőzi a telepítést, annak ellenére, hogy a 2008-as szerver (és az R2 is természetesen) az alap operációs rendszer telepítésekor nem teszi kötelezővé a különböző szerver komponensek telepítését, azok később bármikor telepíthetők és konfigurálhatók.

Kicsit nehezebb a helyzet, amikor létező rendszert kell frissíteni. Ekkor eldönthető, hogy ún. „helyben frissítés” történjen, vagy inkább egy **tiszta telepítés** (Clean Install) egy új hardverre, majd pedig a régi létező szerver összes beállításának migrálása a tisztán telepített új rendszerre. Ez utóbbi talán gyakoribb és jobb megoldás is, hiszen elég arra gondolni, hogy pl. a Windows Server 2003 R2-t futtató hardver nem fog olyan hatékonysággal megbirkózni a Windows Server 2008 R2-vel, hiszen a két szoftver kiadása között eltelt öt év alatt nem csak a szoftver, de a hardver is igen sokat fejlődött, a régi „vas” pedig elavulttá vált. Azon kívül, hogy a hardver esetleg túl gyenge az új rendszerhez, az is elő-

[7] Microsoft hardver kompatibilitási lista: http://www.microsoft.com/windows/compatibility/windows-7/en-us/default.aspx

fordulhat, hogy néhány hardverelem már nem támogatott, azaz nincs az új rendszerhez megfelelő eszközillesztő program.

Ha sikerült eldönteni, hogy frissítés vagy telepítés és migrálás, vagy „csak telepítés” lesz, akkor a következő kérdés a kiadás kiválasztása. Ebben is segít az előzetes terv készítése, hiszen a kiadások pl. különböző szolgáltatások licensz számában is különböznek, azaz a kifogástalan működéshez helyes méretezés is szükséges. A következő táblázat megmutatja a kiadások közötti különbségeket és egyben segít eldönteni, hogy melyik kiadást érdemes választani.

Features	Web	Foundation	Standard	Enterprise	Datacenter	Itanium
Max RAM	32GB	8GB	32GB	2TB	2TB	2TB
Max CPU	4	1	4	8	64	64
Azonnali RAM bővítés	Nem	Nem	Nem	Igen	Igen	Igen
Azonnali CPU bővítés	Nem	Nem	Nem	Nem	Igen	Igen
Azonnali RAM csere	Nem	Nem	Nem	Nem	Igen	Igen
Azonnali CPU csere	Nem	Nem	Nem	Nem	Igen	Igen
DFS-R	Nem	Nem	Nem	Igen	Igen	Igen
RRAS licensz	Nincs	50	250	korlátlan	korlátlan	Nincs
IAS licensz	Nincs	10	50	korlátlan	korlátlan	2
RDS-GW licensz	Nincs	50	250	korlátlan	korlátlan	Nincs
RD Admin kapcsolatok	2	2	2	2	2	2
Virtualizáció használati jog	Vendég	Nincs	Host+1VM	Host+4VM	korlátlan	korlátlan

1. *Windows Server 2008 R2 kiadások táblázata*

Ugyanezek igazak a kliensekre is, bár itt a migrálásnál egészen más dolgokra kell odafigyelni, hiszen például a hálózati szolgáltatások nagy része a szerveren fut. A kliensek esetében inkább az jelenti a kihívást, hogy a migráció után a felhasználó mennyire fogja magát kiismerni a rendszerben. Azaz ugyanúgy és ugyanott találja-e meg a dokumentumait illetve használandó programjait.

2.2.5 A munkaállomás és szerver operációs rendszerek tiszta telepítése

A telepítés lépései a tiszta telepítés folyamán azonosak a szerver és a munkaállomás esetében. Itt inkább arra kell odafigyelni, hogy egy kiszolgálónál esetleg máshogyan érdemes a tárterületet szétosztani. Előfordulhat, hogy több lemez és/vagy partíció használatára lesz szükség.

A tananyag virtualizált tesztkörnyezetében ez nagyjából úgy fog megvalósulni, hogy a szerver verziók 1 GB virtuális memóriát és 50GB virtuális lemezt használhatnak majd, a munkaállomások pedig ezen értékek felét, azaz 512MB memóriát és 25GB virtuális lemezt. A következő táblázat bemutatja az elkészítendő két VM paramétereit.

Név	CPU	RAM	HDD	OS	Network	IP
dc1-ws2k8r2	1db	1024MB	50GB	Windows Srvr 2008 R2 Ent	Host-only	192.168.1.1
dc2-ws2k8r2	1db	1024MB	50GB	Windows Srvr 2008 R2 Ent	Host-only	192.168.1.2
win7x64	1db	512MB	25GB	Windows 7 Ent	Host-only	DHCP

2. *A létrehozandó VM-ek paramétereit tartalmazó táblázat*

A tiszta telepítést részletező leírás mind két változat esetében megtalálható Kerecsendi András: Hálózati Operációs Rendszerek tankönyvében[8], ezért itt különösebb magyarázat nélkül, a legfontosabb lépéseket érintve kerül csak bemutatásra.

A tiszta telepítés legfontosabb lépései – Windows 7

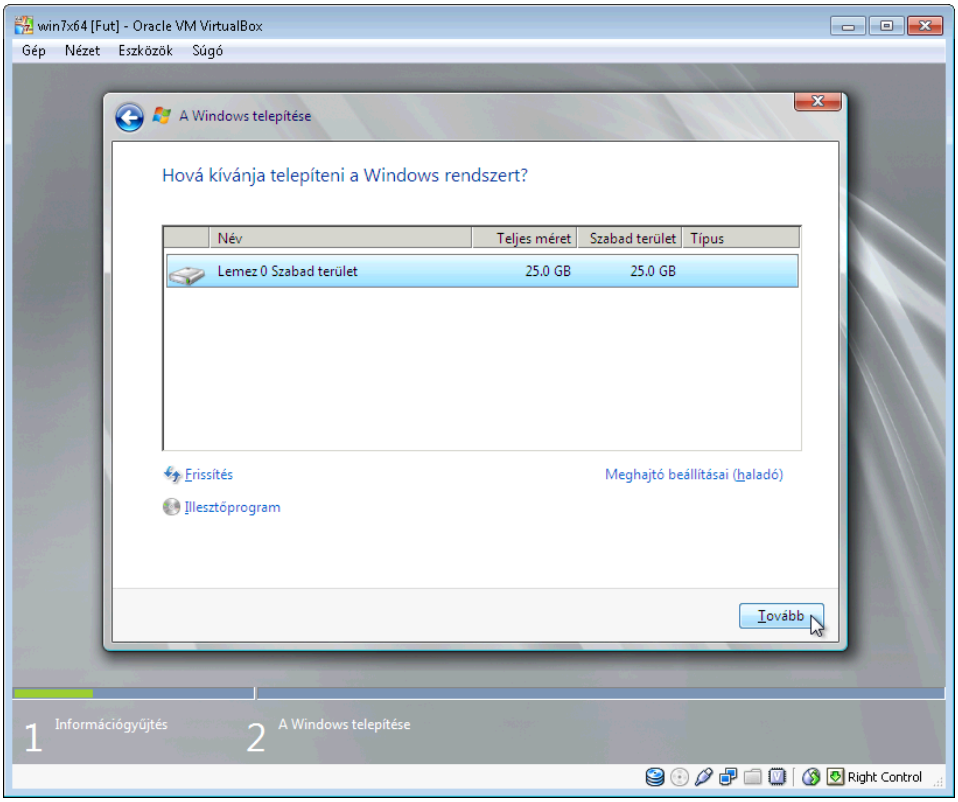
A DVD-ről indítva a számítógépet először a Windows előtelepítési környezet töltődik be, majd elindul a telepítőprogram. Az első beállítások, amelyeket meg kell adni a **telepítendő nyelv** (Language to install), és az olyan a helyi beállítások, mint az **idő és pénznem formátuma** (Time and currency format) vagy a **billentyűzet vagy beviteli módszer** (Keyboard or input method). (Itt mindhárom beállítás esetében az alapértelmezett magyar nyelv van kiválasztva.)

A **tovább** (Next) gombra kattintva megjelenik a Windows 7 telepítő ablaka, amelyen a **telepítés** (Install now) gombra kattintva elindul a telepítés. Ebben az ablakban olvasnivaló is található a telepítésről **a tudnivalók a telepítés előtt** (What to know before installing Windows) szövegre kattintva érhető el, valamint található itt egy **számítógép javítása** (Repair your computer) szöveg is, amelyet sérült, nem induló operációs rendszer esetében célszerű használni.

A következő lépés a **licenszfeltételek** (License terms, End User Licence Agreement – EULA) elolvasása és elfogadása. A szöveg figyelmes elolvasása után, ha elfogadhatóak a feltételek, akkor be kell kapcsolni az **elfogadom a licenszfeltételeket kapcsolót** (I accept the license terms), utána pedig a **tovább** (Next) gombra kell kattintani.

A megjelenő ablakban választani kell a **frissítés** (Upgrade) és az **egyéni (haladó)** (Custom (advanced)) telepítési típus között. A tiszta telepítés ez utóbbihoz tartozik, ezért ezt kell választani. Elbizonytalanodott rendszergazdák **a segítséget kérek a döntéshez** (Help me decide) szövegre kattintva olvashatnak egy-két gondolat erről a dilemmáról.

[8] Kerecsendi András: Hálózati Operációs Rendszerek, Eger, EKF, 2013



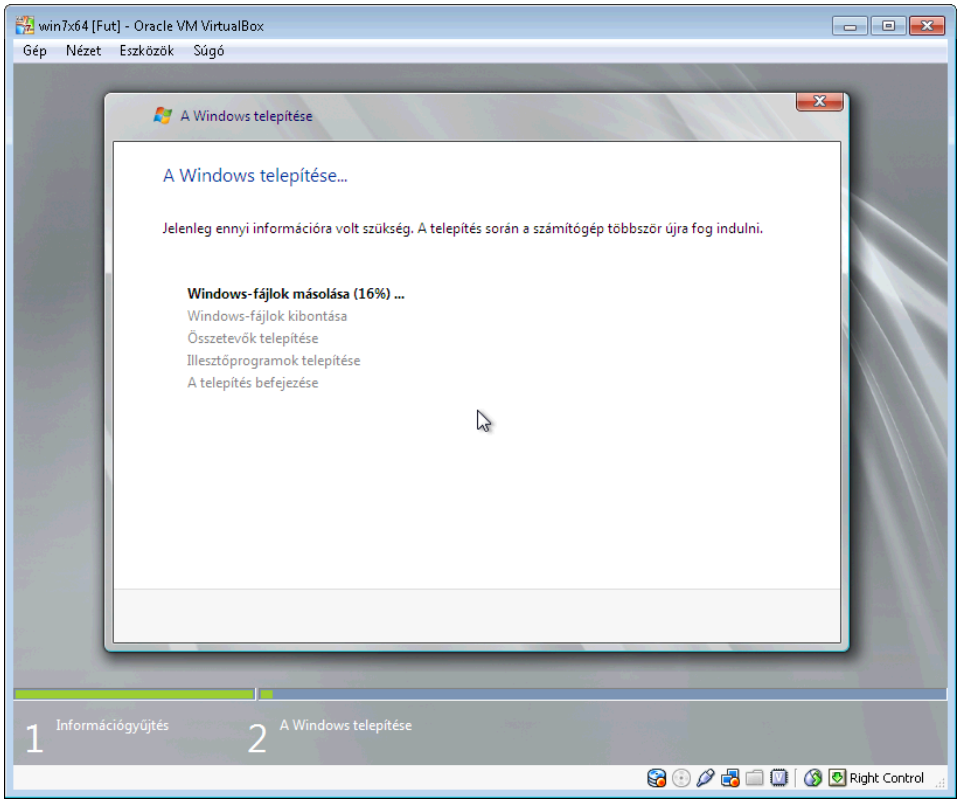
13. ábra: „Hová kívánja telepíteni a Windows rendszert?”

A következő ablakban a telepítés helyét lehet megadni, azaz azt, hogy a Windows operációs rendszert melyik lemez, melyik partíciójára telepítse a telepítő. Itt akár partícionálni is lehet a lemezeket a beépített partícionáló programmal, amely elérhető a **meghajtó beállításai (haladó)** (Drive options (advanced)) szövegre kattintva. Mivel itt most egy tiszta telepítés történik egy lemezre, ezért egyszerűen a **tovább** (Next) gombra kell kattintani. A telepítő ekkor automatikusan partícionálja a lemezt, amelynek során létrehoz egy kisebb 100MB-os partíciót a rendszer számára, a többi lemezterületből pedig létrehoz egy elsődleges partíciót, erre fogja NTFS-re (New Technologie File System – új technológia fájlrendszer) formázás után a Windows operációs rendszert telepíteni.

Előfordulhat, főleg új hardver esetén, hogy a rendszer nem látja a lemezt, mert pl. annyira új a lemezvezérlő, hogy a meghajtóprogramja (illesztőprogram) nem található meg a telepítő lemezen, hiszen amikor az készült, még nem létezett ilyen hardvereszköz. Ilyenkor az **illesztőprogram** (Load Driver) szövegre kattintva van lehetőség az új meghajtóprogram betöltésére pl. USB pendrive-

ról. Miután ez megtörtént, a lemez és a rajta lévő esetleges partíciók megjelennek, és minden ugyanúgy folytatható tovább.

Az ezután következő lépések nem igényelnek közbeavatkozást. A telepítő először formáz, majd fájlokat másol, amelyeket a másolás után kitömörít. Ezután telepíti az összetevőket, illesztő programokat, majd pedig a kiadás óta megjelent frissítéseket. Ezután a számítógép újraindul. Ez az újraindulás elméletileg nem igényel beavatkozást a felhasználótól vagy a rendszergazdától.

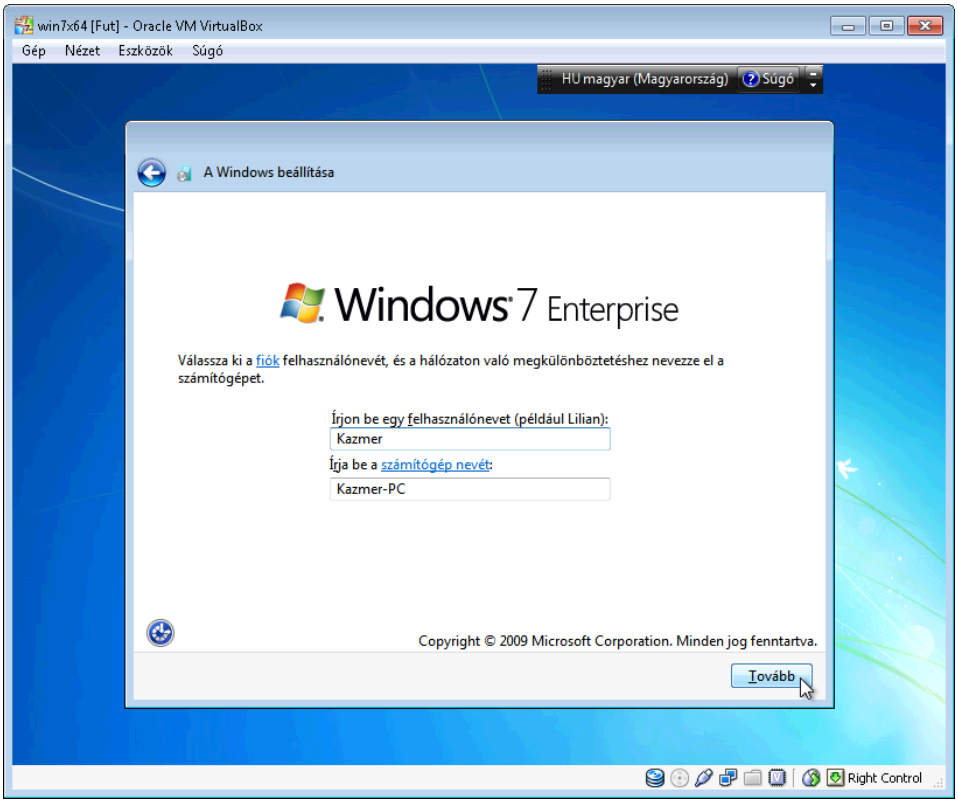


14. ábra: A várakozás ideje

Az újraindítás után az ún. kezdőélmény beállítással folytatódik a telepítés. Az első megjelenő ablakban az első **felhasználó nevét** (user name), valamint a **számítógép nevét** (computer name) kell megadni, majd pedig a **tovább** (Next) gombra kell kattintani. (Itt a felhasználó és a számítógép neve; Kazmer és Kazmer PC.)

A következő párbeszédpanelen meg kell adni az előzőekben megadott felhasználóhoz tartozó **jelszót** (password), illetve egy **jelszó emlékeztetőt**

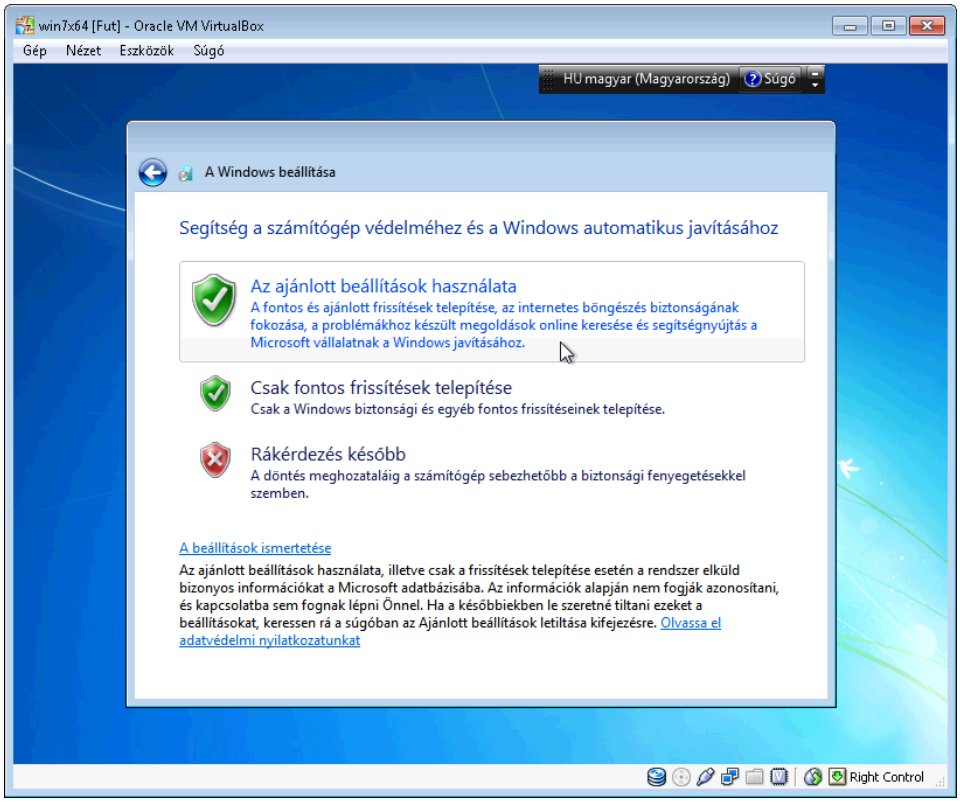
(password hint). Ezzel a felhasználóval lehet majd a rendszert használni, ugyanis az automatikusan létrejövő rendszergazda (Administrator) és vendég (Guest) felhasználók letiltva maradnak.



15. ábra: Kinek a gépe?

A Windows 7 kiadások nagy részénél a telepítés következő képernyőjén a **termékkulcsot** (Product Key) kell megadni, amely az enterprise verzió esetében elmarad.

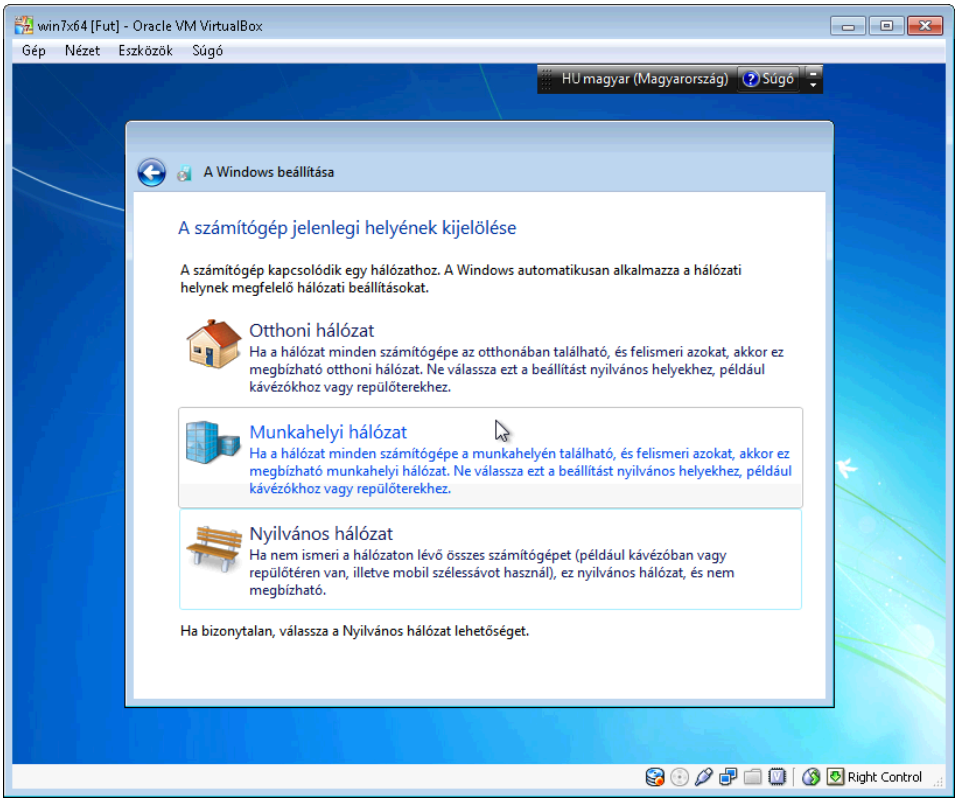
Ezután még néhány egyszerű beállítás következik. Elsőként a számítógép biztonsági beállításai jönnek. Általában a három lehetőség közül az **ajánlott beállításokat** (Use recommended settings) érdemes választani néhány speciális esettől eltekintve.



16. ábra: Az ajánlott beállításokat érdemes választani

Kiválasztása után az **időzóna** (Time zone), a nyári időszámításra való automatikus áttérés (Automatically adjust clock for Daylight Saving Time), a **dátum** (Date) és az **idő** (Time) beállítása következik. Ha minden rendben van a számítógéppel, akkor általában itt elég a **tovább** (Next) gombra kattintani.

Az utolsó beállítási lehetőség a hálózati kapcsolat helyének megadása. A három különböző választási lehetőség, melyek rendre az **otthoni hálózat** (Home network), **munkahelyi hálózat** (Work network), **nyilvános hálózat** (Public network) három különböző hálózati biztonsági sémát jelent, hiszen könnyen belátható, hogy pl. egy kávézóban nyílt wifi hozzáférést használó laptop, és egy tűzfal rendszerrel védett munkahelyi hálózatba kötött, állandóan karbantartott asztali gép különböző védelmet igényel.

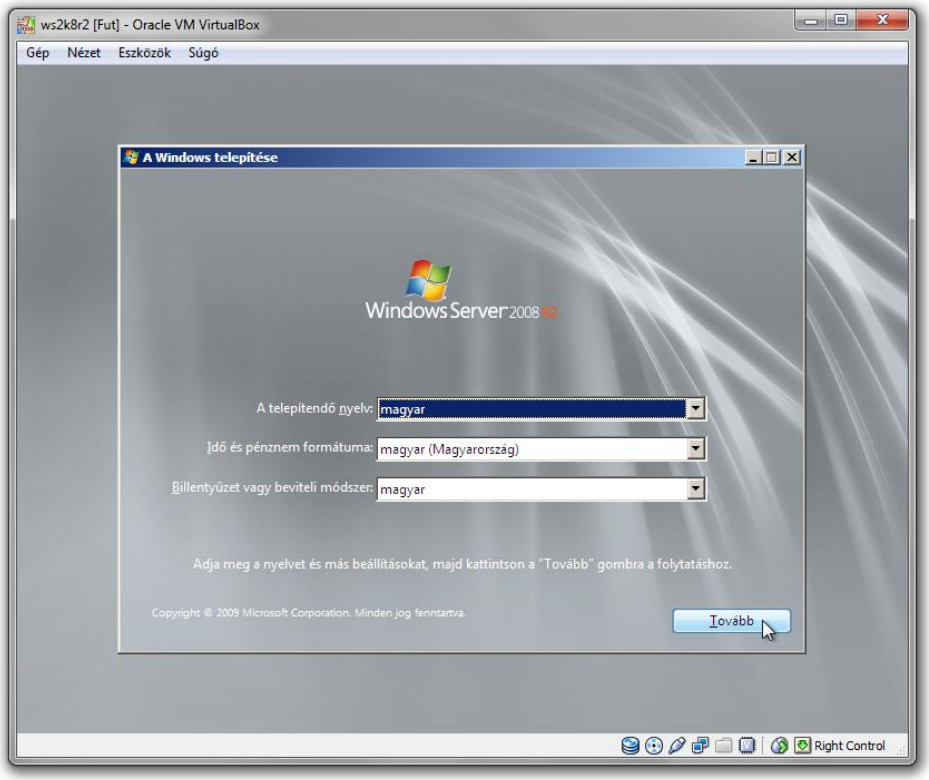


17. ábra: Munkahelyen munkahelyit

Ezek után a rendszer beléptetve a megadott felhasználót működésre készen áll.

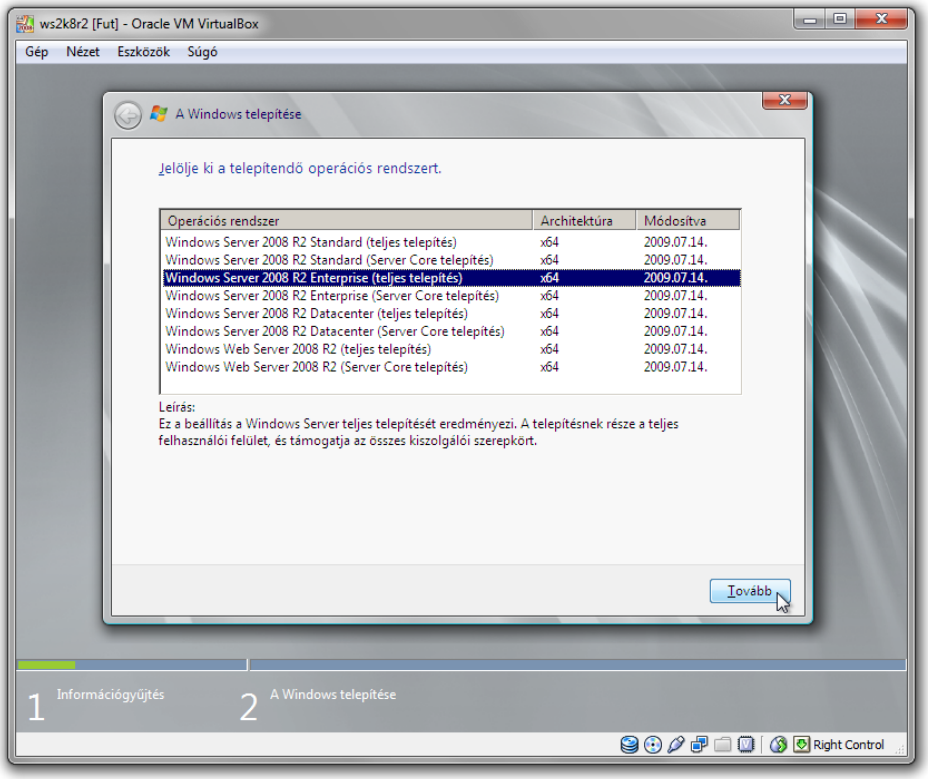
A tiszta telepítés legfontosabb lépései – Windows Server 2008 R2

Mint már említésre került a kiszolgáló és a munkaállomás változatok telepítése szinte teljesen megegyezik, ezért itt csak a különbségek lesznek említve.



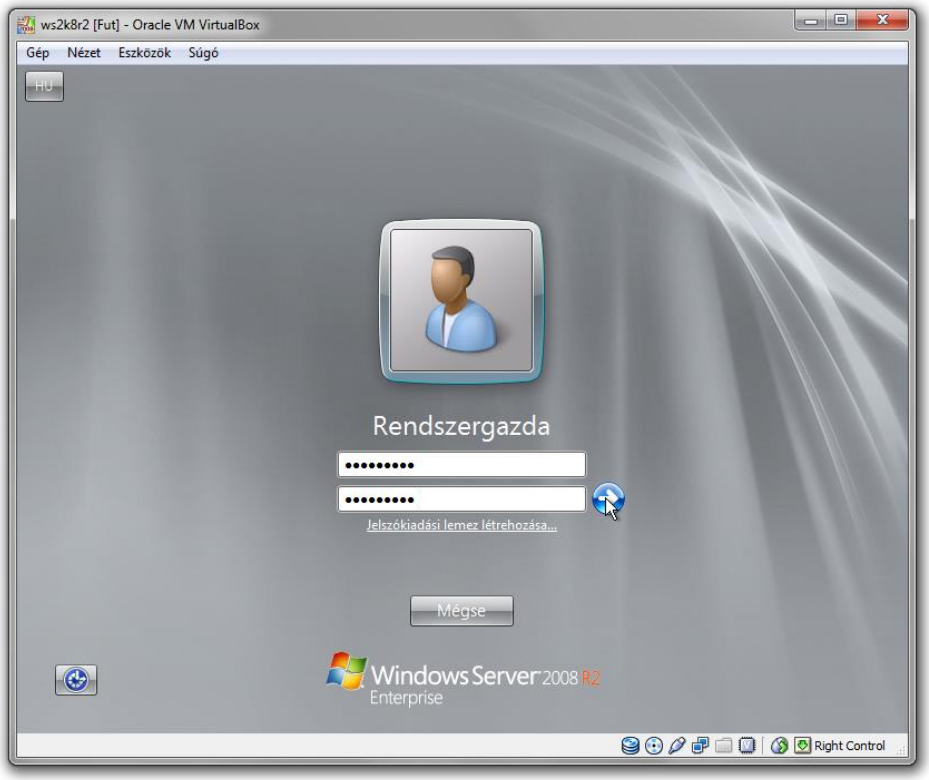
18. ábra: Indulhat a telepítés, de milyen nyelven?

Az első különbség a telepítő indulása és a **telepítés** (Install Now) gombra való kattintás után jön, amikor megjelenik a jelölje ki a **telepítendő operációs rendszert** (Select the operating system you want to install) ablak, ahol a Windows Server különböző kiadásai közül lehet választani, mert a telepítő médián található telepítési képfájl minden kiadást tartalmaz. A tervezésnek megfelelő kiadás választása után a **tovább** (Next) gombra kell kattintani. (Ebben az esetben a Windows Server 2008 R2 Enterprise (teljes telepítés) x64 architektúra.)



19. ábra: Természetesen Enterprise (teljes)

A következő említendő különbség már a rendszer első indításánál és beállításánál jelentkezik: itt nem kell egy felhasználó nevet és számítógépnevet megadni. E helyett a **Rendszergazda** (Administrator) felhasználó jelszavát kell a jelszóházirendnek megfelelően megváltoztatni. Ez egyelőre annyit jelent, hogy legalább 8 karakter hosszúnak kell lennie, tartalmaznia kell minimum 2-2-2 kisbetűt, nagybetűt és számjegyet.

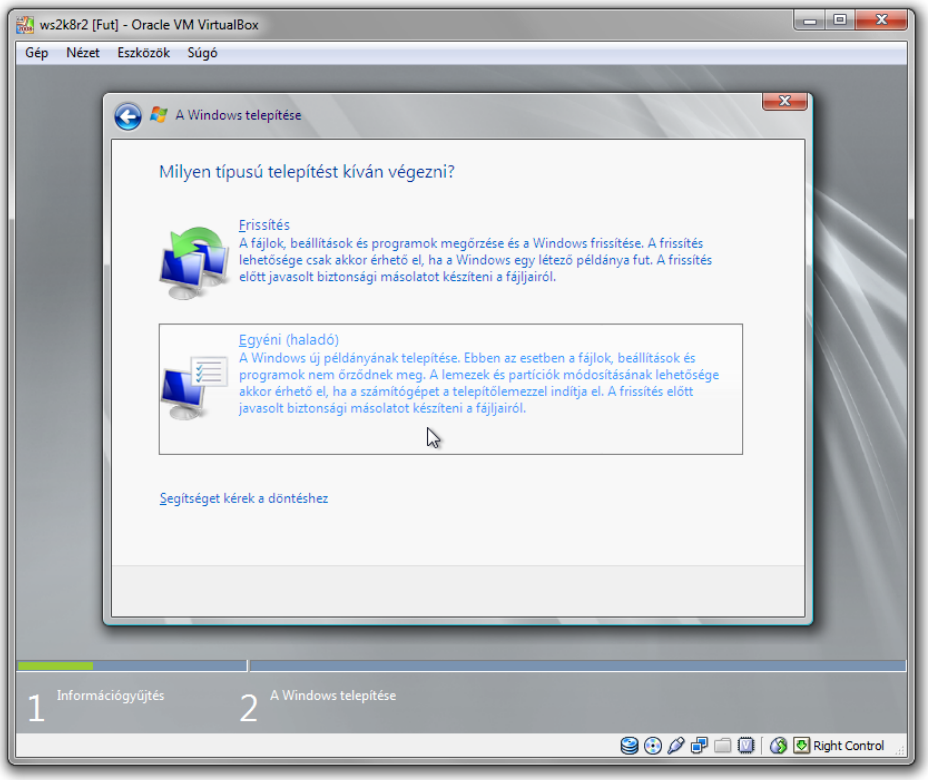


20. ábra: A megfelelő jelszó megadása

Ezzel kész is a telepítés, nincs további beállítási lehetőség. A fontosabb konfigurációs lépéseket a már működő rendszeren kell megtenni, amelyekről a későbbi fejezetekben lesz szó.

2.2.6 Frissítés vagy migráció?

Ha a számítógépen telepítve van egy korábbi Windows verzió, akkor a legújabb verziót bizonyos esetekben ún. **helyben frissítéssel** (In-place Upgrade) is fel lehet telepíteni. Ez azt jelenti, hogy az előző Windows verzióban telepített programok, beállítások megmaradnak és a telepítés után már nem kell ezekkel többet bíbelődni. Ha a helyben frissítés valamilyen okból nem megoldható, de lenne igény a beállítások átvitelére, akkor marad a **tiszta telepítés** (Clean Install), amely után jöhet a beállítások és adatok migrációja, illetve a programok újratelepítése. A félreértések elkerülése végett a továbbiakban a frissítés a helyben frissítést, a migráció a tiszta telepítés és az azt követő a migrációs lépések egymásutánját fogja jelenteni.



21. ábra: Frissítés vagy telepítés?

Látható, hogy a frissítés mindenképpen kényelmesebb dolog, hiszen a telepített programokat nagyrészt nem kell újratelepíteni. Ahhoz, hogy frissítés történhessen, elég sok dolognak kell egyeznie. Az első és legfontosabb dolog, hogy a hardvernek kompatibilisnek kell lennie az új verzióval, azaz az új verziónak támogatnia kell a hardvert. Minden hardvereszköznek kell, hogy legyen **illesztőprogramja** (meghajtó programja – Driver) az új verzió alá.

A következő fontos feltétel, hogy a telepített és az új rendszernek azonos architektúrájúnak kell lennie. Azaz 32 bites rendszerről nem lehet 64 bites rendszerre frissíteni és fordítva sem működik a dolog.

Az utolsó megvizsgálandó dolog pedig az, hogy a telepített kiadásról lehetséges-e a frissítés a kívánt kiadásra, vagy sem. Ezenkívül még arra is oda kell figyelni, hogy mind a telepített, mind az új rendszer nyelvi verzió szempontjából is megegyezzen. A konkrét kritériumok és lépések először a munkaállomás változat esetén kerülnek ismertetésre.

A frissítés legfontosabb lépései – Windows 7

A Windows 7 verzióra való frissítés esetén nem árt már az elején leszögezni, hogy az csak a Windows Vista verzió egyes kiadásairól a Windows 7 verzió bizonyos kiadásaira lehetséges. Az architektúrának természetesen meg kell egyeznie, azaz 32 bites rendszerről nem lehet 64 bites rendszerre frissíteni és fordítva. Ezen felül az alapelv természetesen az, hogy a Windows 7 kiadás szintjének azonosnak vagy magasabbnak kell lennie, mint a Windows Vista kiadás szintje. Az alábbi táblázat ezt összegzi.[9]

Miről/Mire	Windows 7 Home Premium	Windows 7 Professional	Windows 7 Ultimate
Windows Vista Home Basic	igen		igen
Windows Vista Home Premium	igen		igen
Windows Vista Business		igen	igen
Windows Vista Ultimate			igen

3. *Windows 7 frissítési lehetőségek a különböző Windows Vista kiadások esetében (forrás[10])*

Itt kell megjegyezni azt is, hogy kiadási szintekkel kapcsolatos frissítési elv létezik Windows 7 esetén is, azaz egy Windows 7 Starter kiadás frissíthető Windows 7 Home Premium kiadásra, vagy egy Windows 7 Home Premium frissíthető Windows 7 Professional, de akár Ultimate kiadásra is. Természetesen az archhitektúra és a nyelvi verziók adta szabályok itt is irányadóak.

A gyártó weboldalán és különböző források táblázataiból is hiányzik az ebben a tankönyvben használt Windows 7 Enterprise. Erre a kiadásra ugyanaz vonatkozik, mint az Ultimate kiadásra.

[9] Microsoft Corporation: Frissítés Windows Vista rendszerről Windows 7 rendszerre. Online cikk, Microsoft Corporation <http://windows.microsoft.com/hu-hu/windows7/help/upgrading-from-windows-vista-to-windows-7>, 2012.09.15

[10] Microsoft Corporation: Frissítés Windows Vista rendszerről Windows 7 rendszerre. Online cikk, Microsoft Corporation <http://windows.microsoft.com/hu-hu/windows7/help/upgrading-from-windows-vista-to-windows-7>, 2012.09.15

A hardver és különböző programok kompatibilitása végett érdemes a régi operációs rendszerre telepíteni és futtatni a **Windows 7 frissítési tanácsadót** (Windows 7 Upgrade Advisor), amely a kompatibilitási vizsgálatokat elvégzi és tájékoztat az esetleges problémákról, valamint javaslatot tesz ezek megoldására. A frissítési tanácsadó futtatását a gyártó a Windows 7 magasabb kiadási szintre történő frissítése esetén is ajánlja. A Tapasztaltabb felhasználóknak természetesen ajánlott, hogy megvizsgálják a HCL-t illetve a telepített programok gyártójától érdeklődjenek a kompatibilitás végett, mivel a frissítési tanácsadó a speciális szoftverek és hardverek esetén problémát jelezhet.

Az esetek túlnyomó részében elmondható azonban, hogy ha az adott számítógép minden hardver- és szoftvereleme megfelelően működött Windows Vista rendszerrel, akkor nagy valószínűséggel a Windows 7 is megfelelően fog működni.

Egy másik nagyon fontos dolog, amely felmerül a frissítésnél (és a migrációnál is célszerű), hogy a frissítendő rendszer naprakész legyen, azaz fel legyenek telepítve a legfrissebb javítások és **szerviz csomagok** (Service Pack - SP) a rendszerre. Továbbá, ha elérhetők ilyenek a telepített illesztőprogramok és alkalmazói szoftverek esetében is, akkor azokat is hasznos lehet frissíteni.

A gyártó még olyan további tanácsokkal is ellátja a felhasználót, mint hogy a frissítés idejére érdemes előkészíteni a termékkulcsot (Product Key), valamint nem árt, ha a frissítés ideje alatt ki van kapcsolva a vírusirtó szoftver.

Ha az operációs rendszer frissítésének nincs további akadálya, akkor a telepítőt tartalmazó adathordozó gyökerében található **setup.exe**-t megnyitva el kell indítani a telepítőt. A megjelenő ablak már ismerős lehet a tiszta telepítésből, itt a **telepít** (Install) gombra kell kattintani.

Amennyiben a frissítendő operációs rendszer még nem naprakész (up to date), akkor az elsőként megjelenő párbeszédablakban még van lehetőség a javítások, SP-k letöltését és telepítését választani. Ehhez az első, ajánlott opciót kell választani, míg a frissítések keresésének mellőzésére a másodikat. Érdemes azonban ebben az esetben is az ajánlott opciót választani, mert előfordulhat, hogy valamit vagy nem sikerült megfrissíteni, vagy a legutolsó frissítés óta kijött egy újabb frissítés.

A frissítések letöltése és telepítése (vagy azok mellőzése) után a liceszfeltételek (EULA) elolvasása következik. A frissítés csak a feltételek elfogadás esetén folytatható, ehhez az **elfogadom a licencfeltételek** (I accept the licence terms) kapcsolót be ki kell pipálni, majd a **tovább** (Next) gombra kell kattintani.

Az ez után következő képernyőn kell a **frissítést** (Upgrade) választani, az **egyéni (haladó)** (Custom (Advanced)) lépés helyett. Ezután megjelenhet egy **kompatibilitási jelentés** (Compatibility Report), melyet a telepítő készít el, majd az **asztalra ment** (saved to desktop). Itt a **tovább** (Next) gombra kell kattintani és a frissítési folyamat elkezdődik.

Ezután a telepítő felmásolja fájljait (Copying Windows files) a merevlemezre, majd a **fájlok beállítások és programok összegyűjtése** (Gathering files, settings, and programs) lépése következik. A **Windows fájlok kibontása** (Expanding Windows files) művelet közben a számítógép újraindul. A művelet befejezése után az **összetevők és frissítések telepítése** (Installing features and updates) lépéssel folytatódik az operációs rendszer frissítése.

A képernyőn látható utolsó lépés a **fájlok, beállítások és programok áttelepítése** (Transferring files, settings, and programs) előtt a számítógép megint újraindul. Ennek a lépésnek az időtartama nagyban függ a telepített alkalmazások számától, és amely után a frissített rendszer még utoljára újraindul.

Az ezután elinduló már frissített Windows 7 rendszer a három utolsó beállítása teljesen megegyezik a tiszta telepítés utolsó három lépésével. Ezek a biztonsági beállítások, az idő, dátum, időzóna beállításai, valamint a hálózati kapcsolat megadása. Ezek beállítása után már használható is az új Windows 7 rendszer.

Megjegyzendő, hogy abban az esetben, ha valamelyik Windows 7 kiadást kell magasabb verzióira frissíteni, érdemes igénybe venni Windows Anytime Upgrade szolgáltatást, de azt is lehetőleg a frissítési tanácsadó után használata után. A Windows Anytime Upgrade szolgáltatás a %systemroot%\system32\WindowsAnytimeUpgradeUI.exe futtatható fájlt megnyitva lehet elindítani. A megjelenő ablakban a **frissítési kulcs beírását** (Enter an upgrade key) kell választani (már ha rendelkezésre áll a frissítési kulcs), majd meg kell adni a kulcsot és a tovább (Next) gombra kell kattintani, majd követni a szolgáltatás utasításait. Magyarországon sajnos a frissítés automatikus, a kulcs interneten keresztüli megvásárlására épülő frissítési metódus nem használható.

A frissítés legfontosabb lépései – Windows Server 2008 R2

A Windows Server 2008 esetén már az elején érdemes leszögezni, hogy csak abban az esetben lehetséges a frissítés, ha a kiszolgálón a Windows Server 2008 64 bites verziója futott, minden más esetben migrációra lesz szükség. Nem is olyan nagy baj ez, ha még a gyártó is inkább tiszta telepítést javasol minden esetre kivéve, ha valami különösen indokolja a helyben történő frissítést.

A Windows kiszolgáló változat esetén is különösen ajánlott, hogy a rendszer naprakész legyen, azaz minden rendszerfrissítést, a hardver eszközökhöz tartozó illesztőprogram frissítést, illetve az alkalmazói szoftverek frissítését meg kell lépni. Ebben az esetben is fontos a hardver kompatibilitása (HCL), valamint itt még arra is oda kell figyelni, hogy R2 esetén már csak 64 bites verzió létezik. Azaz 64 bitet támogató processzorra, valamint legalább 2GB RAM-ra is szükség lesz. Természetesen itt is a Windows Server R2 hardverkövetelményei táblázat adatai az irányadóak.

A frissítés lépései egyébként szinte teljes mértékben megegyeznek a Windows 7 frissítés lépéseivel. Itt is az adathordozóról való indítás (setup.exe) után megjelenő ablak **telepítés** (Install) gombjára kattintva kezdődik a frissítés. A következő megjelenő ablakban még ugyanúgy van lehetőség a hiányzó frissítések telepítésére, vagy mellőzésére, mint a Windows 7 frissítés esetén.

A következő ablakban a szerver változat telepítésénél megszokott lista látható, amelyből a megfelelő kiadás kiválasztása a feladat. Ezután kell a frissítés lehetőséget választani a helyben frissítéshez. A lépés után (ugyanúgy, mint a Windows 7 estében) megjelenhet egy kompatibilitási jelentés (Compatibility Report), melynek elkészüléséről a telepítő számol be, amelyet az asztalra ment (saved to desktop). Itt a tovább (Next) gombra kell kattintani és a frissítési folyamat elkezdődik. A folyamatnak ugyanazok a lépései, mint a Windows 7 esetén, melynek a végén a frissített Windows Server 2008 R2 használatba vehető.

2.2.7 A migráció

Minden olyan esetben a migrációt kell alkalmazni, amikor a helyben frissítés (röviden frissítést) nem lehetséges. A fejezet elején már szó volt arról, hogy ez gyakorlatilag egy tiszta telepítést jelent, majd pedig a különböző beállítások, alkalmazások migrációját. Valamivel bonyolultabb a tehát a helyezet, mint a frissítés esetén, de szerencsére rendelkezésre állnak különböző eszközök is ahhoz, hogy a migráció zökkenőmentes legyen. Ezek az eszközök a munkaállomás változat esetén a már ismert **Windows 7 frissítési tanácsadó** (Windows Upgrade Advisor), a **Windows áttelepítő** (Windows Easy Transfer), illetve a kiszolgáló változat esetén a **Windows Server áttelepítési eszközök** (Windows Server Migration Tools – WSMT). Természetesen a felhasználói beállításokat kézzel is lehet migrálni, bár nem lehetetlen, de mindenképpen hosszadalmas és bonyolult feladat. Előnye viszont az, hogy különböző, eszközök szabta korlátok nem jelentek akadályt.

Fontos tudni, hogy a rendszerre telepített alkalmazásokat nem lehet migrálni, hacsak nem létezik hozzájuk valamilyen speciális áttelepítő eszköz.

Ennek hiányában az új rendszeren ezeket az alkalmazásokat kézzel kell telepíteni.

Először is érdemes átgondolni azt, hogy nem véletlenül nincs támogatva a helyben frissítés az adott verzióról, hiszen a hardver valószínűleg már nem bírná el az új rendszert, akkora a különbség a frissítendő és az új rendszer között. Ebből kiindulva olyan eset nem is kerül tárgyalásra, amikor is a telepítendő számítógép nem teljesen új lenne. A régi rendszer számítógépének pedig mindaddig rendelkezésre kell állnia, amíg a migráció folyamata véget nem ér. Nem szabad elfelejteni azt sem, hogy a migrálandó adatok egyik számítógépről a másikra való átviteléhez szükség lesz egy megfelelő adathordozóra. Erre a legjobb egy külső USB-s merevlemez vagy egy megfelelő nagyságú USB pendrive.

Bár említésre került már, de nem lehet eleget hangsúlyozni, hogy a migráció esetén is nagyon fontos, hogy a migrálandó rendszert naprakész állapotba kell hozni. Amíg ez nincs meg, nem is érdemes nekikezdeni a folyamatnak.

A migráció legfontosabb lépései – Windows 7

Windows 7-re történő migráció esetében gyakorlatilag mindegy, hogy Windows XP vagy Windows Vista a migrálandó rendszer. Az eszközökkel segített migrálásnál a frissítés következő alapelveit kell szem előtt tartani: csak azonos architektúra esetén lehetséges a migráció, illetve a nyelvi verzióknak is egyeznie kell.

Az első lépés mindenképpen a Windows 7 frissítési tanácsadó letöltése, telepítése, majd futtatása. (Ha itt a rendszer kéri a .NET 2.0 telepítését, akkor azt is telepíteni kell, mert nélküle nem fog a tanácsadó működni.) A futtatás akár több percig is eltarthat, melynek a végén az eszköz egy kompatibilitási jelentést készít. Ahhoz, hogy a migrációval ne legyen probléma érdemes átnézni a kapott listát és a problémákra adott megoldási javaslatokat követve ki kell azokat javítani. Fontos, hogy minden megoldás, javítás, frissítés után újra le kell futtatni a frissítési tanácsadót. Arra is érdemes odafigyelni, hogy új számítógépre lesz telepítve a Windows, ezért a hardver kompatibilitást (HCL) azzal a számítógéppel kapcsolatban kell vizsgálni a telepítésnél ismertetett módon, a frissítési tanácsadó régi hardverre vonatkozó jelentését pedig mellőzni kell. A jelentést azonban érdemes elmenteni vagy kinyomtatni.

A következő lépés a Windows áttelepítő letöltése, telepítése és futtatása. Ennek az eszköznek a segítségével olyan elemek migrálhatók, mint a felhaszná-

lói fiókok, illetve olyan mappák tartalma, mint a dokumentumok, zene, képek, e-mailek, internetes kedvencek, videók és az egyebek.[11]

Az áttelepítő megnyitása utána a megjelenő képernyőn a **tovább** (Next) gombra kell kattintani. Ezután a **külső merevlemez vagy USB meghajtó** (An external hard disk or USB flash drive), majd pedig az **ez a régi számítógépem** (This is my old computer) lehetőséget kell választani. Ezután az eszköz átvizsgálja a számítógépet.

A megjelenő ablakban ki kell jelölni azokat a felhasználókat, akiknek az adatait át kell migrálni az új számítógépre. A **tovább** (Next) gomb megnyomása után meg kell adni és egy jelszót, amelyet majd az áttelepítés után kérni fog az eszköz, majd a **mentés** (Save) gombra kell kattintani. Az áttelepítő egyetlen fájlba csomagolja be az összes migrálandó adatot, fájlt, beállítást. A felugró párbeszédablakban meg kell jelölni azt a helyet, ahová az áttelepítőnek el kell mentenie ezt a fájlt.

A **mentés** (Save) gombra kattintva az áttelepítő elkezdi lementeni a kívánt adatokat. Ez jó ideig eltarthat a tárolt fájlok mennyiségtől függően. A művelet végén megjelenik **a rendszer mentette a fájlokat és a beállításokat az áttelepítéshez** (These files and settings have been saved for your transfer) üzenet, amely után a **tovább** (Next) gombra kattintva egy összegző képernyő jelenik meg, amely megmutatja az elmentett fájl helyét és nevét. Ezek után a tovább, majd a bezárás gombra kell kattintani és ezzel véget ért az áttelepítés első lépése.

A migráció következő lépése a Windows 7 tiszta telepítése az új hardverre. Ennek részletes folyamata a 2.2.6 fejezetben található. A Windows 7 telepítése után az adathordozót, amelyre az áttelepítő fájl le lett mentve csatlakoztatni kell az új számítógéphez. A Windows Intézőt elindítva meg kell keresni a csatlakoztatott adathordozót, és meg kell keresni rajta az elmentett áttelepítő fájlt, majd meg kell nyitni.

A megnyitás után meg kell adni a mentéskor megadott jelszót a folytatáshoz, majd a **tovább** (Next) gombra kell kattintani. **Az áttelepítendő elemek kiválasztása** (Choose what to transfer to this computer) lapon lehet dönteni az áttelepítés módjáról. Itt érdemes az aktuális fiókleképezést választani, majd az **átvitel** (Transfer) gombra kattintani. Ritkán előfordulhat, hogy a fiókleképezés nem megfelelő. Ilyen esetben az áttelepítési fiókleképezés módosításához a **speciális beállítások** (Advanced Options) elemre kell kattintani.

[11] Microsoft Corporation: Windows áttelepítő. Online cikk, Microsoft Corporation. <http://windows.microsoft.com/hu-hu/windows7/products/features/windows-easy-transfer>, 2012.09.15

Az átvitel végén az **áttelepítés befejeződött** (Your transfer is completed) ablakban az **áttelepített elemek listája** (See what was transferred) elemre kattintva megtekinthető az áttelepített fiókok, fájlok és beállítások. A **lista azokról a programokról, amelyekre az új számítógépen szüksége lehet** (See a list of programs you might want to install on your new computer) elemre kattintva megjelenik azoknak a szoftvereknek a listája, amelyek a régi számítógépre voltak feltelepítve. Ezeket a szoftvereket kell az új számítógépre feltelepíteni a migráció utolsó lépéseként. Az áttelepítő **bezárása** (Close) után újra kell indítani a számítógépet. Több felhasználói fiók áttelepítése esetén az újraindítás utáni első bejelentkezéskor a Windows kérheti a jelszó megváltoztatását. Ha megjelenik az erre felszólító üzenet, akkor meg kell adni az új jelszót, majd az OK gombra kell kattintani.[12]

A migráció utolsó lépéseként fel kell telepíteni az előbb említett listában felsorolt programokat. Ehhez természetes szükség lesz a programok telepítőjére is. Előfordulhat, hogy vannak olyan programok, amelyek a Windows korábbi verziójának voltak részei, de a Windows 7-ben már nem léteznek (pl. Windows Mail vagy Outlook Express). Ezeket a programokat más programokkal kell helyettesíteni (pl. Windows Live Mail).

A migráció befejeztével a Windows 7 használatba vehető.

A migráció legfontosabb lépései – Windows Server 2008 R2

A kiszolgáló változat migrációt támogató eszköze valami egészen más, mint a munkaállomásé. Ki lehet mondani, hogy jóval bonyolultabb, és ez nem is csoda, hiszen egy kiszolgáló estén a szerepkörök számával nő az eset bonyolultsága. A Windows Server áttelepítési eszközök (WSMT) a PowerShell (PS) segítségével működik, mind a régi, és mind az új kiszolgáló esetén. Segítségével jelenleg a következő beállításokat, szerepköröket, képességeket lehet migrálni:

- TCP/IP konfiguráció
- DHCP kiszolgáló
- Active Directory
- DNS kiszolgáló
- Fájlkiszolgáló
- Nyomtatókiszolgáló
- Helyi felhasználók és csoportok

[12] Microsoft Corporation: Windows áttelepítő. Online cikk, Microsoft Corporation. <http://windows.microsoft.com/hu-hu/windows7/products/features/windows-easy-transfer>, 2012.09.15

A terjedelem korlátai miatt itt most csak a TCP/IP beállítások, a DHCP kiszolgáló és a helyi felhasználók és csoportok migrációjáról lesz szó. A többi ezek analógiájára működik, a gyártó által nyújtott dokumentáció ezekre is kitér.[13]

A következő táblázatban látható, hogy szinte minden verzióról van lehetőség migrációra, kivéve hogy a Windows Server 2008 Server Core változatról nem lehet migrálni a WSMT segítségével, mivel nem tartalmazza a .NET Framework-öt, amely a WSMT működéséhez elengedhetetlen. Pontosabban mind a régi kiszolgálón, mind az új kiszolgálón a .NET Framework 2.0 minimum követelmény. Korlát továbbra is, hogy különböző nyelvi verziók esetén sem működik ez a típusú migráció. Fontos, hogy a régi rendszeren és az új rendszeren is legyen PS, a régin 1.0-ás, az újon 2.0-ás verziójú, hiszen a WSMT nem más, mint egy PS cmdlet (parancs) gyűjtemény.

Régi kiszolgáló	Régi architektúra	Új kiszolgáló	Új architektúra
Windows Server 2003	x86/x64	Windows Server 2008 R2 Server Core és teljes	x64
Windows Server 2003 R2	x86/x64	Windows Server 2008 R2 Server Core és teljes	x64
Windows Server 2008 teljes	x86/x64	Windows Server 2008 R2 Server Core és teljes	x64
Windows Server 2008 R2	x64	Windows Server 2008 R2 Server Core és teljes	x64
Windows Server 2008 R2 Server Core	x64	Windows Server 2008 R2 Server Core és teljes	x64

4. *WSMT migrációs lehetőségek a különböző kiszolgáló verziók és architektúrák esetén (forrás[14])*

A WSMT telepítéséhez a tisztán telepített Windows Server 2008 R2-n a **kiszolgálókezelőben** (Server Manager) jobb gombbal a **szolgáltatásokra** (Features) kattintva a megjelenő helyi menüből a **szolgáltatás hozzáadása** (Add features) menüpontot kell kiválasztani. A **tovább** (Next) gombra kattintva települ a szolgáltatás. A folyamat végét a **bezár** (Close) gombbal lehet nyugtázni.

[13] GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

[14] GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

Első lépésként létre kell hozni egy mappát az új kiszolgálón. Legyen ez most a C:\WSMT. A mappa meg is osztható a régi kiszolgáló számára és a migrációval kapcsolatos fájlcserék ezen keresztül folyhatnak. Természetesen, mint ahogy a Windows 7 migrációnál, itt is működő alternatíva a külső adathordozó (USB-s merevlemez, pendrive).

Ha eldőlt, hogy milyen módszerrel vándorolnak át a fájlok a számítógépek között, akkor a kezdéshez el kell indítani egy parancssort, méghozzá rendszergazdaként. Ehhez a **start menü** (Start), **minden program** (All Programs) almenü **kellékek** (Accessories) almenüjében, jobb gombbal kell kattintani a **parancssor** (Commandline) menüponton, és a megjelenő helyi menüből ki kell választani a **futtatás rendszergazdaként** (Run as Administrator) menüpontot.

A megjelenő parancssorban elsőként a **cd** parancs segítségével be kell lépni a WSMT mappájába.

```
1   cd %Windir%\System32\ServerMigrationTools
```

Ezután a SmigDeploy.exe parancsot attól függően megfelelően felparaméterezve, hogy milyen architektúrával és operációs rendszerre rendelkezik a régi kiszolgáló, ki kell adni. Az architecture értéke x86 és amd64, az os értéke WS03 és WS08 lehet. A path pedig legyen az erre a célra létrehozott mappa (itt: 64 bites Windows Server 2008 a régi rendszer és C:\WSMT a mappa).

```
2   SmigDeploy.exe /package /architecture amd64 /os
WS08 /path C:\WSMT\
```

A kiadott parancs a megadott mappa alá létrehoz egy mappát, amelynek nevét az architektúra és az operációs rendszer nevéből kreálja (itt: SMT_ws03_amd64), és különböző fájlokat másol bele. Ezt a mappát, vagy a megosztás, vagy egy külső tároló segítségével át kell vinni (másolni) a régi kiszolgálóra.[15]

A régi kiszolgálóra belépve a másolt mappát el kell helyezni valahol a rendszerben (itt a C:\WSMT\SMT_ws03_amd64 helyre kerül). Itt is indítani kell rendszergazdaként egy parancssort és be kell lépni az adott mappába a **cd** paranccsal.

15 GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

```
3   cd C:\WSMT\SMT_ws03_amd64
```

Majd innen futtatni kell a SmigDeploy.exe parancsot.

```
4   .\SmigDeploy.exe
```

Ezek után a régi rendszeren el kell indítani a PS-t, kiválasztva a **start menü** (Start), **felügyeleti eszközök** (Administrative Tools) almenü, **Windows Server áttelepítési eszközök** (Windows Server Migration Tools) almenüjének **Windows Server áttelepítési eszközök** menüpontját. Sima PS konzol indítása esetén a várt hatáshoz még a következő parancsot kell kiadni.

```
5   Add-PSSnapin Microsoft.Windows.ServerManager.Migration
```

Arra is van lehetőség, hogy sima parancssort indítva is elérhetővé váljon a PS, méghozzá ebben az esetben a ServerMigration modullal.

```
6   Powershell.exe –PSConsoleFile ServerMigration.psc1
```

A DHCP kiszolgáló migrációjánál oda kell figyelni a hálózati interfészek számára, hiszen elképzelhető, hogy a DHCP kiszolgáló több alhálózatban is működik, melyek közvetlenül csatlakoznak a kiszolgálóhoz. Fontos tehát, hogy az új számítógépen legalább annyi hálózati interfész legyen, mint a régiben. Ha ez így van, akkor ki kell adni az exportálás parancsát:

```
7   Export-SmigServerSetting –featureID DHCP –User All
–Group –IPConfig –path C:\WSMT\DHCP\ –Verbose
```

A parancs kiadásának hatására a WSMT elkezdi összegyűjteni a kért adatokat, a végén kér egy jelszót, amelynek minimum 6 karakteresnek kell lennie, majd megjeleníti (a –Verbose hatására) az eredmény részleteit. Az export kimenete egy **srvmig.mig** fájl a célmappában, amelyet vagy az új gép megosztott mappájába kell átmásolni, vagy külső adathordozón kell átvinni az új gép migrációs mappájába.[16]

```
8   Import-SmigServerSetting -featureid DHCP –User All
–Group –IPConfig All –SourcePhysicalAddress 08-00-27-
```

16 GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

```
CC-0F-B7 –TargetPhysicalAddress 08-00-27-CC-0F-B7 –
Force -path C:\WSMT\DHCP\ –Verbose
```

A megjelenő üzenet végén a WSMT figyelmeztet, hogy a számítógépet újra kell indítani a változások érvénybelépéséhez.

Ha még nem volt DHCP kiszolgáló telepítve a számítógépre a WSMT a fenti parancs (featureID DHCP) DHCP specifikus része miatt ezt érzékeli és feltelepíti a szerepkört. Bár a telepítés a migrációs lépés előtt is megtörténhetett volna, abban az esetben csak arra kellett volna vigyázni, hogy a migráció ideje alatt a DHCP kiszolgáló le legyen állítva. A kiszolgáló-kezelőből végzett DHCP kiszolgáló telepítés egyébként egy későbbi fejezetben lesz tárgyalva.

A feltelepült DHCP kiszolgáló indítási beállításai és indítása parancssorból a következőképpen adható meg:

```
9   Set-Service DHCPserver –startupType automatic
10  Start-Service DHCPServer
```

További migrációs lépésekről a Microsoft Technet weboldalán lehet bővebben olvasni.[17]

2.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

2.3.1 Összefoglalás

Ebben a leckében a virtualizáció fogalma, valamint az Oracle VirtualBox virtualizációs szoftver és az az által létrehozható virtuális környezet került ismertetése. A virtualizációs környezetre azért van szükség, hogy a tananyag leckéiben szereplő hálózatba kötött kiszolgáló és kliens számítógépek rendszerét szimulálni lehessen. Szó volt a virtuális számítógépek (VM) létrehozásának lépéseiről, valamint ezeknek a virtuális gépeknek az összekötéséről.

Ismertetésre került mind a Windows 7 munkaállomás operációs rendszer, mind a Windows Server 2008 R2 kiszolgáló operációs rendszer tiszta telepítésének folyamata a virtuális környezetben, a tervezéstől a kivitelezésig.

A frissítés és a migráció-használat módjainak és a folyamatok lépéseinek ismertetésével zárult ez a lecke.

[17] Microsoft Corporation: Migrate Server Roles to Windows Server 2008 R. Online cikk, Microsoft Corporation <http://technet.microsoft.com/en-us/library/dd365353(v=ws.10).aspx>, 2012.09.16

2.3.2 Önellenőrző kérdések

1. Soroljon fel a Windows Server 2008 és a Windows Server 2008 R2 újdonságai közül hármat-hármat!
2. Mi a virtualizáció? Soroljon fel hármat a virtualizáció előnyei közül!
3. Melyek egy VM létrehozásának főbb lépései a VirtualBox virtualizációs környezetben?
4. Mire kell odafigyelni a telepítés előtt?
5. Hasonlítsa össze a Windows 7 és a Windows Server 2008 R2 telepítésének legfontosabb lépéseit!
6. Mi a különbség a frissítés és a migráció között?
7. Melyek a különbségek a Windows 7 és a Windows Server 2008 R2 frissítése között?
8. Hasonlítsa össze a Windows 7 migrációjának és a Windows Server 2008 R2 migrációjának legfontosabb lépéseit!

3 A HARDVERESZKÖZÖK, AZ ALKALMAZÁSOK BEÁLLÍTÁSAI, HÁLÓZATI KONFIGURÁCIÓ

3.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Ebben a leckében a Windows munkaállomás és kiszolgáló operációs rendszerének legfontosabb alapbeállításain túl a különböző hardvereszközök kezelése, valamint illesztőprogramjaik telepítése, frissítése, eltávolítsa, valamint a vezérlőpult legfontosabb funkciói kerülnek ismertetésre. A lecke ezek után részletesen foglalkozik a Windows operációs rendszer hálózati működésével, annak támogatásával, továbbá a hálózati beállításokkal. Itt kerül ismertetésre az alkalmazott virtuális hálózati környezet is, valamint e környezet kialakításának lépései.

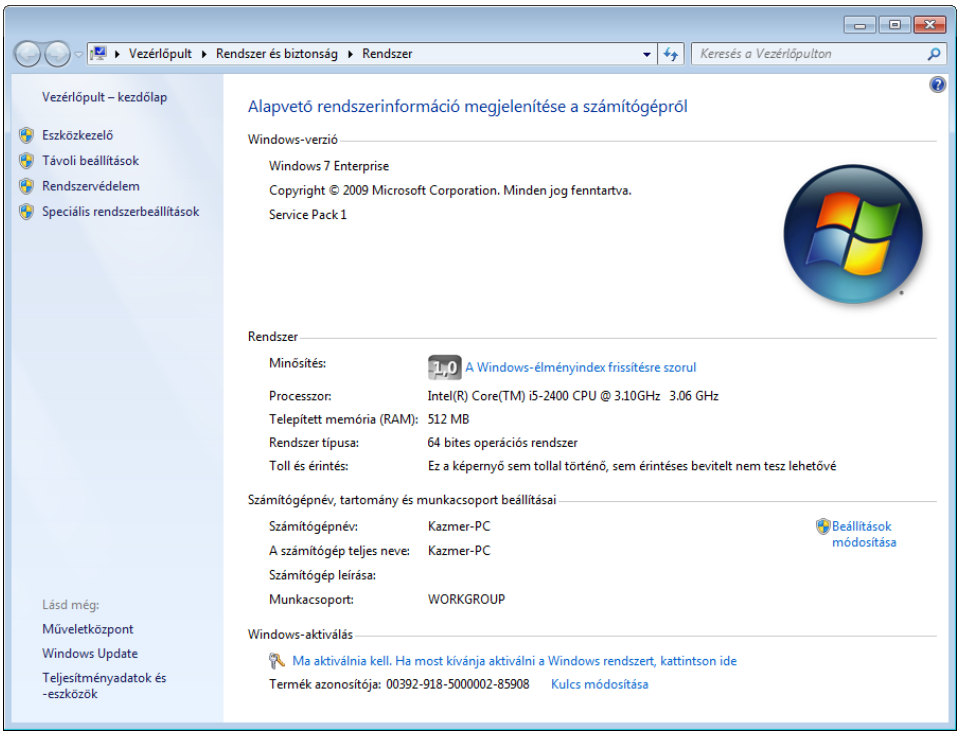
A lecke végén a hallgató képes lesz a különböző hardvereszközökkel kapcsolatos feladatok elvégzésére, mint pl. az illesztőprogramok kezelése (telepítés, frissítés, elétávolítás). Képes lesz a vezérlőpult különböző elemein keresztül az operációs rendszer beállításait a kívánalmaknak megfelelően módosítani.

A tananyag elsajátítása után a hallgató kezelni tudja a Windows operációs rendszerrel telepített számítógépek hálózati konfigurációját, valamint módosítani tudja hálózati működését, illetve meg tudja különböztetni a munkacsoportos és tartományi hálózati modelleket.

3.2 TANANYAG

3.2.1 Alapvető rendszerinformációk

A telepítés után mindenképpen érdemes egy pár dolgot megvizsgálni, hogy minden rendben és megfelelően működik. Először a Start menüből a **számítógépre** (Computer) jobb gombbal kattintva, majd a megjelenő helyi menüből a **tulajdonságokat** (Properties) kiválasztva megjelenik a **vezérlőpult** (Control Panel) **rendszer** (System) lapja, amely alapvető információkat jelenít meg a számítógépről. (A vezérlőpultról bővebben a vezérlőpult fejezetben lehet olvasni.)

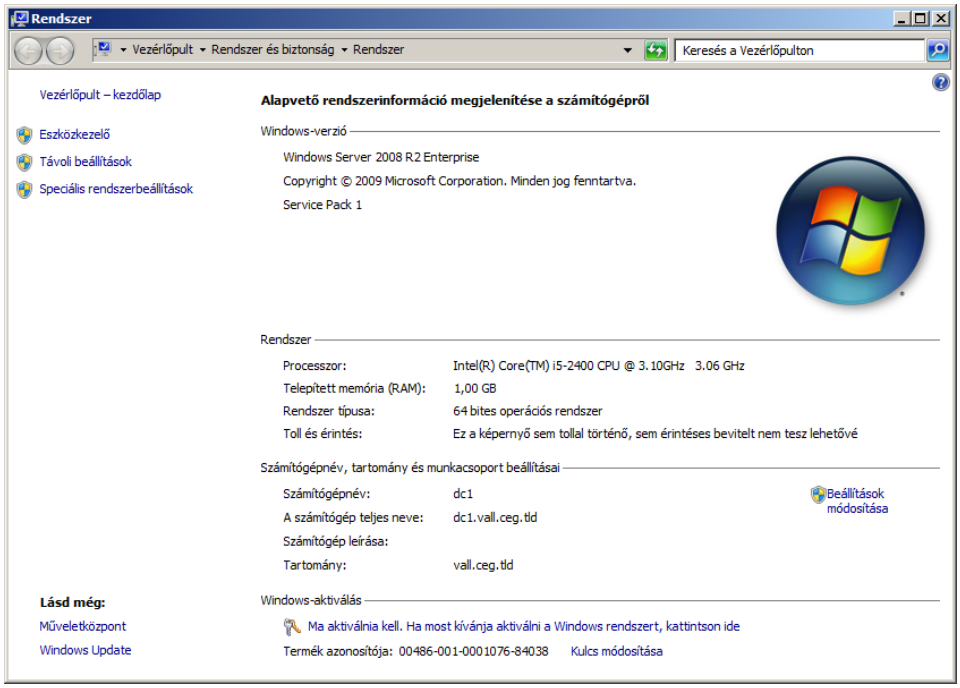


22. ábra: A rendszer lap (Windows 7)

A képernyő felső sávjában látszik, hogy a vezérlőpulton belül hol található a jelenleg megnyitott lap, illetve a sáv jobb szélén lehetőség van a vezérlőpult elemeire keresni. A sáv alatt a lap függőlegesen ketté van vágva. A bal oldali keskenyebb oszlopban, mint egy menü, különböző beállítási funkciók érhetőek el. A jobb oldali nagyobb területen láthatók az alapvető rendszerinformációk négy szakaszra bontva.

Az első szakaszban a Windows verzió és kiadás, valamint a telepített szervizcsomag (Service Pack) verziószáma érhető el. A második szakaszban olyan rendszerelemekkel lehet találkozni, mint a **processzor** (Processor), a **telepített memória (RAM)** (Memory (RAM)) mennyisége, vagy a rendszer típusa (ebben az esetben 64 bites).

A következő szakaszban a **számítógép nevét** (Computer name), **teljes nevét** (Full computer name), **leírását** (Computer description) valamint a **munkacsoport** (Workgroup) vagy **tartomány** (Domain) nevét lehet látni. Az értékek módosíthatók a **rendszer adatlap** (System properties) **számítógépnév** (Computer Name) lapján keresztül a jobb oldalon található **beállítások módosítása** (Change settings) szövegre kattintva.



23. ábra: A rendszer lap (Windows Server 2008 R2)

Az utolsó szakaszban a Windows aktiválásával kapcsolatos információk jelennek meg. Az aktiválás gyakorlatilag egy védelem a Windows illegális használata ellen. A megvásárolt Windows-zal együtt egy ún. termékkulcsot is kap a felhasználó, amelyet a telepítés folyamán, vagy később itt a rendszer lapon keresztül lehet megadni. Ha a számítógép állandó internetkapcsolattal rendelkezik, a Windows megpróbálja magát automatikusan aktiválni. Ha a termékkulcs megfelelő volt, ez általában sikerül is. Internetkapcsolat hiányában lehetőség van telefonos aktiválásra is, ilyenkor a megfelelő számot felhívva és a termékkulcsot megadva aktiválható a Windows.

Ebben a szakaszban látható a Windows aktiválásának státusza, és a termékazonosító. Ha a Windows még nincs aktiválva, akkor az **aktiválásra** (Activate) kattintva ezt meg lehet tenni, illetve ha a **termékkulcs** (Product Key) még nem lett megadva, vagy valamiért módosítani kell, akkor azt a **kulcs módosítására** (Change product key) kattintva lehet megtenni. A Windows aktiválására azért van szükség, mert különben bizonyos funkciók nem érhetők-e el, sőt sima felhasználók esetében nem is lehet használni a számítógépet.

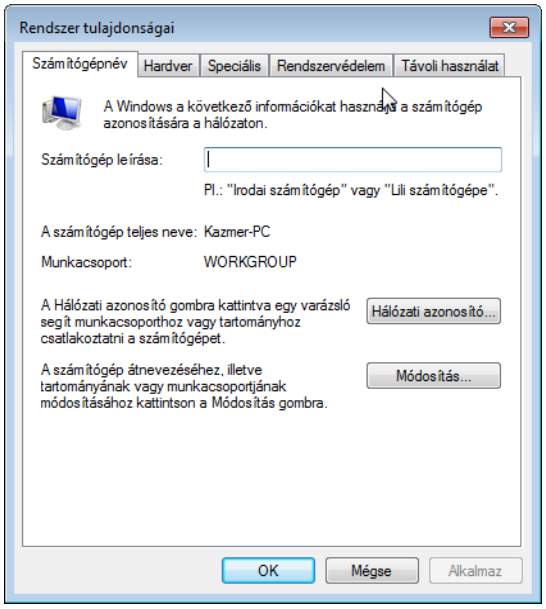
A rendszer lap bal oldalán található „menüből” érhető el az **eszközkezelő** (Device Manager), amellyel részletesebben a következő fejezet foglalkozik,

valamint a **rendszer tulajdonságai** adatlap több funkciója. Ezek a funkciók pedig a **távoli beállítások** (Remote settings), a **rendszervédelem** (System protection) és a **speciális rendszerbeállítások** (Advanced system settings).

3.2.2 A rendszer tulajdonságai adatlap

A számítógépnév és a hardver lap

A rendszer tulajdonságai adatlap 5 különálló lapból áll, amelyek között a nevüket jelző fülekre kattintva lehet váltani. Az első a számítógépnév adatlap. Itt látható, hogy a számítógéphez milyen megjegyzés tartozik, mi a neve van, illetve a munkacsoport vagy tartomány neve, attól függően, hogy milyen típusú hálózathoz csatlakozik a számítógép. A mezők neve sorban: **számítógép leírása** (Computer description), **a számítógép teljes neve** (Full computer name), **munkacsoport/tartomány** (Workgroup/Domain).

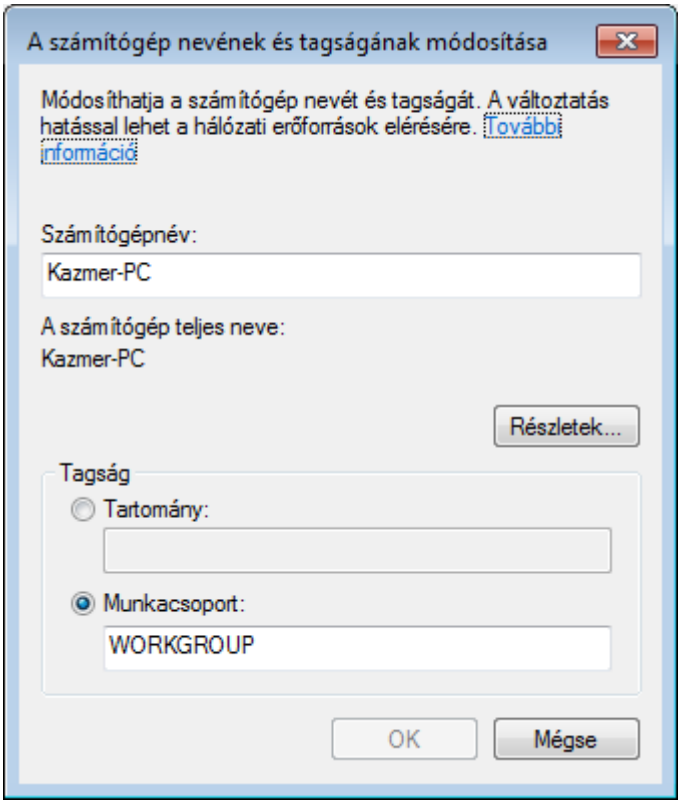


24. ábra: A számítógépnév lap (Windows 7)

A leírás minden különösebb körültekintés nélkül módosítható. A többi beállítás a **módosítás** (Change) gombra kattintva, illetve a munkacsoport/tartomány beállítás a kliens verzióban a **hálózati azonosító** (Network ID) gombra kattintva felugró varázsló segítségével is módosítható.

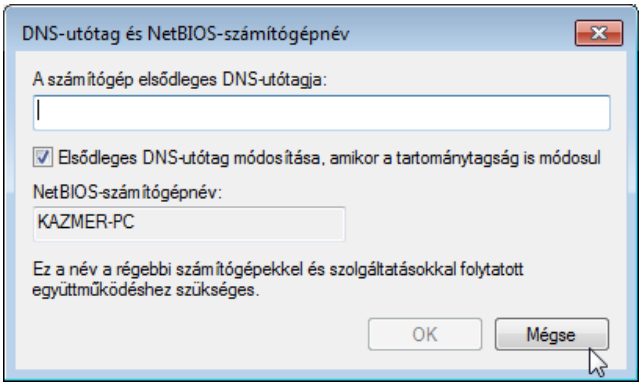
A **módosítás** gomb megnyomására megjelenő **a számítógép nevének és tagságának módosítása** (Computer Name/Domain Changes) párbeszédablak-

ban már módosítható a számítógépnév. Ugyanitt kiválasztható a számítógép **tagságának** (Member of) fajtája és megadható a **tartomány** (Domain) vagy **munkacsoport** (Workgroup) neve.



25. ábra: A számítógép nevének és tagságának módosítása (Windows 7)

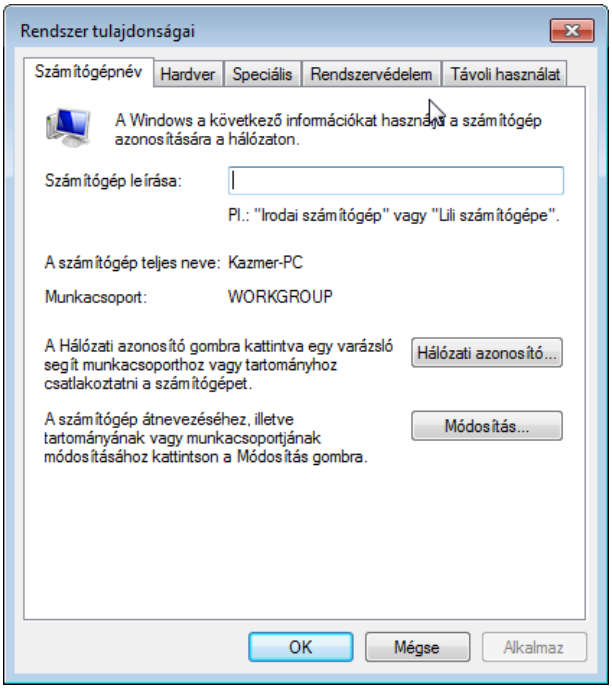
A **részletek** (More) gombra kattintva a **DNS-utótag és NetBIOS-számítógépnév** (DNS Suffix and NetBIOS Computer Name) párbeszédablakban **a számítógép elsődleges DNS utótagja** (Primary DNS suffix of this computer) mezőben lehet megadni a **teljes DNS-beli név** utótagját (Fully Qualified Domain Name – FQDN), azaz a teljes interneten használt név első pont utáni részét. Az alatta lévő **elsődleges DNS-utótag módosítása, amikor a tartománytagság is módosul** (Change primary DNS suffix when domain membership changes) kapcsoló bekapcsolásával tartományi környezetben nem szükséges ezt a mezőt kitölteni, az érték automatikusan a tartomány neve lesz. A párbeszéd ablak alján látható **NetBIOS-számítógépnév** (NetBIOS copmuter name) régebbi rendszerekkel és szolgáltatásokkal folytatott együttműködésre van szükség. Értékét a számítógépnévből állítja elő a Windows, értéke nem módosítható.



26. ábra: DNS-utótag és NetBIOS-számítógépnév (Windows 7)

Nagyon fontos, hogy a számítógépnév és a tagság módosítása után mindig újra kell indítani a számítógépet, hogy az új beállítások érvénybelépjenek.

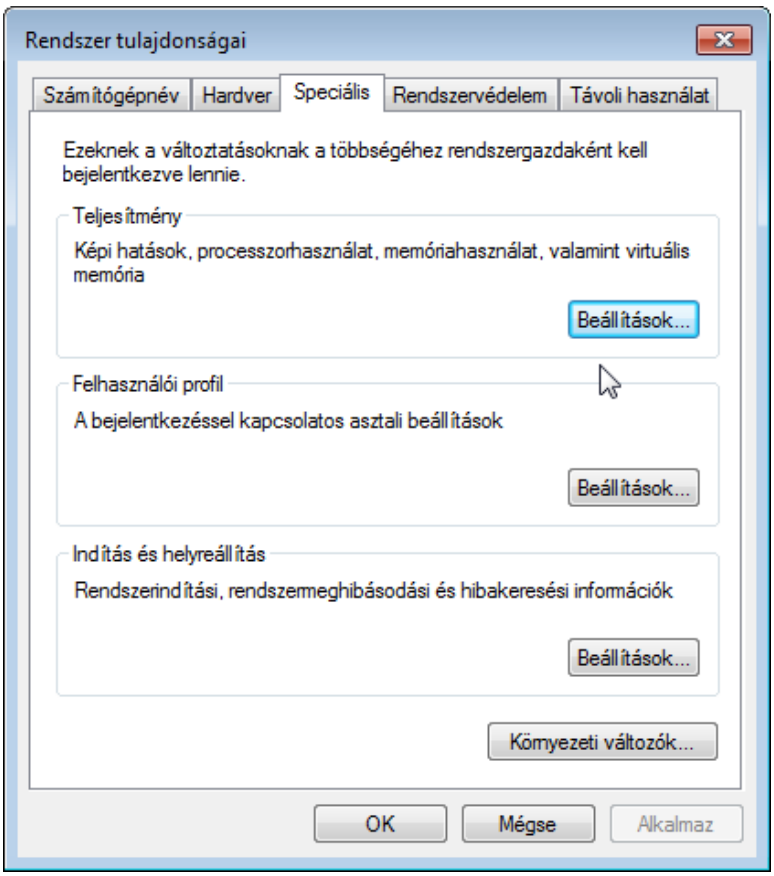
Az adatlap **hardver** (Hardware) fülére kattintva az **eszközkezelő** (Device Manager) és az **eszköztelepítés beállításai** (Device Installation Settings) érhetők el, ezekről később lesz szó részletesebben.



27. ábra: A hardver lap (Windows 7)

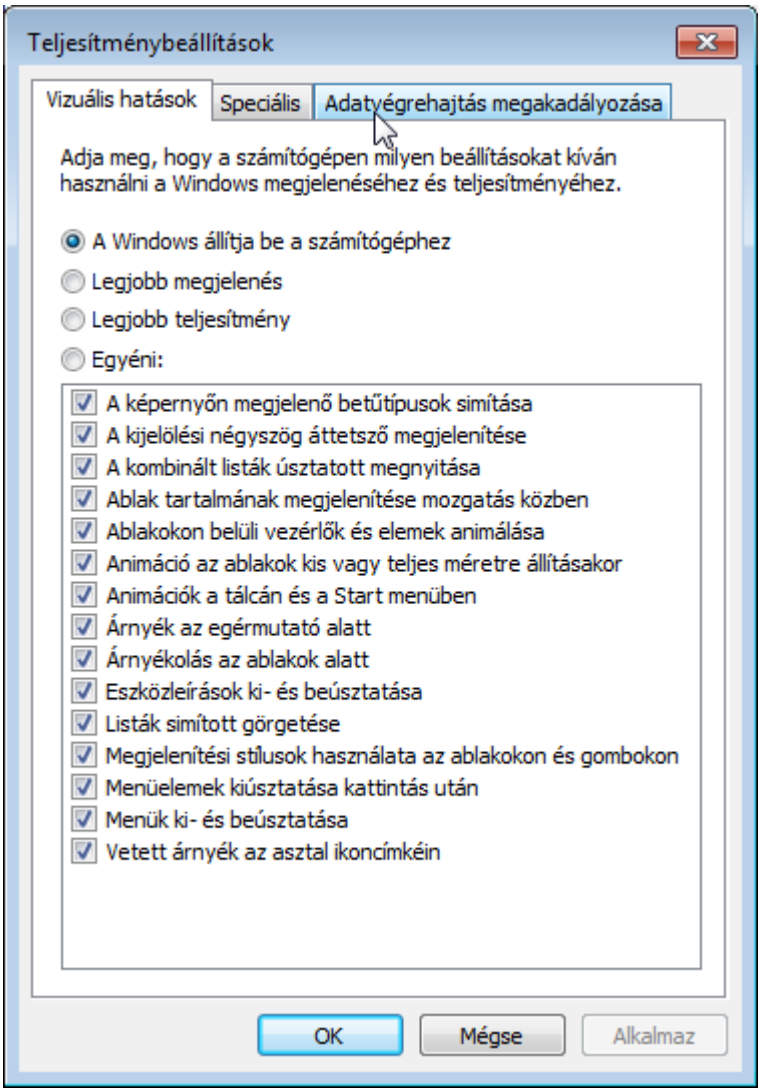
A speciális lap

A **speciális** (Advanced) lapon található beállítások közül az első a számítógép **teljesítményre** (Performance) vonatkozik.



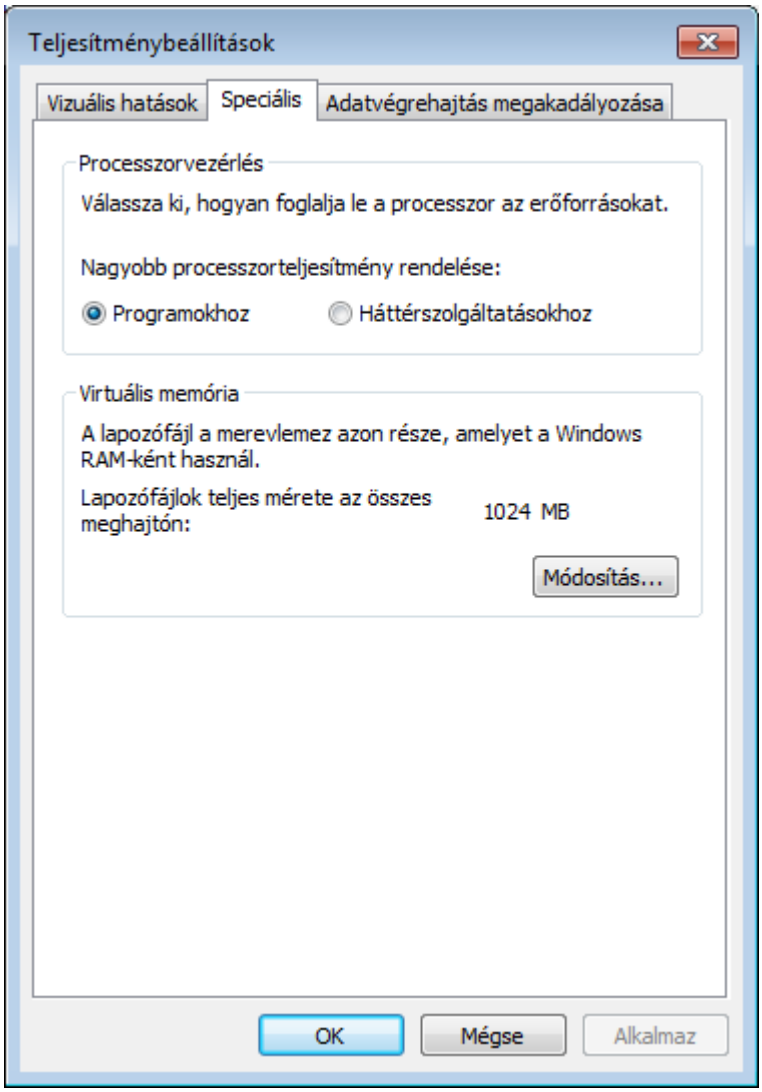
28. ábra: A speciális lap (Windows 7)

A **beállítások** (Settings) gombra kattintva a megjelenő **teljesítmény-beállítások** (Performance Options) tulajdonságlapon, a vizuális hatások fülön állítható, hogy a számítógép erőforrásai inkább a megjelenés, vagy a teljesítmény szolgálatába legyenek állítva. Három előre beállított érték és egy egyénileg testre szabható beállítás választására van lehetőség. Az előre beállított értékek rendre: **a Windows állítja be a számítógéphez** (Let Windows choose what's best for my computer), **legjobb megjelenés** (Adjust for best appearance), **legjobb teljesítmény** (Adjust for best performance).



29. ábra: Teljesítménybeállítások – vizuális hatások (Windows 7)

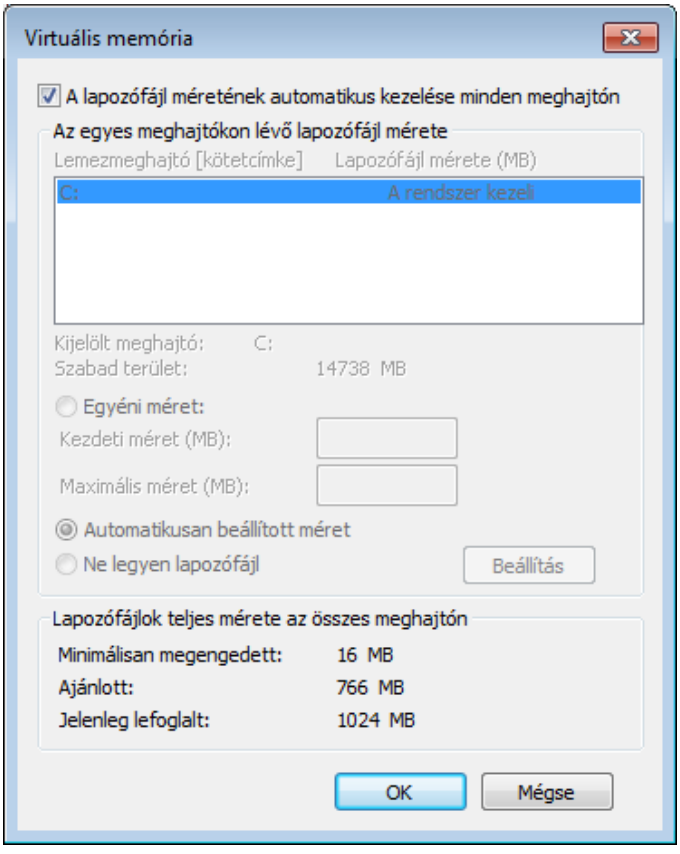
Az adatlap **speciális** (Advanced) fülére kattintva a **processzorvezérlést** (Processor scheduling) és **virtuális memóriát** (Virtual memory) lehet konfigurálni. A processzorvezérlésnél ez annyit jelent, hogy meg lehet mondani a Windowsnak, hogy a processzor mihez rendeljen nagyobb teljesítményt, az előtérben futó **programokhoz** (Programs), vagy a háttérben futó **szolgáltatásokhoz** (Background services).



30. ábra: Teljesítménybeállítások – speciális (Windows 7)

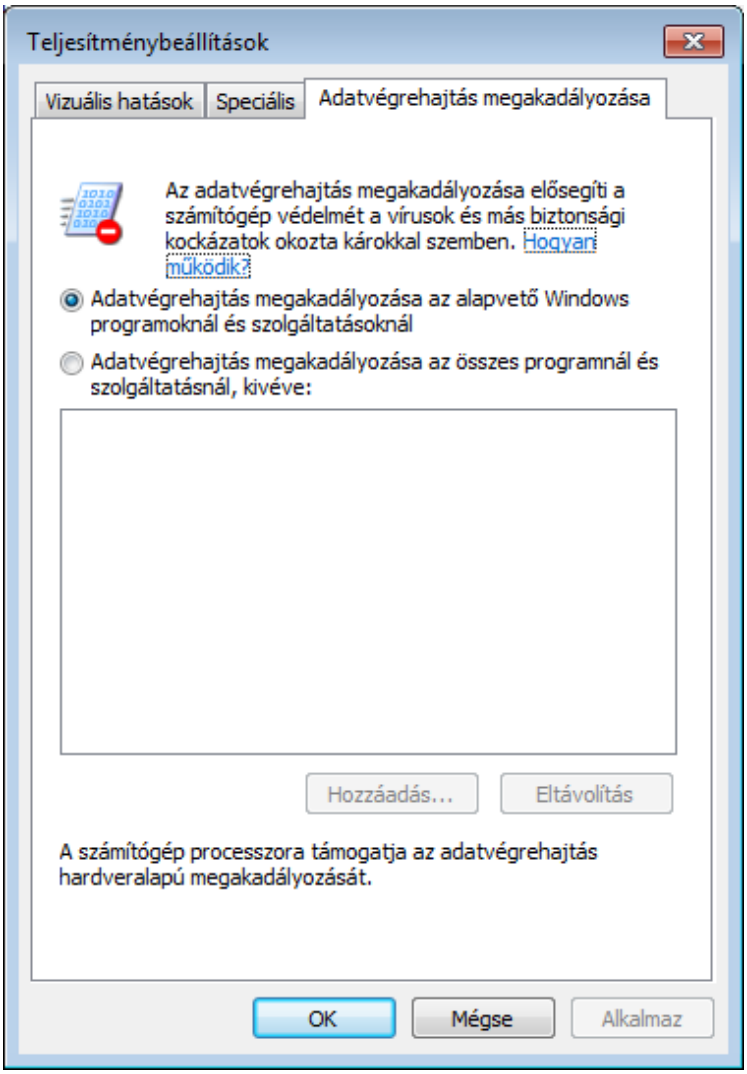
A virtuális memória szakasznál a **módosítás** (Change) gombra kattintva lapozófájl méretét lehet szabályozni. Az alapértelmezett beállítás **a lapozófájl méretének automatikus kezelése minden meghajtón** (Automatically manage paging file size for all drives) bekapcsolt állapota, amelytől eltérni csak nagyon speciális esetben érdemes. Ha ilyen előáll, akkor az előbb említett kapcsolót kikapcsolva és az alatta megjelenő listából a számítógépben található merevlemez-meghajtók közül a megfelelőt kiválasztva külön szabályozható **az egyes meghajtónkon a lapozófájl mérete** (Paging file size for each drive). A

meghajtónkénti szabályozásnál lehetőség van automatikus és egyéni méret beállítására is. Az **egyéni méret** (Custom size) esetében a **kezdeti** (Initial size) és a **maximális értéket** (Maximum size) kell megadni megabbájtban (Mega Byte – MB). Az automatikusan beállított méretet választásán kívül, amely egyébként a meghajtónkénti lemezfájl beállításoknál az alapértelmezett beállítás, lehetőség van még arra is, hogy a rendszer az adott meghajtón nem használjon lapozófájlt. Ehhez a meghajtó kiválasztása után a **ne legyen lapozófájl** (No paging file) opciót kell választani. A megfelelő lapozófájl-kezelést választva a **beállítás** (Set) gombra kell kattintani, ahol is a rendszerre veszélyes értékek választása esetén a Windows figyelmeztet a rendszerhiba előfordulásának veszélyére. A művelet végén, a lap alján összevethetők a beállított értékek a rendszer által jelenleg használt lapozófájlbeállítások értékeivel. Ennek tudatában kell az **OK** vagy a **mégse** (Cancel) gombot választani.



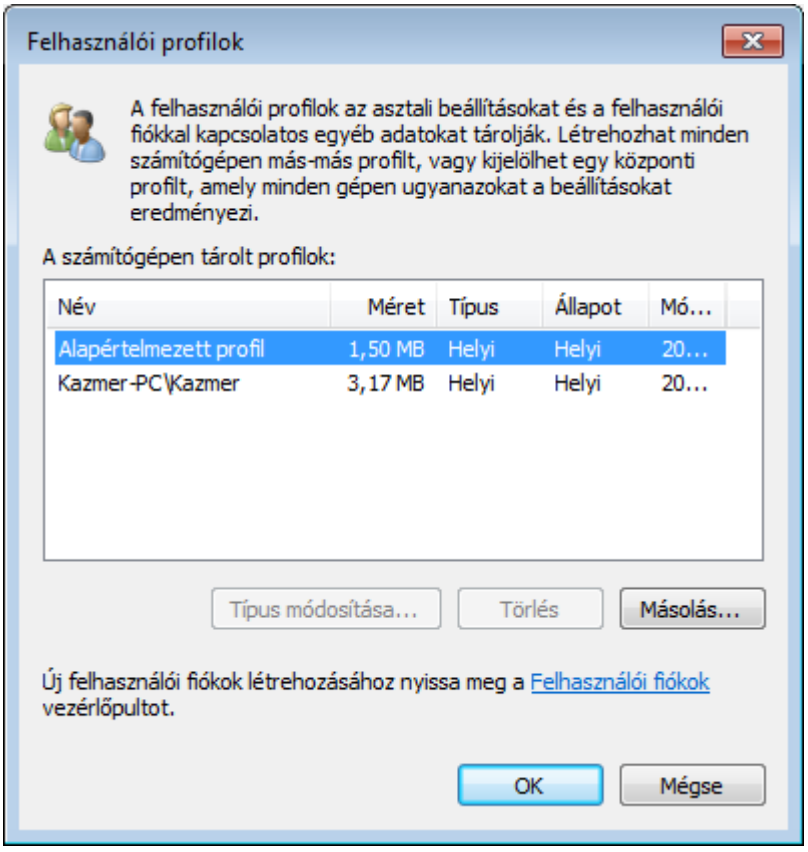
31. ábra: A virtuális memóra beállításai (Windows 7)

A **teljesítménybeállítások** adatlap utolsó lapja az **adatvégrehajtás megakadályozása** (Data Execution Prevention – DEP) egy olyan biztonsági beállítás, amelynek segítségével megakadályozható olyan programok futtatása, amelyek az adatokhoz használt memóriarészből kísérelnek meg utasításokat végrehajtani. Az ilyen programok tipikusan vírusok vagy más típusú kártékony kódok, melyek célja a számítógép feletti irányítás átvétele. Ilyen észlelése esetén a Windows azonnal bezárja a gyanús futó programot.



32. ábra: Teljesítménybeállítások – adatvégrehajtás megakadályozása (Windows 7)

Ha bizonyos programok esetén ezt a szolgáltatást ki kell kapcsolni valamiért, akkor azt az alapértelmezettől eltérő **adatvégrehajtás megakadályozása az összes programnál és szolgáltatásnál, kivéve** (Turn on DEP for all programs and services except those I select) opciót kell választani, majd a **hozzáadás** (Add) gombra kattintva ki kell tallózni a kérdéses futtatható állományt, amelynek futását gyanús művelet esetén sem kell megszakítni. A lista a későbbiekben tovább bővíthető a **hozzáadás** és szűkíthető az **eltávolítás** (Remove) gombokkal.



33. ábra: Felhasználói profilok (Windows 7)

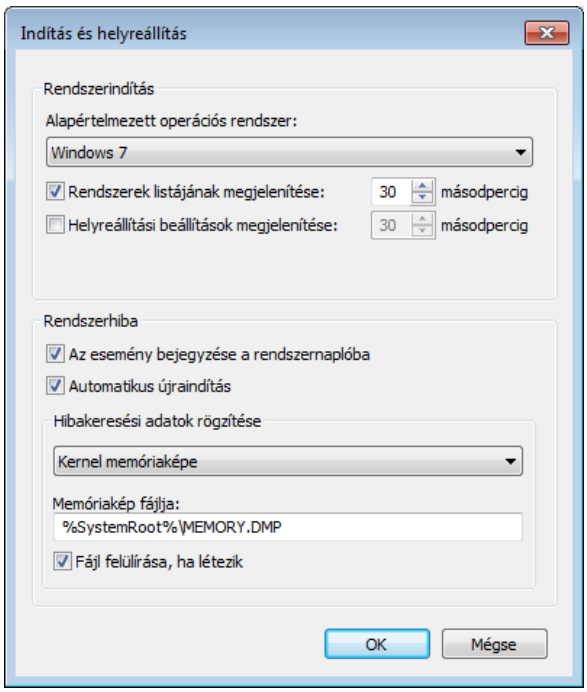
A **rendszer tulajdonságai** adatlap **speciális** lapján a **teljesítmény** szakasz után a **felhasználói profil** (User Profile) a következő szakasz. A felhasználói profil olyan beállítások gyűjteménye, amelyekkel a számítógép kinézete és működése a felhasználó által szabályozható. A beállítások többek között az asztalra, háttérre, képernyőkímélőre, az egérmutató beállításokra, hangbeállításokra és egyéb jellemzőkre, más szóval a felhasználói környezetre vonatkoznak. A profil

gondoskodik arról, hogy a felhasználó minden bejelentkezés után ugyanazt a felhasználói környezetet kapja, amelyet a legutóbbi kijelentkezéskor használt.

A felhasználói profiloknak két típusa létezik, helyi (Local profile) és vándorló (Roaming profile). A helyi profil mindig csak az adott számítógépen található meg és a felhasználó első bejelentkezésekor jön létre. Ezért is tart egy kicsit tovább a felhasználó első bejelentkezése. A vándorló profil általában egy központi kiszolgálón található és a felhasználó minden egyes bejelentkezésekor letöltődik az adott számítógépre, kijelentkezéskor pedig visszatöltődik a kiszolgálóra.

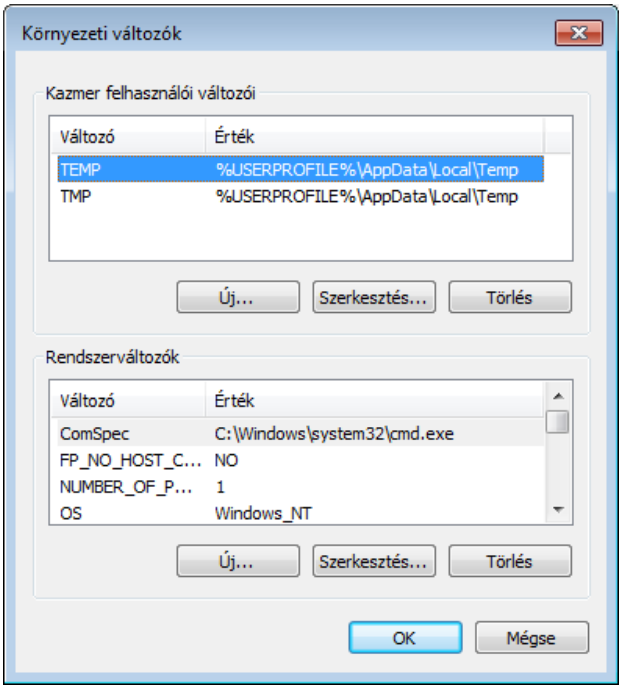
A **beállítások** (Settings) gombra kattintva megjelenik egy lista, amely **a számítógépen tárolt profiok** (Profiles stored on this computer) **nevét** (Name) és azok olyan tulajdonságait tartalmazza, mint a **méret** (Size), a **típus** (Type), **állapot** (Status), és annak a dátuma, hogy a profil mikor lett utoljára **módosítva** (Modified).

A **típus módosítása** (Change Type) gomb segítségével meg lehet egy profil típusát változtatni, a **másolás** (Copy To) gombbal le lehet másolni egy adott profilt, a **törlés** (Delete) gombbal pedig törölni lehet őket.



34. ábra: Indítás és helyreállítás (Windows 7)

A speciális lap utolsó szekciójában, mely az **indítás és helyreállítás** (Startup and Recovery) nevet viseli, olyan apróbb rendszer beállítások tehetők meg, mint **a rendszerek listájának megjelenítése** (Time to display list of operating systems), amely abban az esetben érhető el, ha több operációs rendszer is van telepítve a számítógépre. Lehetőség van **a helyreállítási beállítások megjelenítésére** (Time to display recovery options when needed) is, vagy annak beállítására, hogy **rendszerhiba** (System failure) esetén mit tegyen a Windows. Ez utóbbi olyan lehetőségeket kínál, mint az **esemény bejegyzése a rendszernaplóba** (Write an event to the system log), az **automatikus újraindítás** (Automatically restart), vagy a **hibakeresési adatok rögzítése** (Write debugging information), amikor is egy itt megadott ún. **memóriakép fájlba** (Dump file) mentődik le a memória kért részének tartalma.



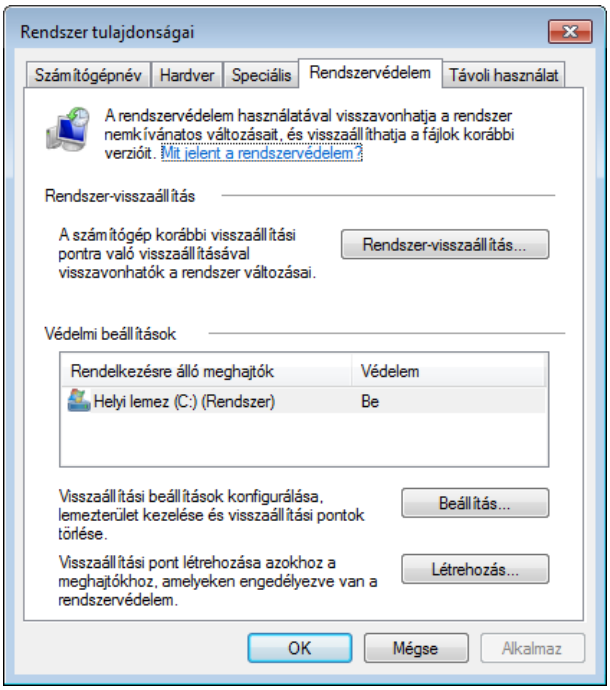
35. ábra: Környezeti változók (Windows 7)

A speciális lapon található még a **környezeti változók** (Environment Variables) gomb az utolsó szekció alatt. Erre kattintva a megjelenő párbeszédablakban mind az aktuális **felhasználó változói** (User variables for), mind a **rendszerváltozók** (System variables) megjeleníthetők, értékeik megváltoztathatók a **szerkesztés** (Edit) gomb segítségével, de akár **új** (New) változókat is be lehet állítani. A rendszerváltozók kezeléséhez természetesen megfelelő jogo-

sultsággal kell rendelkeznie a felhasználónak. Új változó beállítása, vagy meglévő nevének vagy értékének módosítása esetén a megjelenő párbeszédablak megfelelő mezőit kell manipulálni. Fontos, hogy ilyen esetben mindenképpen az OK gombra kell kattintani, mert a változások csak akkor kerülnek érvényre.

A rendszervédelem és a távoli használat lap

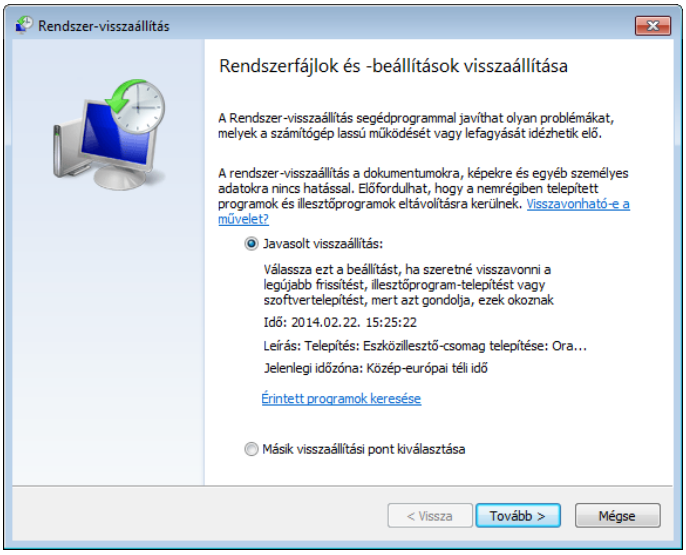
A **rendszervédelem** (System Protection) a Windows egy olyan szolgáltatása, amelynek segítségével olyan ún. **visszaállítási pontokat** (Restore points) lehet létrehozni, amelyek segítségével a számítógép egy korábbi állapotába állítható vissza. A szolgáltatás rendszeresen információkat gyűjt a számítógép rendszerfájljairól, beállításairól, és menti azokat. A Rendszervédelem ezenkívül menti a felhasználó által módosított fájlok korábbi verzióit. Ezeket a fájlokat a visszaállítási pontokba menti, amelyek kizárólag olyan jelentős rendszereseményekt előtt jönnek létre, mint pl. egy program vagy egy illesztőprogram telepítése. Ezenkívül a pontok hétnaponta automatikusan létrejönnek, ha a megelőző egy hetes időszakban nem kellett másikat létrehozni, de bármikor létrehozhatók kézzel is. A szolgáltatás automatikusan be van kapcsolva azon a meghajtón, amelyre a Windows telepítve van, de más meghajtókon is be lehet bekapcsolni, ha azok korábban az NTFS fájlrendszert használnak.



36. ábra: Rendszervédelem (Windows 7)

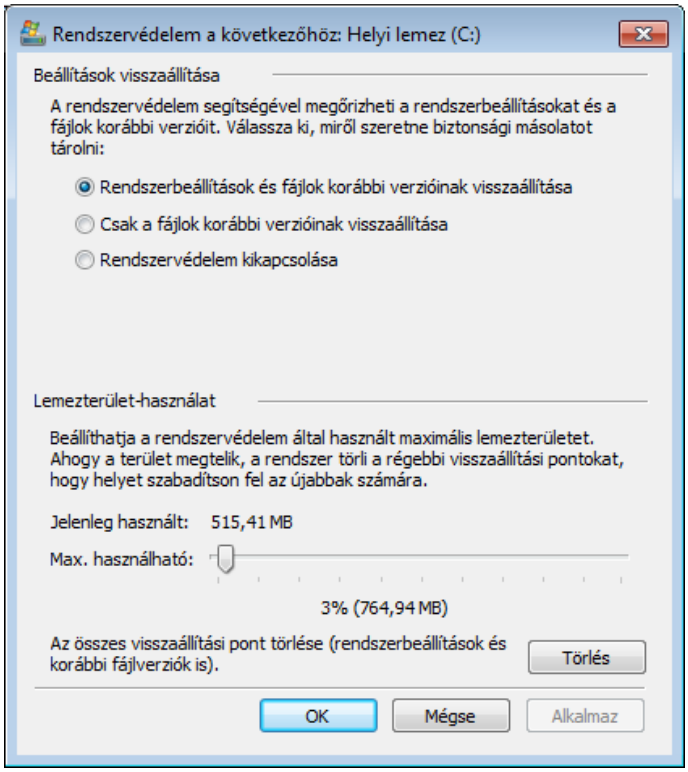
Általában akkor van szükség a visszaállítások használatára, ha egy illesztőprogram, vagy egy alkalmazás telepítése után a rendszer nem működik megfelelően, és a megjelent hibát javítani máshogy nem lehet. Egy másik, gyakori eset, amikor fájlok vagy mappák véletlen módosítása vagy törlése esetén van szükség a visszaállításra, amely a visszaállítási pontban tárolt verziók segítségével történhet meg.

A **rendszer-visszaállítás** (System Restore) gombra kattintva a számítógép egy korábbi visszaállítási pontban elmentett állapotba állítható vissza. A megjelenő párbeszédablakban kijelölhető a kívánt visszaállítási pont, majd a **tovább** (Next) gombra kattintva a kívánt visszaállítás adatait figyelmesen átolvasva a **befejezés** (Finish) gombra kell kattintani. A visszaállítási pont kijelölésénél található **érintett programok keresése** (Scan for affected programs) gombra kattintva a Windows megjeleníti azokat a programokat, frissítéseket, amelyek visszaállítás esetén eltávolításra kerülnek, hiszen azok a az adott visszaállítási pont létrehozása után kerültek telepítésre.



37. ábra: Rendszer-visszaállítás (Windows 7)

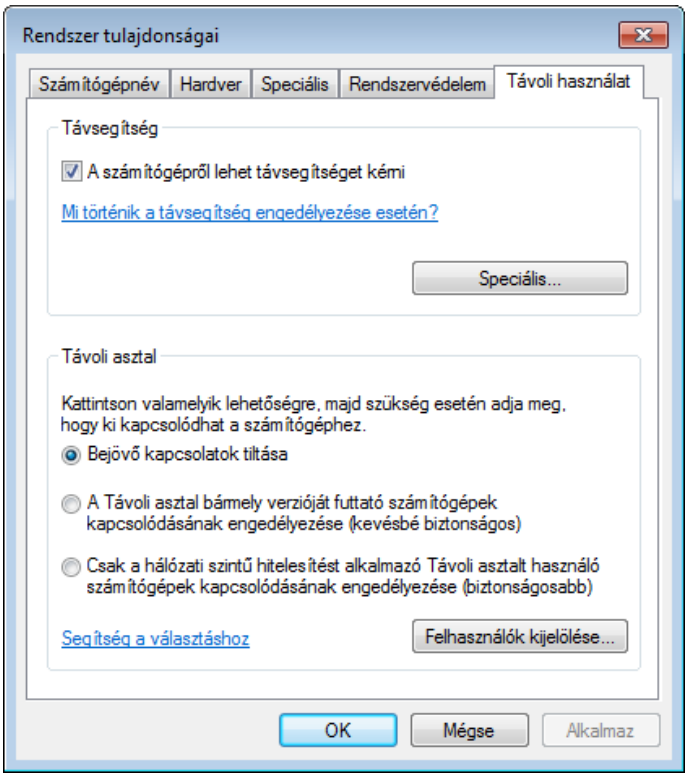
A **védelmi beállítások** (Protection Settings) szakaszban látható listában felsorolásra kerülnek a rendszer által használt **meghajtók** (Available Drives) és azok **védelmi** (Protection) beállítása. A meghajtó kijelölése után a **beállítás** (Configure) gombra kattintva a védelmi beállítások bekapcsolhatók, kikapcsolhatók, illetve módosíthatók.



38. ábra: Rendszervédelem a következőhöz Helyi lemez (C) (Windows 7)

Választani lehet, hogy a Windows a **rendszerbeállításokat és a fájlok korábbi verzióinak visszaállítását** (Restore system settings and previous versions of files), **csak a fájlok korábbi verzióinak visszaállítását** (Only restore previous version of files) támogassa, illetve választható még a **rendszervédelem kikapcsolása** (Turn off system protection) a kiválasztott meghajtóra. Ezenkívül a párbeszédablak alján beállítható az is, hogy a rendszervédelem legfeljebb mennyi **lemezterületet használhat** (Max Usage) a meghajtón. Ha ez a tárhely betelik, akkor a rendszervédelem elkezdi törölni a legrégebbi visszaállítási pontokat, hogy az újakat létrehozhassa. Az összes visszaállítási pont törlésére is van lehetőség a legalul elhelyezkedő **törlés** (Delete) gombra kattintva.

A védelmi beállítások másik gombja, a **létrehozás** (Create) segítségével kézzel is lehet visszaállítási pontot létrehozni, mindössze valamilyen nevet kell a visszaállítási pontnak adni. Érdemes itt olyat választani, amely utal a visszaállítási pont létrehozásának okára. Természetesen ebben az esetben arra is figyelni kell, hogy a műveletek végén az OK gombbal nyugtázni kell a megadott beállítások végrehajtását.



39. ábra: A távoli használat beállításai (Windows 7)

A **távoli használat** (Remote) segítségével távsegítség kérhető és nyújtható, valamint a számítógép távoli elérése állítható be távoli asztal protokollon keresztül (Remote Desktop Protocol – RDP). A távoli asztal elérés alapértelmezés szerint ki van kapcsolva, ilyenkor a **bejövő kapcsolatok tiltása** (Don't allow connections to this computer) van az adatlapon megjelölve. Az engedélyezéshez a másik két opció választására van szükség. **A távoli asztal bármely verzióját futtató számítógépek kapcsolódásának engedélyezése (kevésbé biztonságos)** (Allow connections from computers running any version of Remote Desktop (less secure)) választása esetén szinte minden RDP klienssel lehet csatlakozni a számítógéphez, igaz a kapcsolat nem túl biztonságos, így használata csak indokolt esetben célszerű.

Ha nincs ilyen indok, és a számítógépek, amelyekről ehhez a számítógéphez kell kapcsolódni, tudnak hálózati szintű hitelesítést alkalmazni távoli asztal kapcsolathoz, mindenképpen a **csak a hálózati szintű hitelesítést alkalmazó távoli asztalt használó számítógépek kapcsolódásának engedélyezése (bizton-**

ságosabb) (Allow connections only from computers running Remote Desktop with Network Level Authentications (more secure)) opciót kell választani.

Biztonságosabbá tehető a kapcsolat az által is, ha meg vannak jelölve azok a felhasználók, amelyek használhatják ezt a szolgáltatást. Megadásukhoz a **felhasználók kijelölése** (Select Users) gombra kell kattintani, majd a megjelenő ablakban a **hozzáadás** (Add) gombra kattintva meg kell adni a kijelölt felhasználót vagy csoportot. Az **eltávolítás** (Remove) gomb segítségével ez a jogosultság elvehető a kijelölt csoporttól vagy felhasználótól. Jó tudni, hogy alapértelmezésben a Rendszergazdák csoport tagjai használhatják csak ezt a lehetőséget, és ezen felhasználók is csak akkor, ha van nekik jelszó beállítva.

3.2.3 Hardvereszközök

Az operációs rendszer és így a számítógép normális és megbízható működéséhez, a hardver teljesítményének maximális kihasználásához a hardverelemek megfelelő kezelése szükséges. Korábban említésre került már, hogy menynyire fontos, hogy a hardver minden egyes elemét támogassa az operációs rendszer, azaz minden hardverelemhez megfelelő eszközillesztő (meghajtó – driver) program legyen telepítve.

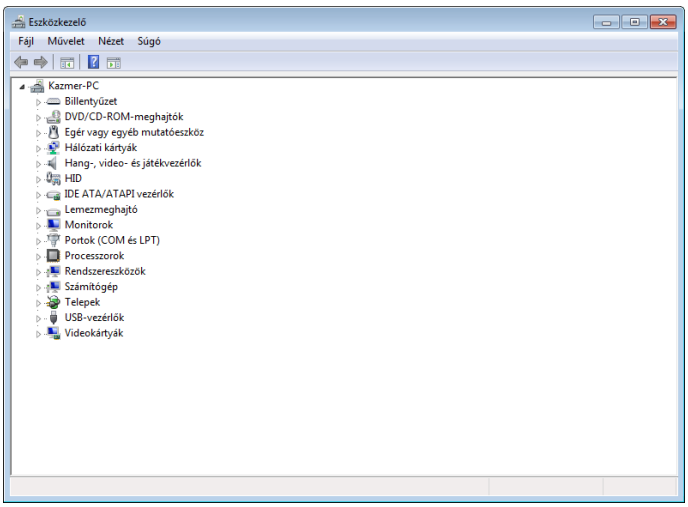
Ha a Windows operációs rendszer (mind a kliens és szerver verziókban) telepítésénél az adott számítógépet (azaz számítógép minden hardverelemét) támogatja a Windows, akkor általában sem a telepítésnél, sem az első használatba vételnél nem szoktak a hardver hibás működéséből fakadó problémák jelentkezni, hiszen a megfelelő illesztőprogramokat a Windows telepítő telepítette. Ez alól kivétel, ha egy hardverelem gyári hibás, vagy pl. szállításkor megsérült, vagy a számítógép úgy lett összeszerelve, hogy bizonyos hardverelemek nem tudnak együttműködni egymással. Utóbbi általában „az ismerős, ismerősének ismerőse majd megveszi és összerakja” szituációkban fordulhat elő, ezért érdemes mindenképpen olyan szállítótól beszerezni a számítógépet, amely garanciát vállal arra, hogy a telepítendő operációs rendszer támogatja a hardvert és megfelelően működik rajta. Ez nagyobb számítógépgyártók esetében magától értetődő.

A telepítés után természetesen előfordulhat, hogy bizonyos hardverelemek nem kerültek telepítésre még akkor is, ha a hardver egyébként a hardver kompatibilitási lista (HCL) szerint támogatott. Ez általában olyan esetekben lehetséges, amikor a telepítési lemezkép készítésekor a hardverelem még nem volt támogatott, a meghajtóprogram így nem került bele a lemezképbe, a későbbiek folyamán azonban az eszköz felkerült a támogatott hardverek listájára, és illesztőprogramja is elérhetővé vált a **Windows frissítési** (Windows Update) oldalán. Ilyen esetben az illesztőprogramot a Windows telepítése után telepíte-

ni vagy frissíteni kell. Ilyen azonban csak olyan eszközök estén fordulhat elő, amely nem feltétlenül szükséges az operációs rendszer elindulásához és működéséhez. Ha például olyan VGA (Video Graphics Array) vagy SVGA (Super VGA) kompatibilis grafikus kártya (interfész) található a gépben, amelyet nem támogat a Windows telepítő, az attól még VGA illetve SVGA módban meg tudja jeleníteni a képet, de extra képernyő felbontásokat, színmélységeket nem tud majd produkálni, azaz nem tudja a hardverben rejlő teljesítményt kihasználni. Olyan eset is lehetséges, amikor pl. hálózati interfész, wifi-kártya, hangkártya stb. nem támogatott a telepítőben, ettől még az operációs rendszer tud működni, igaz a hálózat elérhetetlensége miatt a hardver utólagos telepítése a Windows Update oldalról kicsit nehézkes. A lemezkezeléssel kapcsolatos hardverelemek támogatottságának hiánya esetén azonban már maga a telepítés sem lehetséges.

3.2.4 Az eszközkezelő

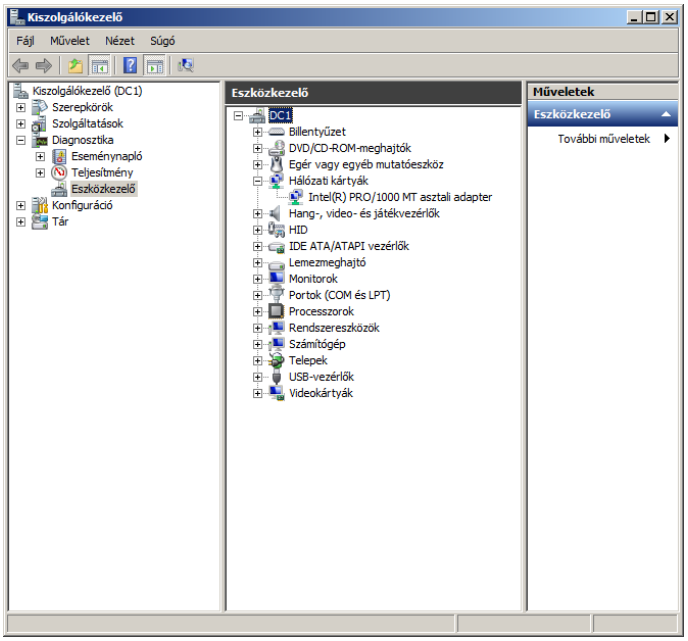
Az **eszközkezelő** (Device Manager) a Windows által a különböző hardverelemek illesztőprogramjának telepítésére, frissítésére, eltávolítására, bizonyos eszközök hardverbeállításainak módosítására készített szoftvereszköz. Az eszközkezelő egy felügyeleti konzolban az ún. Microsoft Management Console-ban (MMC) fut, amely segítségével további olyan elemek felügyelete is biztosított, mind a lemezek, a felhasználók, vagy a szolgáltatások.



40. ábra: Az eszközkezelő (Windows 7)

Az eszközkezelő több helyről is elérhető, elindításához a Start menüben a **vezérlőpultot** (Control Panel) kell választani, azon belül pedig **hardver és hang** (Hardware and Sound), **eszközök és nyomtatók** (Devices and Printers) szaka-

szában lévő **eszközkezelő** (Device Manager) bejegyzésre kell kattintani, de elérhető a már korábban említett szintén a vezérlőpultban található alapvető rendszerinformációkat tartalmazó rendszer lap bal oldali sávjából is.



41. ábra: Eszközkezelő a kiszolgálókezelőben (Windows Server 2008 R2)

Az eszközkezelő fastruktúrában mutatja meg a számítógép hardverelemeit. A fa gyökerében, legfölül a számítógép neve található. Ebből indulnak ki a különböző eszköz típusok, amelyek a konkrét eszközöket tartalmazzák.

A fontosabb típusok:

- billentyűzet (Keyboards),
- dvd-cd-rom-meghajtók (DVD/CD-ROM drives),
- egér vagy egyéb mutató eszköz (Mice and other pointing devices),
- hálózati kártyák (Network adapters),
- hang-, video- és játékvezérlő (Sound, video and game controllers),
- IDE ATA/ATAPI vezérlők (IDE ATA/ATAPI controllers),
- képeszközök (Imaging devices),
- lemezmeghajtók (Disk drives),
- monitorok (Monitors),

- portok (COM és LPT) (Ports (COM & LPT)),
- processzorok (Processors),
- rendszereszközök (System devices),
- számítógép (Computer),
- USB vezérlők (Universal Serial Bus controllers),
- videokártyák (Display Adapters),
- egyéb eszközök (Other devices).

Az eszközök megjelenítéséhez a típus neve előtti kis háromszög motívumra kell kattintani, amelynek hatására kinyílik a típus, és alatta megjelennek az eszközök nevei. Abban az esetben, ha egy adott, a számítógéphez csatlakoztatott eszköz a már korábban említett okok miatt nem került telepítésre, akkor az eszköz az egyéb eszközök típusba kerül. Ha egy eszközzel valamilyen probléma van, akkor azt az ikonja mellett megjelenő kis sárga felkiáltójel jelzi, ebből lehet tájékozódni egy eszköz állapotáról, működésének megfelelőségéről. Ilyen felkiáltójel látható az eszköz ikonján például akkor is, amikor az nincs megfelelően telepítve.

Eszközök telepítése

A Windows támogatja a Plug and Play (PnP) szabványt, amely meghatározza azt, hogy a számítógép hogyan ismerje fel és konfigurálja az újonnan hozzáadott hardvereket, amely után automatikusan telepíti az eszközillesztőt. Manapság az eszközök túlnyomó többsége PnP kompatibilis, azonban még mindig előfordulhat a Windows által **régi típusú hardvernek** (Add legacy hardware) hívott eszköz is. Ilyen eszköz telepítés esetén manuálisan kell konfigurálni az eszközt a számítógéphez csatlakoztatás előtt. Szerencsére ez igen ritkán fordul elő.

A PnP hardver és a PnP-kompatibilis operációs rendszer együttes használata esetén, a felhasználónak egyszerűen csak csatlakoztatnia kell a hardvert, az operációs rendszer pedig automatikusan megpróbálja telepíteni az illesztőprogramot, és beállítani az eszközt, hogy az más eszközzel ne ütközzön.

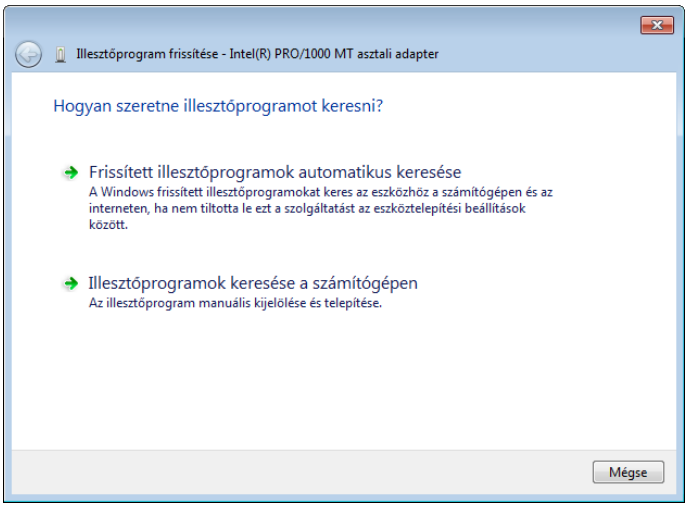
Fontos tudni, hogy az illesztőprogramok úgy futnak, mintha az operációs rendszer részei lennének, így korlátlan hozzáféréssel rendelkeznek a számítógép egészére. Ebből kifolyólag nagyon fontos, hogy csak ismert és hitelesített illesztőprogramok futtatását szabad engedélyezni.

A Windowsban egy új eszköz telepítésének folyamata a következőképpen zajlik:

1. A felhasználó csatlakoztatja az eszközt, a Windows ezt észleli és utasítja a PnP szolgáltatást, hogy kezelje az eszközt.

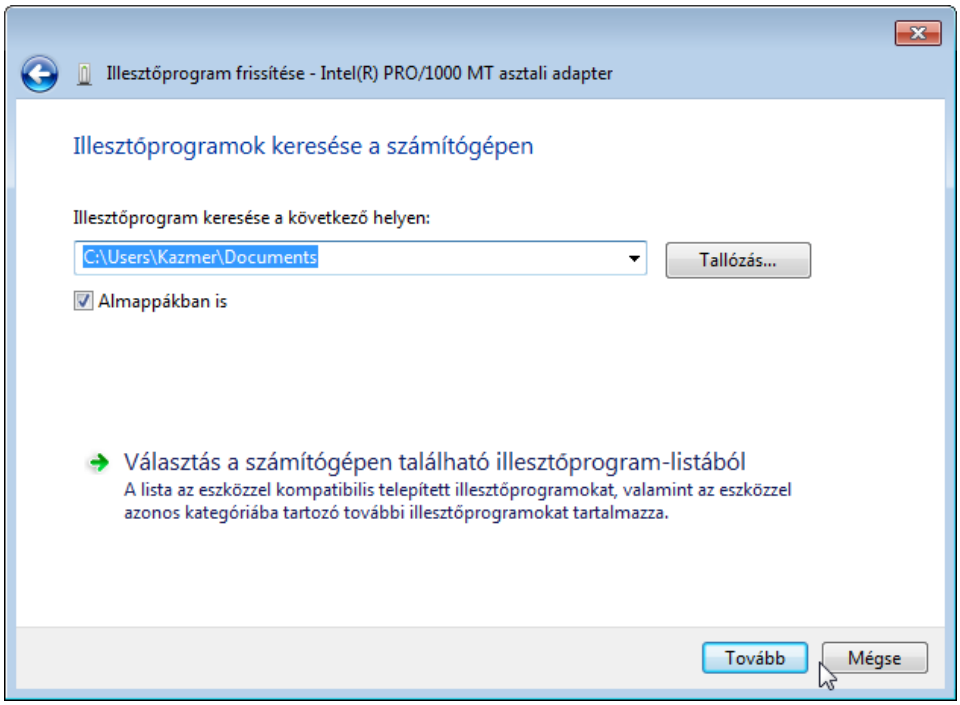
2. A PnP szolgáltatás lekéri az eszköz azonosítóit, ezzel azonosítja az eszközt.
3. A PnP szolgáltatás az ún. illesztőprogramtárban (amely a számítógépen található és a Windows telepítésekor jön létre) el kezdi keresni a hardverhez tartozó, megfelelő illesztőprogramot. Ha talál ilyet, akkor az illesztőprogramot a működési helyre másolja, amely rendszerint a %systemroot%\windows32\drivers mappa. Ha nem talál, akkor a DevicePath beállításjegyzékben (rendszerleíró adatbáis - Registry) megadott keresőmappákban kezdi el keresni. Ha ott sem találja, akkor a Windows Update helyen folytatja a keresést, ehhez a lépéshez internetkapcsolat szükséges. Ha ez a lépés is sikertelen, akkor a Windows elhelyezi a hardvert az egyéb eszközök között és a folyamat véget ér. Ilyen esetben az eszköz telepítését az illesztőprogram frissítése funkcióval lehet majd telepíteni.
4. Ha valamilyen módon megvan az illesztőprogram, a Windows ellenőrzi, hogy a felhasználó rendelkezik-e a megfelelő engedélyekkel. (Ez általában a rendszergazdai engedélyeket szokta jelenteni, de házirendben ez szabályozható.)
5. A Windows ellenőrzi, hogy az illesztőprogram rendelkezik-e megfelelő, érvényes tanúsítvánnyal. Ha rendelkezik és a tanúsítvány megtalálható a megbízható gyártók tanúsítványtárolóban, akkor az illesztőprogramot automatikusan az illesztőprogram tárolóba másolja. Ha a tanúsítvány nem található meg a megbízható gyártók tárolóban, akkor a telepítés egy további lépéssel bővül, melyben a Windows megerősítést kér a felhasználótól, hogy megbízhatónak tartja-e a gyártó illesztőprogramját.
6. Az illesztőprogram tárolóból a működési helyre másolódik az illesztőprogram. (általában a %systemroot%\windows32\drivers mappa).
7. A PnP szolgáltatás konfigurálja a beállításjegyzéket és bemutatja a Windowsnak, hogy hogyan kell használni az új hardvert.
8. A szolgáltatás elindítja az illesztőprogramot. Ezt a lépést a számítógép minden indításakor elvégzi.

Mint már említésre került, abban az esetben, ha a Windowsnak nem sikerült telepítenie a megfelelő illesztőprogramot, a felhasználó azt manuálisan az illesztőprogram frissítése funkció segítségével teheti meg. Ez a funkció azonban nem csak ilyen esetben használható, hanem akkor is, ha az adott hardverelemhez már új, frissebb illesztőprogram is létezik.



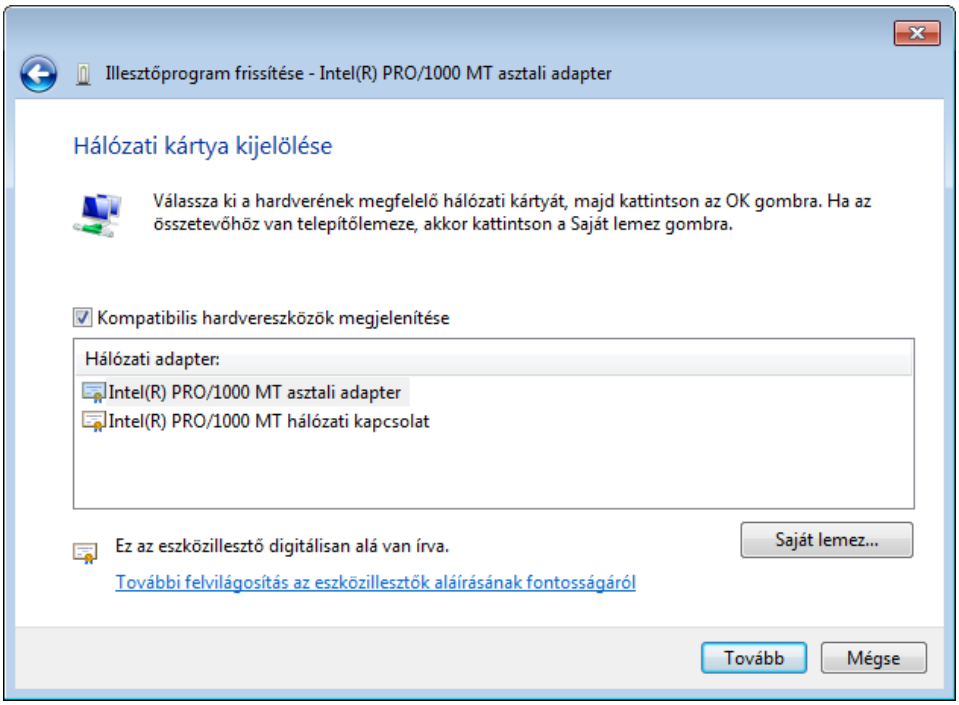
42. ábra: Illesztőprogram frissítése (Windows 7)

A művelethez az adott eszközre jobb gombal kattintva, a megjelenő listából az **illesztőprogram frissítése** (Update Driver Software) menüpontot kell kiválasztani. A megjelenő **illesztőprogram frissítése** párbeszédablakban két lehetőség közül lehet választani. Az egyik **a frissített illesztőprogramok automatikus keresése** (Search automatically for updated driver software), az automatikus frissítéshez. Célszerű ezt választani abban az esetben, ha valóban az illesztőprogram frissítése a cél, különösen akkor, ha az új illesztőprogram megtalálható a Windows Update webhelyen, az illesztőprogramtárban, vagy DevicePath beállításjegyzékben megadott mappák valamelyikében. Ezt a lehetőséget választva a Windows automatikusan telepíti a frissített illesztőprogramot, amennyiben az létezik és elérhető a felsorolt helyeken. A művelet végén a Windows tájékoztat a végeredményről, melyet a **bezárás** (Close) gombbal lehet nyugtázni.



43. ábra: Illesztőprogramok keresése a számítógépen (Windows 7)

A másik lehetőség, az **illesztőprogramok keresése a számítógépen** (Browse my computer for driver software), amikor kézi beavatkozást igényel a telepítés. Ezt a lehetőséget választva a megjelenő párbeszédablakban meg kell adni az **illesztőprogram keresése a következő helyen** (Search for driver software in this location) mezőben az illesztőprogramot tartalmazó mappa elérési útját. Ez beírható billentyűzetről is, de a **tallózás** (Browse) gombra kattintva ki is jelölhető a megjelenő mappastruktúrából. Ebben az esetben külső adathordozót (pl.: CD/DVD lemezt, USB pendrive-ot vagy egyéb USB külső tároló eszközt, de akár hálózati meghajtót) is meg lehet adni. Az **almappákban is** (Include subfolders) kapcsoló segítségével egy egész mappastruktúra legfelső szintjének magadásával esetén elérhető, hogy a Windows megkeresse a megfelelő illesztőprogramot, amennyiben az valamelyik almappában található. Az illesztőprogram helyének megadása után a **tovább** (Next) gombra kattintva a Windows automatikus megkeresi és telepíti a kérdéses illesztőprogramot, amennyiben az létezik és a megadott helyen található.



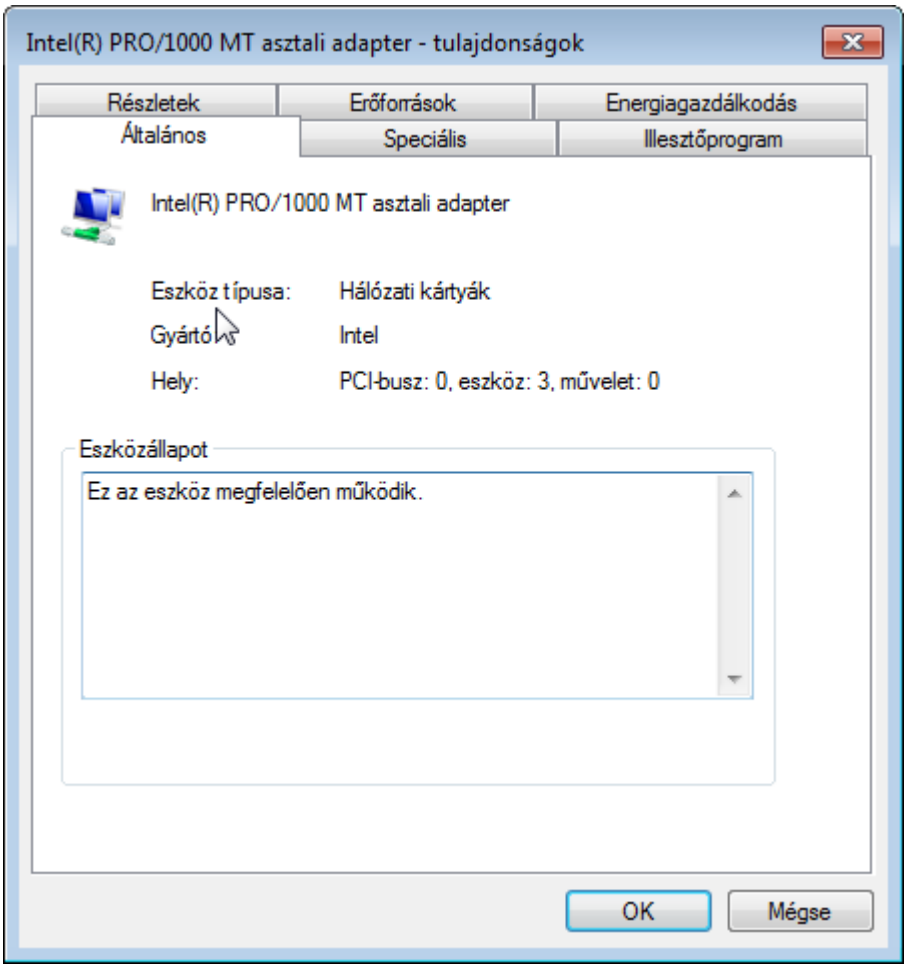
44. ábra: Illesztőprogram frissítése – hálózati kártya kijelölése (Windows 7)

A kézi telepítést választva más lehetőség is adódik a telepítésre, mint az illesztőprogram helyének megadása. Nevezetesen, a hely megadása helyett a **választás a számítógépen található illesztőprogram-listából** (Let me pick from a list of device drivers on my computer) lehetőséget választva megjelenik egy lista az adott eszköz típussal azonos típusú eszközök Windows által ismert illesztőprogramjairól. Ha a **kompatibilis hardvereszközök megjelenítése** (Show compatible hardware) be van kapcsolva, akkor csak a Windows által kompatibilisnek ismert illesztőprogramok láthatók a listában (és választhatók a listából). Ha ez a kapcsoló kikapcsolt állapotban van, a Windows által ismert összes ilyen típusú eszköz illesztőprogramja megjelenik, méghozzá gyártónként csoportosítva. Ha ebben a listában nem található meg a kívánt eszközillesztő, akkor a **saját lemez** (Have disk) gombra kell kattintani, a megjelenő párbeszédablakban pedig meg kell adni az illesztőprogram helyét, amelyet vagy közvetlenül beírva, vagy a tallózás gombra kattintás után a mappastruktúrából megjelölve kell megadni. Ezután a Windows automatikusan telepíti az illesztőprogramot.

További műveletek

Az eszközkezelőben az eszközre jobb gombbal kattintva az **illesztőprogram frissítésén** túl több funkció is elérhető. Először említendő az **eltávolítás** (Uninstall), amelynek segítségével az eszköz illesztőprogramja nem csak a

működési helyéről, hanem akár az illesztőprogramtárból is eltávolítható. Ez utóbbihoz a megjelenő párbeszédablakon a **törölje le az eszköz illesztőprogramját** (Delete the driver software for this device) kapcsolót be kell kapcsolni. Ez akkor lehet hatásos, ha a Windows egy már telepített hibás illesztőprogramot mindig újra akar telepíteni. Az eltávolítás funkció általában egy eszköz újratelepítésének első lépése szokott lenni.



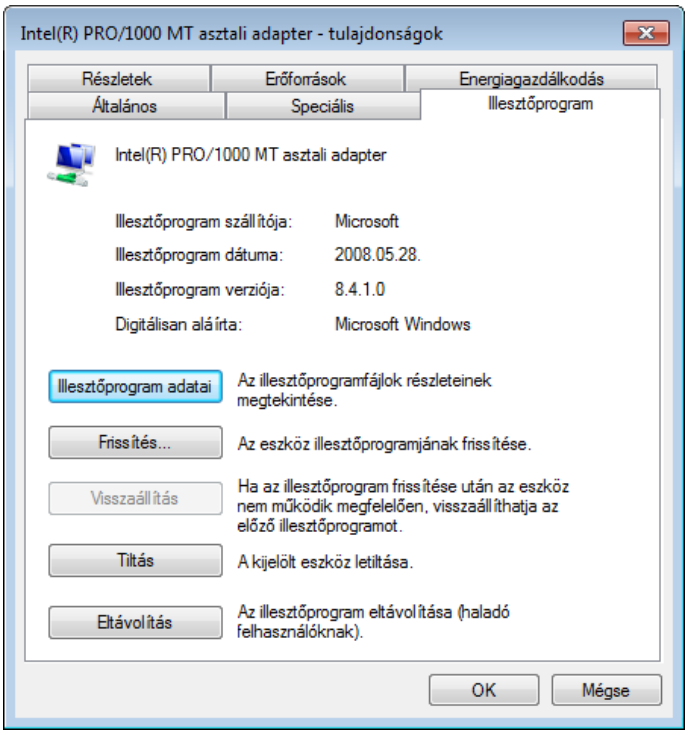
45. ábra: Eszköz tulajdonságok – általános lap (Windows 7)

Egy másik hasznos funkció az eszköz letiltása és engedélyezése, amely szintén az eszköz helyi menüjéből választható ki. Engedélyezett eszköz esetén a **tiltás** (Disable), tiltott eszköz esetén az **engedélyezés** (Enable) menüpont választható ki. Hasznos lehet különböző eszközök ütközéseinek vizsgálatára és kiküszöbölésére, vagy csak egyszerűen az illesztőprogram újraindítására.

A **hardverváltozások keresése** (Scan for hardware changes) funkció bármelyik eszköz helyi menüjéből választható. Segítségével a PnP szolgáltatás újból lekéri a csatlakoztatott eszközök azonosítóit és megvizsgálja, hogy azok telepítve vannak-e. Ha van olyan, amely nincs telepítve, azt a már ismertetett módon megpróbálja telepíteni. Akkor érdemes használni, ha a számítógéphez csatlakoztatott eszköz automatikusan nem jelenik meg az eszközkezelőben, illetve ha az eszköz előzőleg el lett távolítva, de még mindig csatlakoztatva van és az eszköz illesztőprogramjának újratelepítését kell elvégezni.

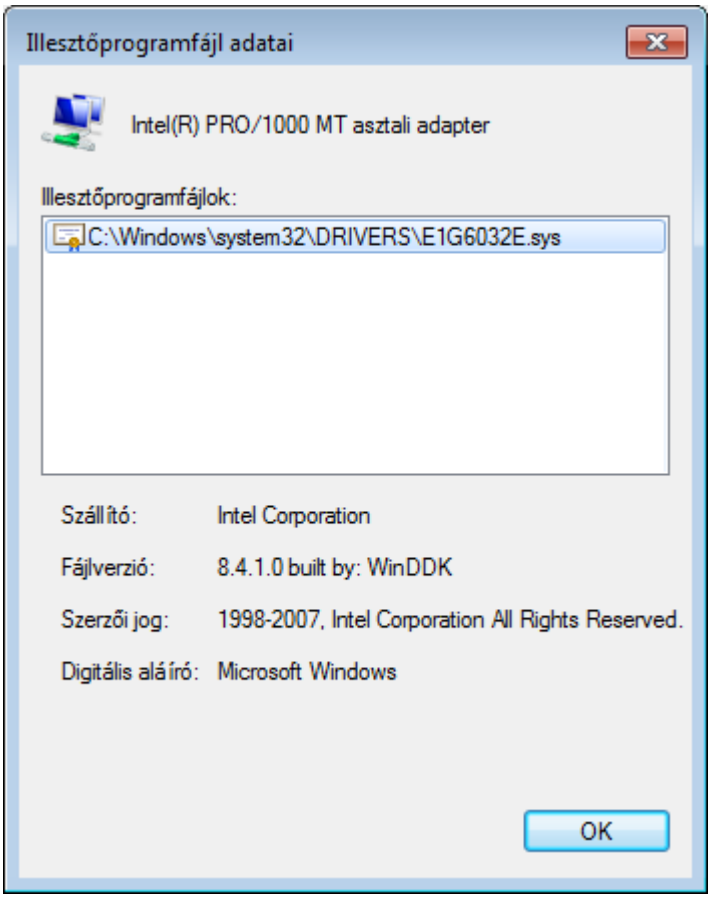
A helyi menüből a **tulajdonságokat** (Properties) választva, vagy az eszközre duplán kattintva az adott eszköz tulajdonságlapja jelenik meg. Az **általános** (General) lapon olvasható az eszköz neve, **típusa** (Device type), a **gyártó** (Manufacturer), és a **hely** (Location), ahol a hardvereszköz található. Ez utóbbi az eszköz számítógéphez való csatlakozási pontjának az azonosítója.

Ezek alatt található az **eszközállapot** (Device status) mező, amelyben az eszköz működésére vonatkozó információk, vagy hibaüzenetek olvashatók. Itt a kívánt üzenet az „Ez az eszköz megfelelően működik.”.



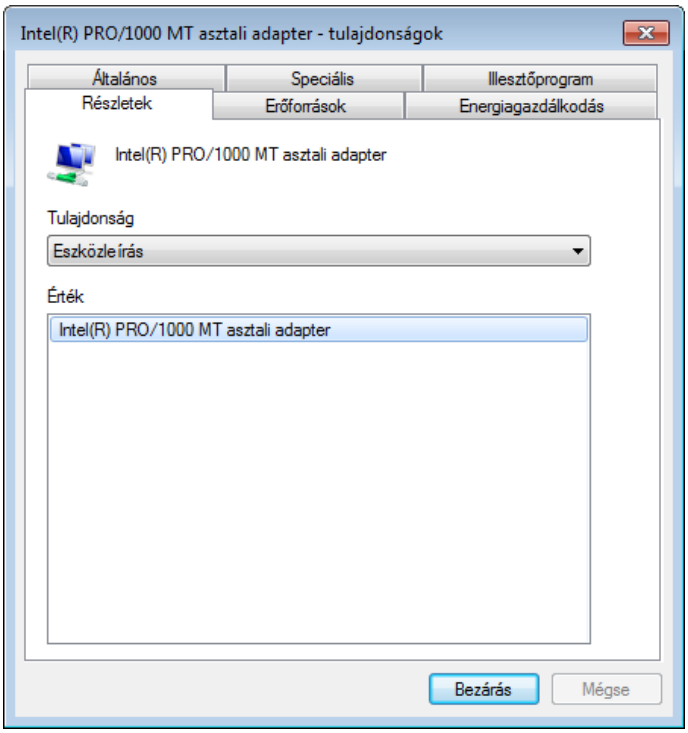
46. ábra: Eszköz tulajdonságok – illesztőprogram lap (Windows 7)

Az **illesztőprogram** (Driver) lapon az **illesztőprogram szállítója** (Driver Provider), **dátuma** (Driver date), **verziója** (Driver Version) és a **digitális aláírója** (Digital Signer) olvasható. Ezek alatt több gomb is található, melyek közül három funkciója máshonnan is elérhető és már ismertetésre került korábban. Ezek a **frissítés** (Update Driver), a **tiltás/engedélyezés** (Disable/Enable) és az **eltávolítás** (Uninstall).



47. ábra: Eszköz tulajdonságok – illesztőprogram adatai (Windows 7)

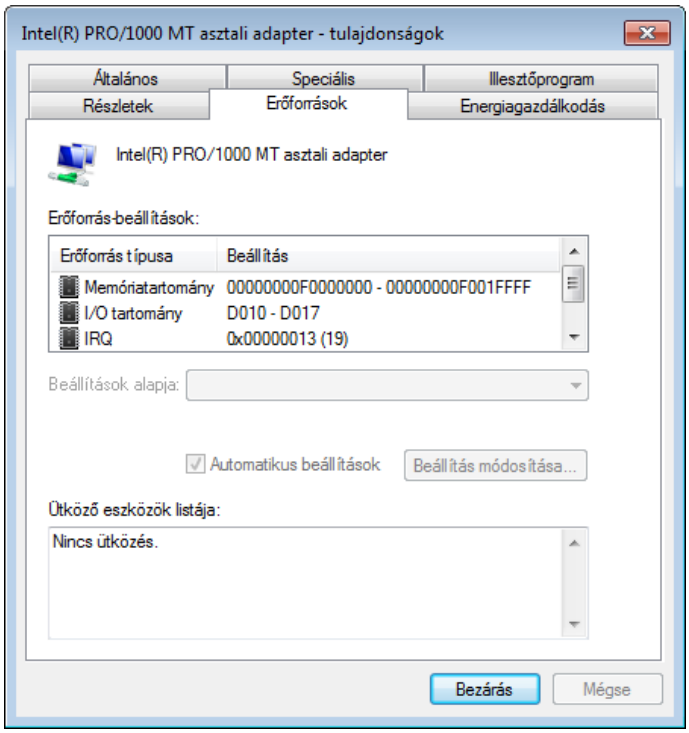
Az **illesztőprogram adatai** (Driver Details) gombra kattintva az azonos nevű adatlap jelenik meg, melynek **illesztőprogramfájlok** (Driver files) mezőjében felsorolt fájlok közül a kijelölt részletes adatai láthatók a lista alatt úgy, mint **szállító** (Provider), **fájlverzió** (File version), **szerzői jog** (Copyright), **digitális aláíró** (Digital Signer).



48. ábra: Eszköz tulajdonságok – részletek lap (Windows 7)

A **visszaállítás** (Roll back) gombra illesztőprogram frissítés után lehet kattintani abban az esetben, ha a frissített illesztő program nem működik megfelelően és ezért az eredeti állapot visszaállítása kívánatos.

A **részletek** (Details) adatlapon az eszköznek különböző **tulajdonságainak** (Property) **értékei** (Value) jeleníthetőek meg. Az **erőforrások** (Resources) lapon az olyan **erőforrás beállításokról** (Resource settings), mint az **I/O tartomány** (I/O Range), a **memóriatartomány** (Memory Range) vagy az **IRQ** megszakítás lehet tájékozódni, de az esetlegesen **ütköző eszközökkel** (Conflicting device list) kapcsolatban is itt lehet többet megtudni. Általában ezeket a beállításokat a Windows kezeli és a legtöbb esetben nem is lehet ezt módosítani. Ha van olyan eszköz, amelyiknél mégis lehetséges az automatikus beállítások kikapcsolása, ott a beállítás módosítása gombra kattintva módosíthatók az értékek. Azonban ez ilyen esetben sem célszerű, csak kivételes esetekben érdemes és akkor is csak szakembereknek.

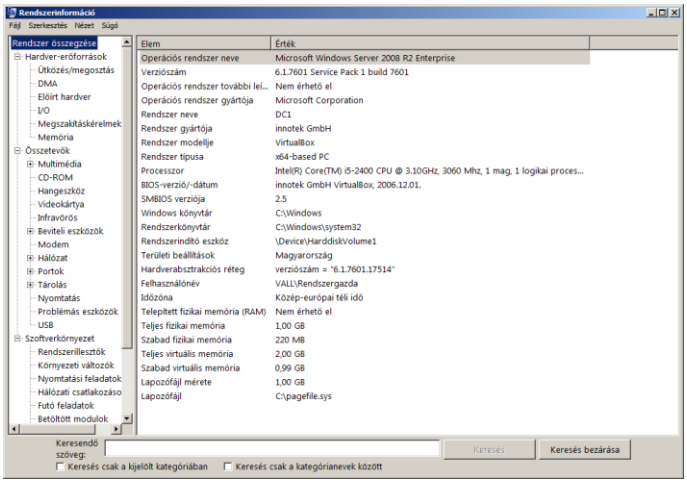


49. ábra: Eszköz tulajdonságok – erőforrások lap (Windows 7)

További lapok is előfordulhatnak, bár vannak olyan eszközök, amelyeknél az előzőleg bemutatott két lap sem található meg. A további lapokon eszközspecifikus beállítások találhatók, melyek módosítása ugyancsak szakértelmet igényel, ezért ezek esetén is érdemes az alapértelmezett értékeket használni.

Az eszközkezelő egy igen hasznos alkalmazás arra, hogy a számítógép hardver eszközeit és az ahhoz tartozó illesztőprogramokat karban lehessen tartani.

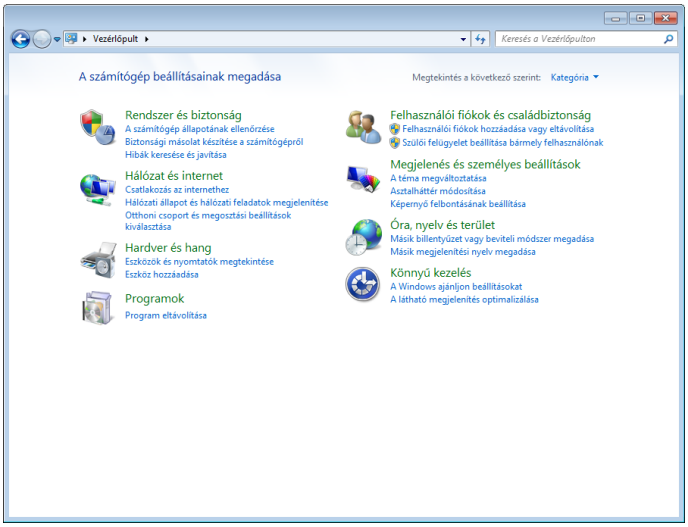
Az utóbbi fejezetekben említett eszközökön kívül található még egy alkalmazás, amelynek segítségével a hardver eszközökről részletesebb információt kaphat a felhasználó. Ez a rendszerinformáció alkalmazás, amely a **Start menü** (Start), **minden program** (All Programs) almenü, **kellékek** (Accessories) almenü, **rendszereszközök** (System Tools) almenüjében található **rendszerinformáció** (System Restore) menüponttal indítható.



50. ábra: Rendszerinformáció (Windows Server 2008 R2)

1.1.3 A vezérlőpult

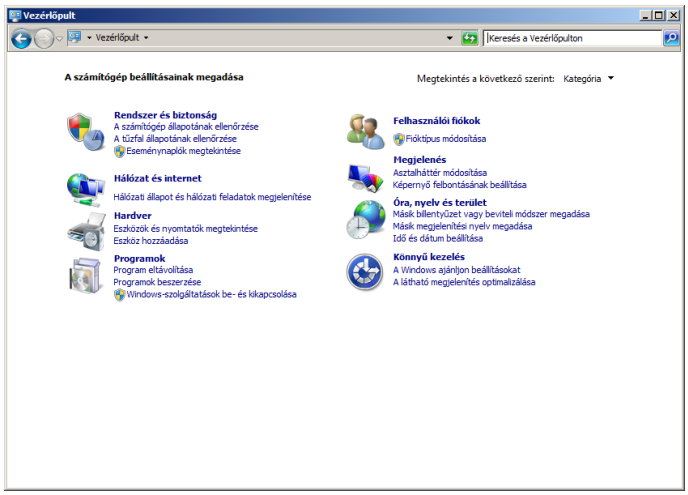
A **vezérlőpult** (Control Panel) a Windows beállításainak módosítására szolgáló eszköz, amely a Windows Start menüjéből érhető el. A vezérlőpult a Windows verziók fejlődésével együtt fejlődött.



51. ábra: A vezérlőpult (Windows 7)

A jelenlegi vezérlőpultban kétféle nézet közül lehet választani. Az egyik a kategóriánként elosztott nézet, a másik pedig az összes lehetőség megjeleníté-

se **kicsi** (Small icons) vagy **nagy ikonok** (Large icons) segítségével. Az alapértelmezett a **kategória** (Category) nézet, amelyet a **megtekintés a következő szerint** (View by) legördülő listával lehet módosítani.



52. ábra: A vezérlőpult (Windows Server 2008 R2)

Érdemes a kategória nézetet használni, mert valamivel áttekinthetőbb, a leggyakrabban használt lehetőségek közvetlenül is elérhetők, és abban az esetben, ha egy-két elem nem lenne megtalálható, még mindig lehet használni a **keresés a vezérlőpulton** (Search Control Panel) funkciót, amely az ablak jobb felső sarkában a nézet mód felett helyezkedik el.

A vezérlőpult elemei a következő kategóriákra vannak szétbontva:

- **Rendszer és biztonság** (System and Security): Ebben a kategóriában a **számítógép állapotának ellenőrzését** (Review your computer status) lehet elvégezni a **műveletközpont** (Action Center) eszköz segítségével, de innen érhetőek el a **biztonsági másolat a számítógépről** (Back up your computer), és a **hibák keresése és javítása** (Find and fix problems) funkciók is.
- **Hálózat és internet** (Network and Internet): Itt a **hálózati állapot és hálózati feladatok megjelenítésére** (View network status and tasks) kattintva a későbbiekben ismertetésre kerülő hálózati és megosztási központ indul el. Az **otthoni csoport és megosztási beállítások kiválasztása** (Set up sharing with a homegroup) lehetőségre kattintva az otthoni csoport olyan beállításait lehet módosítani, mint a különböző mappák megosztása, vagy az otthoni csoport jelszavának megadása, módosítása, de csak otthoni hálózati kapcsolat esetén.

- **Hardver és hang** (Hardware and Sound): A kategóriában az **eszközök és nyomtatók megtekintése** (View devices and printers) lehetőséget választva a megjelenő ablakban a számítógéphez csatlakoztatott különböző eszközök (Devices), illetve nyomtatók és faxok (Printers and faxes) válnak láthatóvá. Újabb eszköz illetve nyomtató telepítéséhez az **eszköz hozzáadása** (Add a device) illetve a **nyomtató hozzáadása** (Add a printer) gombot kell választani. Az **eszköz hozzáadása** (Add a device) a kategória nézetből közvetlenül is elérhető, akárcsak a **kapcsolódás kivetítőhöz** (Connect to a projector), melynek segítségével megadható, hogy mi és hogyan jelenjen meg a kivetítő képén. A **gyakran használt mobilitási beállítások megadása** (Adjust commonly used mobility settings) olyan beállítási lehetőségeket jelent, mint a hangerő és más hangbeállítások, az akkumulátor állapota és az energiagazdálkodási séma, a vezeték nélküli hálózat, a külső képernyő, a szinkronizáló központ és a bemutató beállításai.
- **Programok** (Programs): A programok kategória leggyakrabban használt funkciója a **program eltávolítása** (Uninstall a program), amelynek segítségével a telepített szoftverek biztonságosan távolíthatóak el a számítógépről. Ezenkívül természetesen rengeteg más funkció is elérhető, többek között a szolgáltatások kezelése, az alapértelmezett programok beállításai vagy az asztali minialkalmázások beállításai.
- **Felhasználói fiókok és családbiztonság** (User Accounts and Family safety): Ebben a kategóriában a **felhasználói fiókok hozzáadása vagy eltávolítása** (Add or remove user accounts) eszköz a helyi felhasználók és csoportok menedzsmentjét teszik lehetővé, míg a **szülői felügyelet beállítása bármely felhasználónak** (Set up parental controls for any user) segítségével a családi felügyelet szolgáltatást lehet beállítani. Ez utóbbi segítségével lehetségessé válik, hogy a szülők korlátozhassák a gyermekeik számítógép használatát. Ez utóbbit a Windows Essentials szolgáltatással kiegészítve akár online is szabályozható a gyermekek hozzáférése.
- **Megjelenés és személyes beállítások** (Appearance and Personalization): Innen olyan beállítási lehetőségek érhetőek el, mint a **téma megváltoztatása** (Change the theme), amely magában foglalja az asztal hátterétől kezdve az ablakok színein és a Windows által kiadott hangokon át a képernyőkímélőig minden beállítási módot. Az **asztalháttér megváltoztatása** (Change desktop background), mint gyakran használt beállítási lehetőség közvetlenül is elérhető a kategória nézetből. Ugyancsak gyakori megjelenítési beállítás a **képernyő felbontásának beállítása** (adjust screen resolution).

- **Óra, nyelv és terület** (Clock, Language and Region): A területi beállítások közül a leggyakrabban használt a **másik billentyűzet vagy beviteli módszer megadása** (Change keyboards or other input methods), amely segítségével a billentyűzetkiosztás nyelvét lehet megválasztani és beállítani. A **másik megjelenítési nyelv megadása** (Change display language) funkció csak Enterprise kiadás esetén érhető el. Ebben az esetben egyszerűen lehet pl. magyar nyelvű Windows-ról angol nyelvűre váltani.
- **Könnyű kezelés** (Ease of Access): Ez a kategória a csökkent képességű felhasználóknak nyújt segítséget. **A Windows ajánljon beállításokat** (Let Windows suggest settings) lehetőség egy varázslót indít el, amelynek segítségével a Windows egyszerű, öt kategóriában (látás, kézhasználat, hallás, beszéd, gondolkodás) feltett kérdéseire válaszolva automatikusan ajánl egy felhasználói környezetet. **A látható megjelenés optimalizálása** (Optimize visual display) segítségével tovább hangolható a rendszer megjelenítése a csökkent képességű felhasználó számára.

A vezérlőpult ezenkívül még rengeteg beállításnak a helye, ezeknek részletes tárgyalása túlmutat a tankönyv anyagán. A teljes ismertetéshez érdemes az operációs rendszer valamelyik referenciakönyvét áttanulmányozni.

3.2.5 Microsoft Networks – a Windows hálózati modellje

Egy Windows-t futtató számítógépekből álló hálózat alapvetően kétféle felépítést követ. A Microsoft a felhasználás helyszínét alapul véve, és így a felhasználás módjának szemszögéből próbálja megközelíteni a kérdést. Az egyik, és egyben az egyszerűbb színhely az otthon, a mód pedig az otthoni felhasználás, amelyre az a jellemző, hogy néhány felhasználó és pár számítógép egy adott szegmensre csatlakozva megpróbálja egymás erőforrásait használni. Ilyen jellegű felhasználás szokott előfordulni egyébként mikro cégek és irodák esetében is. Ezt a felhasználási típust és az erre kialakított hálózati felépítést nevezzük munkacsoportos (Workgroup) hálózatnak és alapjait már a MS-DOS-os időkben lerakta a gyártó.

A másik felépítés a vállalatok működésén, a számítógépek professzionális felhasználásán alapul. Erre a típusra olyan hálózati felépítést kellett kitalálni, amelynek segítségével kezelhetővé válik több száz, de akár több tízezer felhasználó és számítógép, illetve utóbbi megosztott erőforrásai is. Ennek a modellnek tartományi (Domain) hálózat a neve és alapjai a Windows NT-nél jelentek meg.

Munkacsoportok

A munkacsoportos hálózat egyenrangú számítógépekből áll, a gépek pedig egy laza, ún. egyenrangú (peer-to-peer) hálózatot alkotnak. Ez azt jelenti, hogy egyik gép sem vezérli a másikat, mégis el tudják egymás erőforrásait érni. Ehhez a munkacsoport elérni kívánt gépén rendelkezni kell egy felhasználói fiókkal (User Account). Mivel egy egyenrangú hálózatban előfordulhat, hogy minden számítógépnek van olyan erőforrása, amelyet egy másik számítógépről el szeretnénk érni, ezért célszerű minden számítógépen minden felhasználónak felhasználói fiókot készíteni. Könnyen belátható, hogy nagy számítógépszám és nagy felhasználói létszám esetén ennek a rendszernek a működtetése, karbantartása, üzemeltetése igen nagy kihívást jelent, ezért a munkacsoportos modellt a kis felhasználói létszámú, néhány számítógépet (max. 10-20) tartalmazó, nagyrészt egy hálózati szegmensből álló helyi hálózatoknál (Local Area Network – LAN) célszerű kialakítani és működtetni.

Tartományok

A tartományi hálózati modell egyik legfontosabb jellemzője, hogy tartalmaz kiszolgáló (szerver) számítógépeket. Ez által egy ún. szerver-kliens hierarchiájú hálózat jön létre, amelyben a szerver számítógép osztja meg erőforrásait a hálózat többi számítógépe és felhasználója között. A Windows tartományi hálózat azonban még ennél a klasszikus struktúránál is tovább megy. A hálózat bármelyik számítógépe megoszthatja bármilyen erőforrását a többi számítógéppel úgy, hogy a felhasználói fiókok és a hozzáférési engedélyek egy kiemelt szerepű szerver számítógépen, az ún. tartományvezérlőn (Domain Controller – DC) helyezkednek el. Látszik, hogy a központosított felhasználói adminisztráció nagyban megkönnyíti a rendszer kezelhetőségét nagy, akár több tízezres számítógépszám és nagy felhasználói létszám esetén is. Tartományi hálózatban egyetlen felhasználói fiók segítségével akár a hálózat bármelyik számítógépére be lehet lépni és használni lehet azt, miközben a felhasználói környezet nem változik. Ennél a hálózati felépítésnél a számítógépek akár különböző hálózatokban is lehetnek, még úgy is, hogy a világ két különböző pontján helyezkednek el. A tartománnyal kapcsolatos információk, a felhasználói fiókok, a megosztott erőforrások stb., mind egy speciális adatbázisban, a címtárban, az ún. Active Directoryban (AD) találhatók. A Windows tartományok természetesen össze is kapcsolhatók és struktúrába – fába, vagy akár erdőbe is szervezhetők. Részletesebben a címtár fejezet foglalkozik a témával.[18]

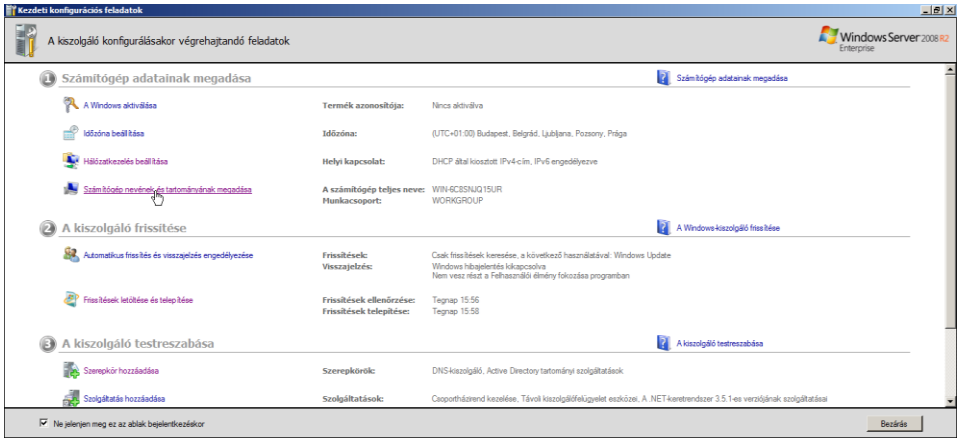
[18] William R. Stanek: Windows Server 2008, a rendszergazda zsebkönyve, Redmond, Washington, USA, Microsoft Corporation, 2008 (Magyar kiadás, Bicske, Szak Kiadó, 2008)

3.2.6 Windows hálózati konfiguráció

A tankönyv fő gerincét a Windows vállalati felhasználása adja, így a hálózati konfiguráció is ezt figyelembe véve kerül ismertetésre. Mivel a Windows szerver és munkaállomás verziói az alapszolgáltatásokban és konfigurációs beállítási lehetőségekben nagyrészt megegyeznek, ezért a Windows Server 2008 R2 verzió beállításai lesznek ismertetve, és ha ettől különbözik a Windows 7 beállítása, csak akkor lesz ez külön feltüntetve.

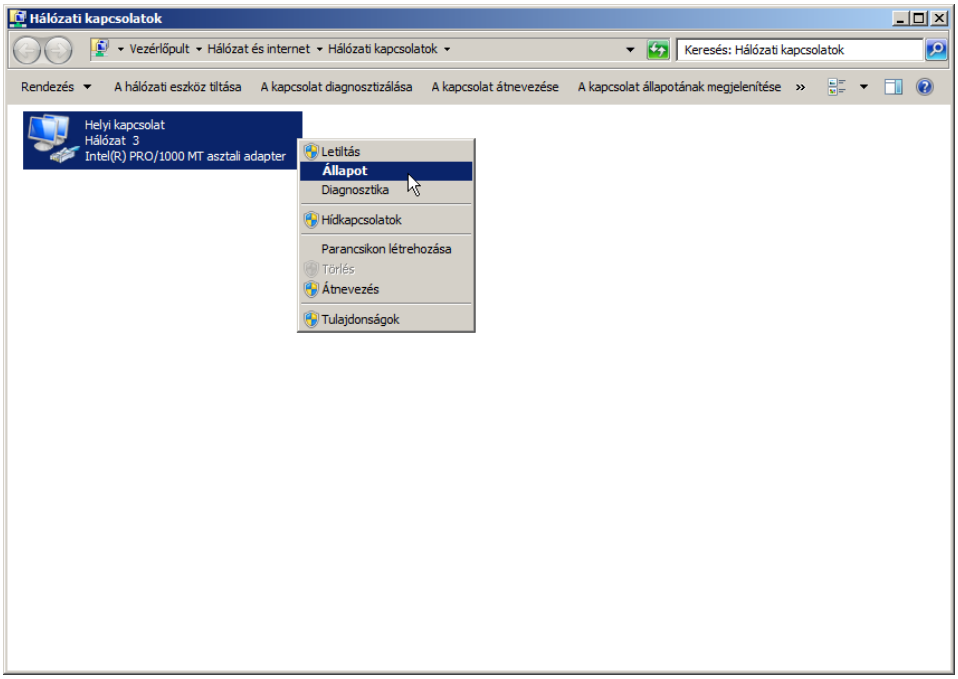
Hálózati kapcsolatok és a kapcsolatok állapota

A Windows Server 2008 R2 telepítés utáni indítási képernyőjén automatikusan elinduló **kezdeti konfigurációs feladatok** (Initial Configuration Tasks) ablaka abból a szempontból egy jó dolog, hogy a fontos, már a telepítés után végrehajtandó és végrehajtható feladatokat egy csokorba szedi és így nehéz pl. a kezdeti hálózati konfigurációs lépéseket kihagyni. Mindenesetre, ha ennek az ablaknak a megjelenítése indításkor ki lett kapcsolva, akkor sincsen nagy gond, mert a szükséges funkciók eredeti helyéről történő elérése is ismertetésre kerül, már csak azért is, mert a Windows 7 klienseken nincsen ilyen ablak.



53. ábra: Kezdeti konfigurációs feladatok (Windows Server 2008 R2)

A megjelenő feladatok közül jelenleg csak a hálózatkezelés beállítása és a számítógép nevének és tartományának megadása érdekes. A **hálózatkezelés beállítására** (Configure networking) kattintva a **hálózati kapcsolatok** (Network Connections) ablaka jelenik meg, és benne a számítógép telepített hálózati kapcsolatai.

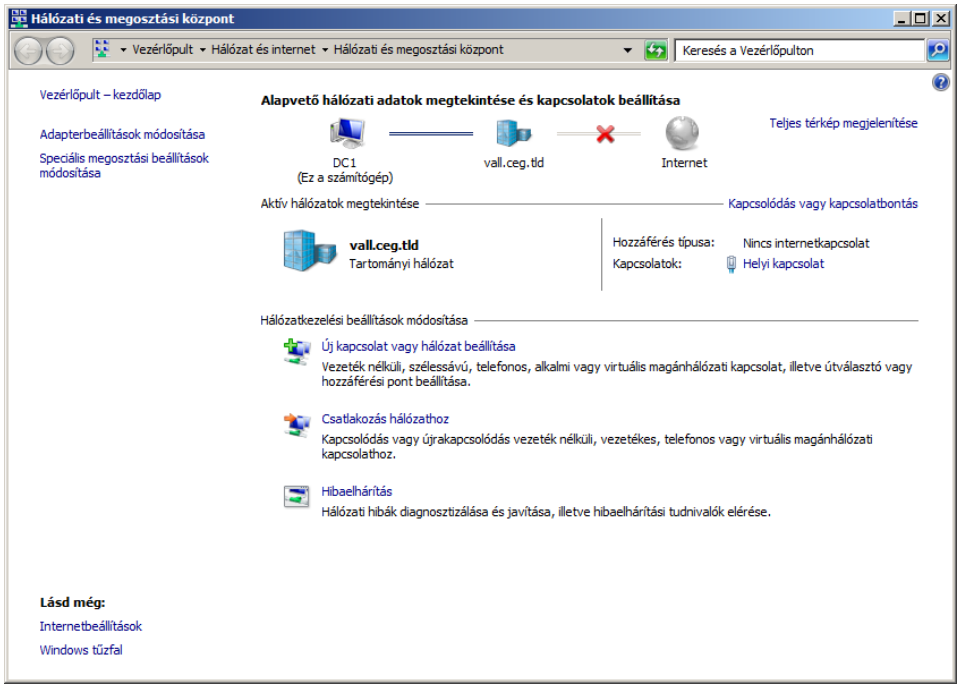


54. ábra: Hálózati kapcsolatok (Windows Server 2008 R2)

Windows 7 esetében, vagy ha a kiszolgálón nem a kezdeti konfigurációs feladatok a kívánt konfigurációs eszköz, akkor először is a hálózati és megosztási központot kell elérni valahogyan, ugyanis a hálózati kapcsolatok ablaka a **hálózati és megosztási központ** (Network and Sharing Center) ablakának bal oldalán lévő oszlopban az **adapterbeállítások módosítását** (Change adapter settings) kiválasztva jeleníthető meg.

A **hálózati és megosztási központ** leggyorsabban pedig a tálca jobb alsó sarkában, a hangszóróikon mellett található hálózati ikonra kattintva, majd a megjelenő menüben legalul a hálózati és megosztási központ megnyitására kattintva érhető el.

Azonban a központ elérhető akár a vezérlőpult **kategória** (Category) nézetében a **hálózat és internet** (Network and Internet) pont alatti **hálózati állapot és hálózati feladatok megjelenítése** (View network status and tasks) szövegre kattintva, vagy teljes nézetben a **hálózati és megosztási központra** kattintva is.



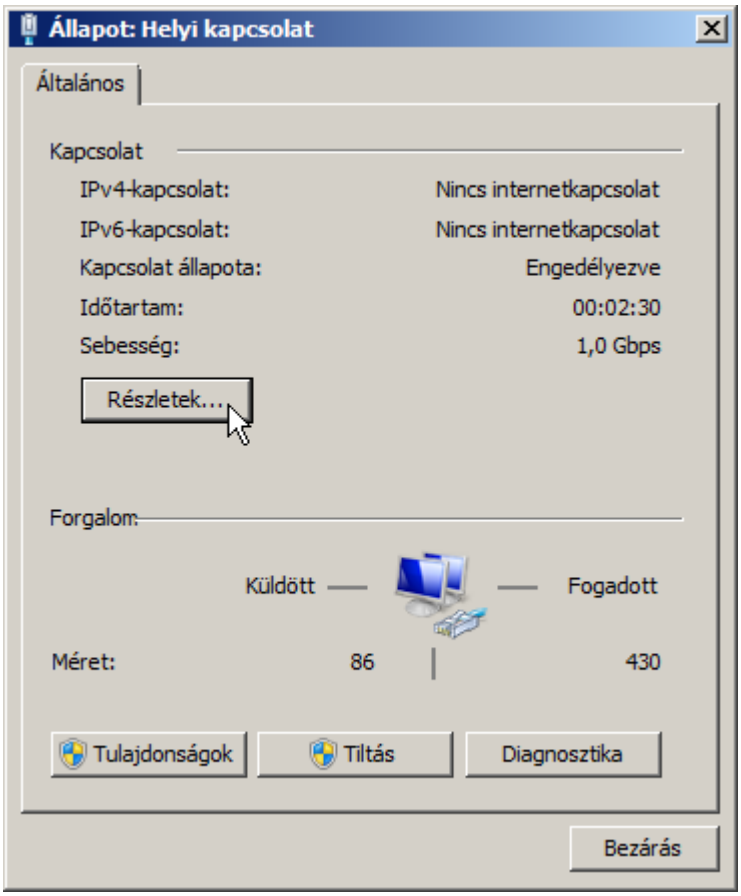
55. ábra: Hálózati és megosztási központ (Windows Server 2008 R2)

Egy helyi hálózatban lévő számítógépnek – mint a virtuális tesztkörnyezetben is – lennie kell legalább egy helyi hálózati interfésznek, amely **helyi kapcsolat** (Local Area Connection) néven látszik. A kapcsolat neve alatt látszik annak a hálózatnak a neve, amelyhez kapcsolódik, a hálózat neve alatt pedig a hálózati interfész, kártya típusa látható.

Ha a **helyi kapcsolat** ki van jelölve, megjelenik felette az eszköztáron pár funkció, amelyet a kapcsolattal el lehet végezni. Az első **a hálózati eszköz tiltása** (Disable this network device), amellyel gyakorlatilag ki lehet kapcsolni a hálózati interfészt és így ezt a kapcsolatot is. Kikapcsolás után **a hálózati eszköz tiltása** helyett **a hálózati eszköz engedélyezése** (Enable this network device) látszik. Erre kattintva újra engedélyezhető lesz az interfész és így a kapcsolat is.

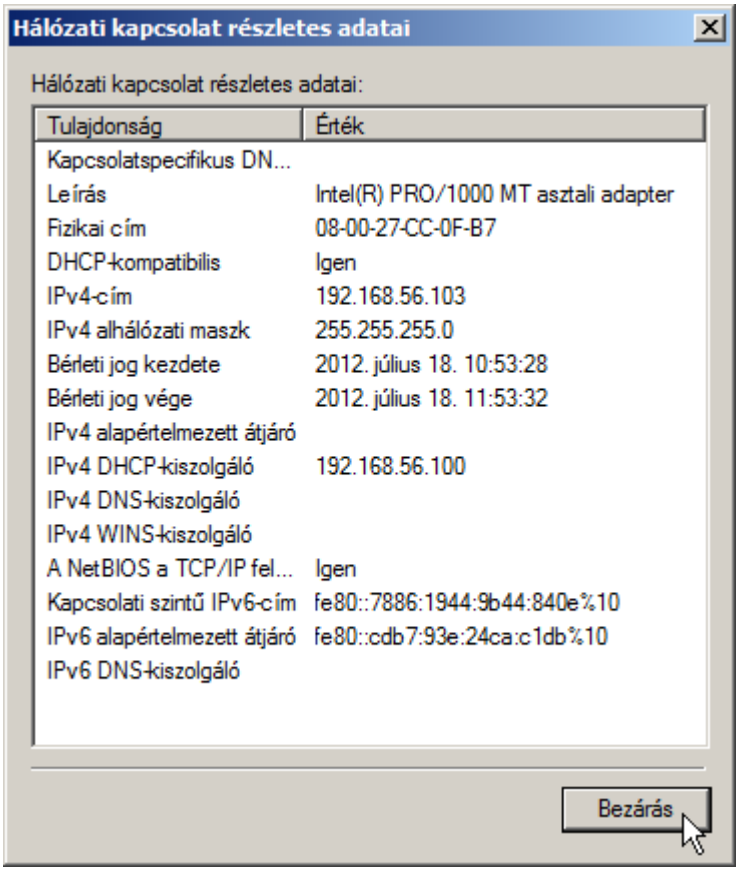
A kapcsolat diagnosztizálása (Diagnose this connection) funkció az ún. **hálózati hibaelhárítót** (Windows Network Diagnostics) indítja el, amely egyszerűbb, automatikusan helyrehozható hálózati problémák megoldására készült, hogy azokat a hozzá nem értő, nem rendszergazda felhasználók is elvégezhessék. Ilyen probléma, pl. ha a kliens valamiért nem kapta meg az IP beállításokat a DHCP kiszolgálótól. Az újrakéréshez elég a diagnosztizálásra kattintani.

A kapcsolat átnevezése (Rename this connection) segítségével módosítható a hálózati kapcsolat neve.



56. ábra: Állapot Helyi kapcsolat (Windows Server 2008 R2)

A kapcsolat állapotának megjelenítése (View status of this connection) funkció a kapcsolatra vonatkozó információkat megjelenítő tulajdonságlapot nyitja meg. A lapon a **kapcsolat** (Connection) szakaszban az internet protokoll (Internet Protocol – IP) 4-es és 6-os verziójának (IPv4, IPv6) állapota látható az internethez való csatlakozás szempontjából. Ezenkívül még látható a **kapcsolat állapota** (Media State), a kapcsolat helyreállása óta eltelt **időtartam** (Duration) valamint a kapcsolat sebessége. Ha ez az információ mennyiség nem kielégítő, akkor érdemes a **részletek** (Details) gombra kattintani.



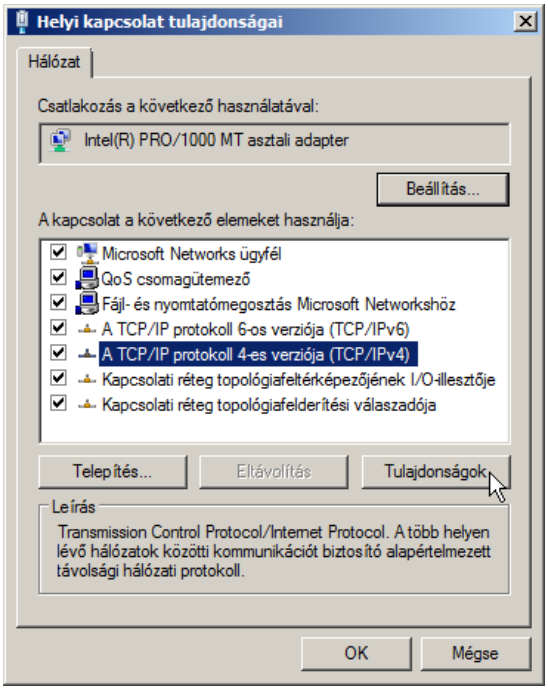
57. ábra: Hálózati kapcsolat részletes adatai (Windows Server 2008 R2)

A **hálózati kapcsolat részletes adatai** (Network Connection Details) adatlapon többek között a **DNS utótagot** (Connection-specific DNS suffix), a hálózati adapter nevét a **leírás** (Descripton) mezőben, a **fizikai címet** (MAC Address), az alap IPv4-es beállításokat, mint **IP cím** (IP Address), **alhálózati maszk** (Subnet Mask), **alapértelmezett átjáró** (Default Gateway), **DNS kiszolgálók** (DNS Servers) címe. Ha az IPv4 konfiguráció DHCP szolgáltatás segítségével történt, akkor a kiszolgáló címe (DHCP Server), a **bérleti jog kezdete és vége** (Lease Obtained and Expires) adatok is megjelennek.

NetBIOS használata TCP/IP felett (NetBIOS over TCP/IP – NBT) akkor lehet indokolt, ha a hálózatban vannak olyan számítógépek, amelyek ilyen alapon nyújtanak fájl és nyomtató megosztási szolgáltatást. Ezt főleg a régi Windowsok (Windows 2000 előtt) használták, de a visszafele kompatibilitás miatt azóta is bekapcsolva maradt mind a kiszolgálókban, mind a munkaállomásokban. Ha van NetBIOS a hálózatban előfordulhat, hogy van Windows internetes névfelol-

dási kiszolgáló is (Windows Internet Naming Server – WINS), ha pedig az be van állítva akár manuálisan, akár DHCP segítségével, akkor a kiszolgáló címe itt olvasható. Végül az IPv6-os alapbeállítások láthatók, mint **IP cím** (IPv6 Address), **átjáró címe** (Default Gateway), **DNS kiszolgáló** címe (DNS Server). A Windows már régóta támogatja az IPv6-ot, de az igazán jól működő IPv4-IPv6 **kettős protokollverem** (Dual-Stack) csak a Windows 2008-tól van jelen. A tankönyv a továbbiakban az IPv6-os konfigurációval nem foglalkozik.

Visszatérve a **kapcsolat tulajdonságlaphoz** a **forgalom** (Activity) szakaszban megjelenítésre kerül az interfész által **küldött** (Sent) és **fogadott** (Received) bájtok száma, itt lehet ellenőrizni, hogy van-e hálózati forgalom az interfészen. Az itt található **tulajdonságok** (Properties) gomb hatására a következő funkció ismertetésében megjelenő **helyi kapcsolat tulajdonságai** (Local Area Connections Properties) adatlapot jeleníti meg. A további gombok már ismertetett funkciókat hívnak elő, úgymint a hálózati eszközre vonatkozó **tiltás** (Disable), vagy a **diagnosztika** (Diagnose).



58. ábra: A helyi kapcsolat tulajdonságai

A kapcsolat beállításainak módosítása (Change settings of this connection) a **kapcsolat tulajdonságai** adatlapot jeleníti meg. A **csatlakozás a következő használatával** (Connect using) mező a használt hálózati interfész

(adapter) nevét jeleníti meg. Az erre vonatkozó beállításokat a **beállítás** (Settings) gombra kattintva lehet elérni. A beállítások magára a hardvereszközre vonatkoznak és ugyanaz az adatlap jelenik meg ekkor, mintha az eszközkezelőből lett volna egy hardvereszköz tulajdonságlapja megnyitva.

A **helyi kapcsolat tulajdonságai** adatlapon **a kapcsolat a következő elemeket használja** (This connection uses the following items) ablakban a kapcsolatban használt, szerver (szolgáltatás), kliens (ügyfél) és protokoll összetevők jelennek meg. Új elemek is felvehetők a listába a **telepítés** (Install) gombra kattintva, illetve a kijelöltek eltávolíthatók az **eltávolítás** (Uninstall) gombbal. (Telepítésre egyébként nem sok lehetőség adódik, hacsak nem valamilyen egyéb gyártó terméke, amely rendelkezésre áll külön lemezen.) A listában található elemek ki és bekapcsolhatók a nevük előtt lévő kapcsoló ki és bejelölésével. A lista egy elemét kijelölve, ha elérhető a **tulajdonságok** (Properties) gomb, akkor az elem tulajdonságlapja jelenik meg.

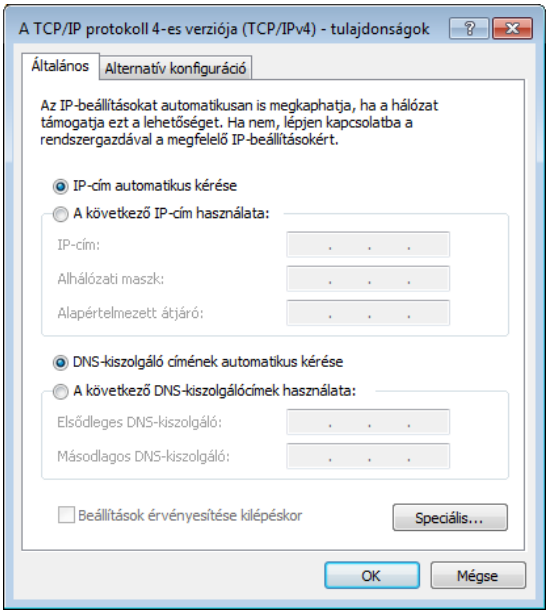
Alapértelmezésben mind a kiszolgálón, mind a munkaállomáson telepítve van a **fájl- és nyomtatómegosztás Microsoft Networkhöz** (File and Printer Sharing for Microsoft Networks) szerver összetevő, amely a Windows hálózatok tulajdonképpeni fájl kiszolgálója. Természetesen az ehhez tartozó kliens is telepítve van alapból, ez a listában a **Microsoft Network ügyfél** (Client for Microsoft Networks) néven szerepel. Ezenkívül még egy szolgáltatás van telepítve, ez a QoS (Quality of Service) csomagütemező, amely a hálózati forgalom vezérlését biztosítja, beleértve az átviteli sebesség szabályozását és a forgalmi prioritások meghatározását.

Alapértelmezésben négy különböző protokoll elem van telepítve, amelyből az IPv4-gyel foglalkozik a tananyag részletesebben. Az IPv6-tal, amely gyakorlatilag az új generációs internet alap protokollja, a helyi hálózatokban még nem elég elterjedt. A **kapcsolati réteg topológiafeltérképezőjének I/O-illesztője** (Link-Layer Topology Discover Mapper I/O Driver), illetve a **kapcsolati réteg topológiafelderítési válaszadója** (Link-Layer Topology Discover Responder) a Windows-ok egy olyan szolgáltatásához szükséges, amelynek segítségével a hálózati infrastruktúra elemei felderíthetőek. A hálózati térkép szolgáltatás a hálózati és megosztási központ teljes térkép megjelenítése szövegre kattintva érhető el, és a Windows itt megpróbálja grafikusan megjeleníteni a hálózat elemeit.

IPv4 beállítások kliensek esetén

A TCP/IPv4-et kiválasztva és a tulajdonságok gombra kattintva az általános IP beállítások adatlapja jelenik meg. **Automatikus konfiguráció** (Obtain an IP address automatically) esetén az IP beállításokat egy, a hálózatban megtalálható DHCP kiszolgáló fogja szolgáltatni. Kliens számítógépek esetén általában ez

a választás a megfelelő, hacsak nincs valami különösebb oka az IP kézi konfigurációjának.



59. ábra: Szokásos TCP/IP beállítások (Windows 7)

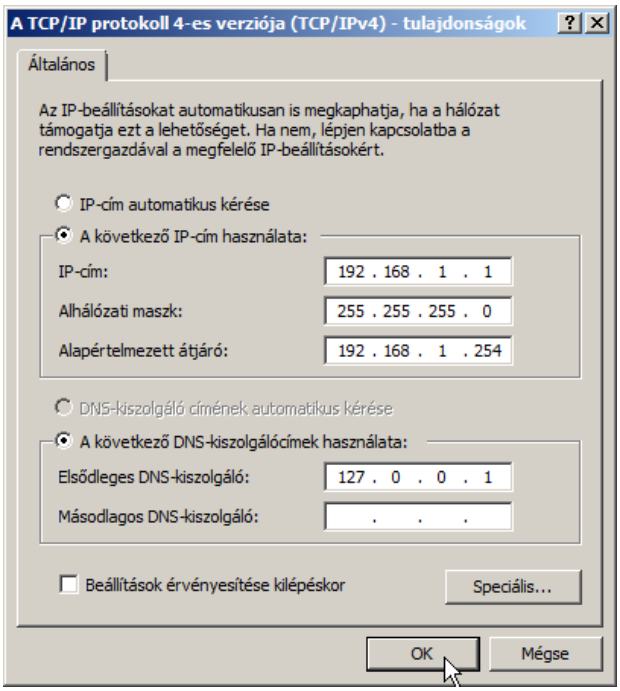
Abban az esetben, ha a hálózatban nem található DHCP kiszolgáló, vagy az valamiért nem érhető el, illetve nem válaszol, akkor az **automata privát IP címzés** (Automatic Private IP Addressing – APIPA) folyamata lép életbe. Ennek segítségével ilyen esetben is kaphat a számítógép egy 169.254.x.y formátumú IP címet 255.255.0.0 alhálózati maszkkal (a 169.254.0.0 – 169.254.255.255 privát IP tartományból), ahol az x és az y az ügyfél egyedi azonosítója. Ennek a címnek a segítségével csak a helyi hálózatban tudnak a számítógépek kommunikálni, és ott is csak akkor, ha az összes számítógép ilyen típusú IP címet kap, így kerülnek ugyanis egy IP hálózatba.

A **DNS-kiszolgáló címének automatikus kérését** (Obtain DNS Server address automatically) szintén a kliens számítógépek esetén érdemes bekapcsolni, legalábbis abban az esetben, ha a hálózatban van olyan DHCP kiszolgáló, amely szolgáltat DNS kiszolgáló címet. Ez vállalati infrastruktúrában természetesen alap.[19]

[19] Petrényi József: Windows Server 2008, TCP/IP alapok, I. kötet, v2.0, Budapest, Microsoft Magyarország, 2010

IPv4 beállítások a szerverek esetén

Kiszolgáló számítógépek estén általában nem javasolt az automatikus IP konfiguráció, hiszen az automatikus konfiguráció alaphelyzetben nem garantálja, hogy a számítógép adott hálózati interfésze mindig ugyanazt az IP címet fogja kapni. Ha megváltozik a kiszolgáló IP címe, előfordulhat, hogy a kliensek nem érik el többé. Másrészt abban az esetben, ha a DHCP kiszolgáló valamilyen okból nem elérhető, a kiszolgáló nem kapja meg IP beállításait és megint csak elérhetetlen lesz.



60. ábra: Szokásos TCP/IP beállítások (Windows Server 2008 R2)

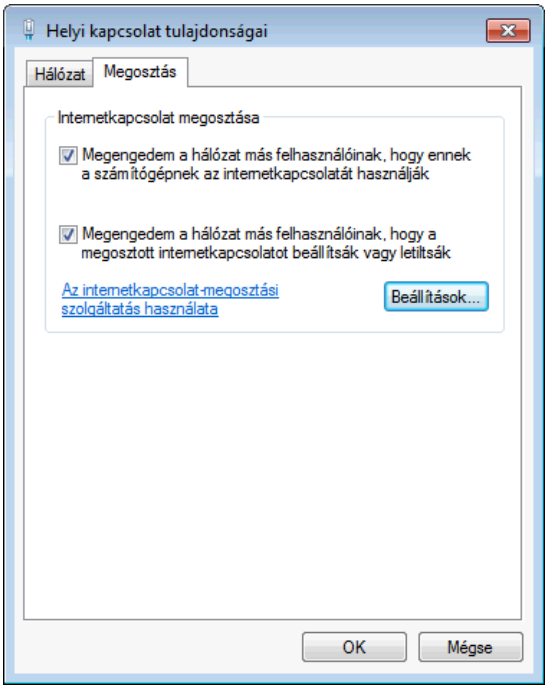
Speciális esetek is léteznek. Egy DHCP kiszolgáló esetén pl. muszáj manuálisan megadni az IP címet főként, ha egy több hálózatot kezelő központi DHCP kiszolgálóról van szó.

IPv4 beállítások a virtuális tesztkörnyezetben

A virtuális tesztkörnyezet hálózatának létrehozása több részből áll. A VirtualBox telepítésével egy időben létrejött egy ún. **csak gazdagép hálózathoz** (VirtualBox Host-Only Network) tartozó **hálózati interfész** (VirtualBox Host-Only Ethernet Adapter). Ez a hálózati interfész fogja tartani a kapcsolatot a virtuális hálózatban található **virtuális gépek** (VM) interfészeivel. A telepítés után tehát létrejött a hálózat egyik része, a többi rész pedig akkor jön létre, amikor a kü-

lönböző VM-eken beállításra kerülnek ugyanezen hálózathoz tartozó Host-Only hálózati interfészek. Látható, hogy a hálózat létrehozásával különösebben nem kell foglalkozni, azonban a megfeleő működéshez pár beállításra és trükkre még szükség lesz.

Mivel így egy zárt hálózat alakul ki, amely nem kapcsolódik semmilyen más hálózathoz, így az internethez sem (és ez akkor is igaz, ha a gazdagépnek van internet kapcsolata), pedig utóbbi elérésre mindenképpen szükség lesz. Nem nehéz elképzelni, hogy ez valóban így van, hiszen a különböző frissítések, programcsomagok nagyrészt már csak az Interneten keresztül érhetők el. A probléma megoldásához a legjobb, ha egy olyan, két hálózati interfésszel épített VM kerül telepítésre, amely egyben útválasztó és esetlegesen támogatja a hálózati címfordítást is. Ez utóbbi persze nem szükséges, ha az egyik Host-Only interfész mellett a másik interfész NAT típus. Ha azonban az útválasztónál pont a hálózati címfordítás kipróbálása a cél, akkor a virtuális hálózat létrehozásához érdemes a bridge-elt kártya (Briged Adapter) típust választani, ekkor viszont szükség lesz egy a gazda gép hálózati interfészével egy IP hálózatban található IP címre. Mivel ennek megvalósítása túlmutat a tankönyv témáján, ezért nem kerül tárgyalásra.



61. ábra: Mi lesz az átjáró? Internet kapcsolat megosztása a gazda gépen

A probléma megoldásához nem kötelező azonban útválasztó VM-et telepíteni, mivel egy kis trükkel megoldható a Host-Only hálózat tagjainak az internetelérés. A trükk az, hogy engedélyezni kell a gazdaszámítógép internet elérést biztosító hálózati interfészén az internetkapcsolat megosztását (Internet Connection Sharing). Ehhez a gazdagépen a hálózati és megosztási központban (Network and Sharing Center) az Internet csatlakozást biztosító kapcsolat nevére kattintva, majd a megnyíló kapcsolat állapot lapján (Connection Status) a tulajdonságok (Properties) gombra kattintva meg kell nyitni a hálózati kapcsolat tulajdonságlapját. Ennek megosztás (Sharing) fülére kattintva, az internetkapcsolat megosztása (Internet Connection Sharing) mezőben pedig ki kell választani a megengedem a hálózat más felhasználóinak, hogy ennek a számítógépnek az internetkapcsolatát használják (Allow other network users to connect through this computer's Internet connection) kapcsolót.

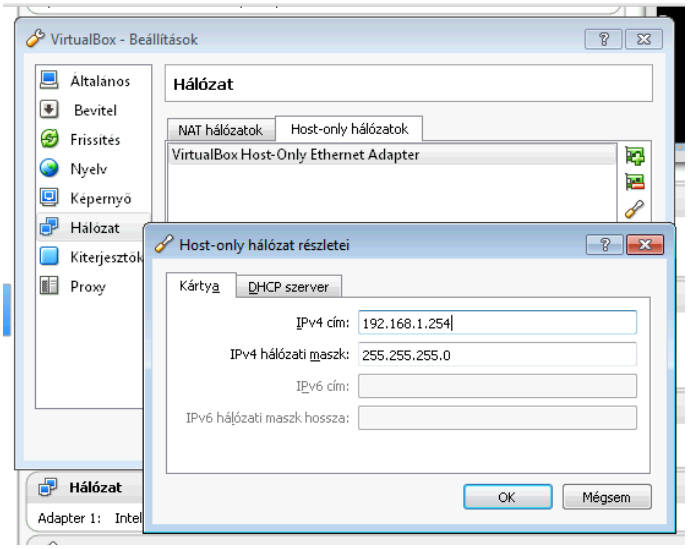
Az internetkapcsolat beállítása tehát ilyen hálózati környezetben már megoldottnak tekinthető, azonban még hátra van a virtuális hálózat IP hálózatának beállítása. Erre különböző okok miatt van szükség. Először is a virtuális tesztkörnyezetben a kliensek beállításához ugyan nem kell nyúlni, megfelelő az alapértelmezett automatikus IP konfiguráció (Obtain an IP address automatically) és a DNS kiszolgáló automatikus kérése (Obtain DNS server address automatically), viszont a kiszolgáló számítógépek esetén manuálisan megadott statikus beállításokra lesz szükség. A következő táblázat a virtuális tesztkörnyezetben található kiszolgálók IP beállításait tartalmazza.

5. *Kiszolgálók IP beállításai*

név	dc1	dc2	rodc
tartomány	vall.ceg.tld	vall.ceg.tld	vall.ceg.tld
IP cím	192.168.1.1	192.168.1.2	192.168.1.3
Netmask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.254	192.168.1.254	192.168.1.254
DNS1	192.168.1.1	192.168.1.2	192.168.1.3
DNS2	192.168.1.2	192.168.1.1	192.168.1.1

Speciális IPv4 beállítások

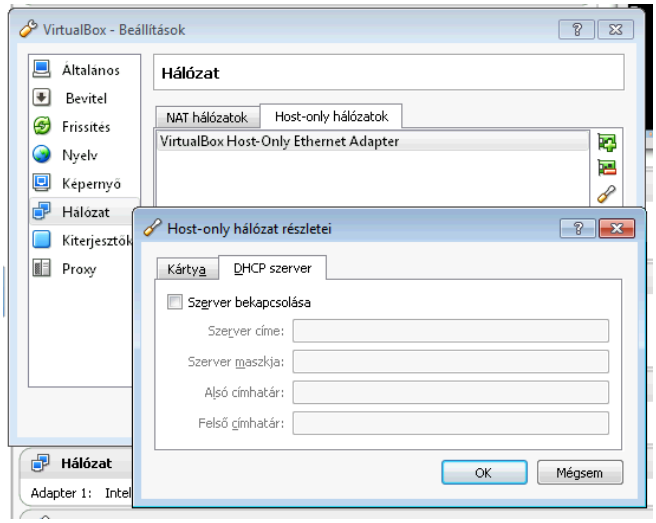
Látható, hogy a virtuális hálózat a 192.168.1.0/24 IP hálózatot fogja használni, azonban a VirtualBox alapértelmezetten a 192.168.56.0/24 IP hálózatot használja (illetve a gazdagép Internetkapcsolat megosztása esetén a 192.168.137.0/24 IP hálózatot), azaz az alapértelmezett beállításokat mindenképpen meg kell változtatni a megfelelő működéshez.



62. ábra: Az új átjáró működéséhez még ez a beállítás is szükséges a gazdagépen a virtuálisgép-kezelőben

Egy másik probléma, hogy a VirtualBox alapértelmezetten DHCP szolgáltatást futtat ezen a hálózaton, amelynek kikapcsolására azért lesz szükség, mert a telepítendő Windows kiszolgálókon is telepítve lesz ez a szolgáltatás. Mivel a Windows kiszolgáló saját DHCP kiszolgálója egyrészt a tananyag része, másrészt jobban is konfigurálható, mint a VirtualBox kiszolgálója, egyértelmű, hogy az utóbbitól meg kell szabadulni, legalábbis ebben a tesztkörnyezetben.

Ezen beállítások megtételéhez a **VirtualBox kezelőben** (VirtualBox Manager) ki kell választani a **fájl** (File) menü **beállítások** (Preferences) menüpontját, majd a megjelenő ablak bal oldalán ki kell választani a hálózat (Network) elemet. A jobb oldalon egy listában megjelennek a Host-Only hálózatokhoz tartozó hálózati interfészek. Ebben az esetben ez egy hálózati interfészt jelent a VirtualBox Host-Only Ethernet Adaptert. A hálózati interfészt kijelölve, majd a csavarhúzó ikonra kattintva megjelennek a hálózathoz tartozó, fentebb felsorolt beállítások.



63. ábra: És ez is szükséges

A **kártya** (Adapter) lapon az **IPv4 cím** (IPv4 Address) mezőbe a táblázatban szereplő **átjáró** (Gateway) címét (192.168.1.254), az **IPv4 hálózati maszk** (IPv4 Network Mask) mezőbe pedig a **hálózati maszkhoz** (Netmask) tartozó címet (255.255.255.0) kell megadni. Ezzel a virtuális hálózat IP beállítása meg is történt. A további beállításokhoz a **DHCP szerver** (DHCP Server) lapon a szerver bekapcsolása jelölő négyzetet ki kell kapcsolni. Ez utóbbira csak akkor van szükség, ha a virtuális tesztkörnyezetben DHCP kiszolgálók „építése” és konfigurálása a cél, mint ahogy ebben az esetben is.

A felsorolt beállításokkal kialakított hálózatnak működőképesnek kell lennie. Nem szabad azonban elfeledkezni a VM-ek megfelelő IP beállításairól, valamint arról, hogy ha DNS és DHCP kiszolgáló VM-ek is készülnek (mint ebben az esetben is), hogy a megfelelő működéshez először a kiszolgálók telepítése és beállítása szükséges, és csak azután következnek a kliensek. Nem kell azonban úgy gondolni ezekre a beállításokra, mint valamiféle egyszer beállított és megváltoztathatatlan dolgokra. A hálózat építése, tesztelése, kiterjesztése során többször is történhetnek kisebb, nagyobb változások a konfigurációkban, ez természetes.

3.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

3.3.1 Összefoglalás

A lecke első felében a Windows alapbeállításai, hardver kezelése került ismertetésre. Kiemelten foglalkozott a tananyag a rendszer tulajdonságai adat-

lap elemeivel, mint a számítógépnév, a hardver, a speciális, a rendszervédelem és a távoli használat lap. Az itt megjelenő olyan beállítások, mint a teljesítmény beállítások közé sorolt processzorhasználat és virtuális memória, vagy a rendszer-visszaállítás, részletesen lettek tárgyalva.

Külön fejezet foglalkozott az eszközkezelő applikációval, melynek segítségével a hardvereszközök kezelése válik könnyebbé. Ismertetésre került az illesztőprogramok telepítésének, frissítésének, valamint eltávolításának módszere. Be lett mutatva a vezérlőpult, amely tulajdonképpen a Windows operációs rendszerek beállító eszközeinek egy gyűjteménye.

A lecke második részében a Windows hálózatok alapelvei kerültek ismertetésre. Meg lettek említve a munkacsoportos és a tartományi hálózat előnyei és hátrányai, valamint egy külön fejezet foglalkozott a Windows operációs rendszerek hálózati beállításaival.

Az utóbb említett fejezetben a hálózati és megosztási központ, mint a hálózat-kezelés és konfiguráció kiindulópontja, került ismertetésre. Tárgyalva lettek az IPv4-es beállítások, mint a statikus és automatikus IP beállítások, előbbi esetén pedig említésre kerültek az IPv4 cím, alhálózati maszk, alapértelmezett átjáró és a DNS kiszolgálók beállítási lehetőségei.

A lecke utolsó részében a tankönyv példáiban alkalmazott a virtuális tesztkörnyezet IP beállításai kerültek ismertetésre.

3.3.2 Önellenőrző kérdések

1. Ismertesse az alapvető rendszerinformációk ablak által nyújtott információkat!
2. Ismertesse a rendszer tulajdonságai adatlap beállítási lehetőségeit!
3. Melyik eszközt célszerű használni hibás szoftverek telepítése után kialakult szoftverhibák elhárítására és hogyan?
4. Mire kell odafigyelni a távoli kapcsolatok engedélyezésénél, beállításánál?
5. Hogyan lehet teljesen eltávolítani egy illesztőprogramot?
6. Mi a különbség a munkacsoportos és a tartományi hálózat között?
7. Ismertesse a Windows IPv4-es beállítási lehetőségeit!
8. A virtuális tesztkörnyezetben milyen hálózati beállításokra kell odafigyelni?

4 CÍMTÁR INFRASTRUKTÚRA

4.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Ebben a leckében a Microsoft Windows Server operációs rendszer által alkalmazott címtár-technológia, az Active Directory kerül ismertetésre. Az inkább elméleti jellegű tananyag tárgyalja a címtár fogalmát és rövid áttekintést nyújt a címtárral kapcsolatos fogalmakról, szabványokról és a címtár alapvető felépítéséről. Ezek után az Active Directory (AD) címtár jellemzői és szolgáltatásai kerülnek ismertetésre. Tárgyalásra kerül, hogy az AD nem csak a címtáradatbázist jelenti, hanem az adatbázist és a címtárszolgáltatás egyben.

Ismertetésre kerül az AD felépítése, a címtárpéldányok szinkronizációja, a címtárpartíciók és a séma szerepe, valamint az ún. egyedi főkiszolgáló műveletek és a globális katalógus szerepkör. Ezek után az AD működési szintjeinek összehasonlítása következik, majd a címtár fizikai tárolásának néhány jellemzője.

A lecke feldolgozása után a hallgatónak megfelelő ismeretei lesznek ahhoz a címtárak fogalmáról, alapvető működéséről és funkciójáról, hogy a jövőben ő is üzemeltethessen címtárat. Képessé válik címtár struktúra tervezésére, valamint címtár sémák alkalmazására.

A tananyag elsajátítása után a hallgató ismerni fogja a különböző főkiszolgálói műveletek és a globális katalógus szerepét. Képes lesz megkülönböztetni az AD működési szintjeit és el tudja majd dönteni, hogy a saját rendszerében melyiket alkalmazza. Ismerni fogja a címtáradatbázis fizikai tárolási egységeit, amely az üzemeltetés, karbantartás esetén nélkülözhetetlen.

4.2 TANANYAG

4.2.1 A címtár

Ahogy a hálózatról szóló fejezetben említésre került; a professzionális tartományi hálózati modell alapja az Active Directory (AD) címtár. Általánosságban a címtár (Directory) egy olyan adatbázis, amely erőforrásokról tárol információkat, illetve biztosítja ezekhez az információkhoz a hozzáférést. Kicsit konkrétabban: a hálózati operációs rendszerek által használt címtárakban tárolt információk általában olyan erőforrásokra vonatkoznak, mint a felhasználók, számítógépek, nyomtatók illetve más megosztott erőforrások. Az ilyen címtárak majdnem mind az 1980-as években az ITU és az ISO által megjelentetett címtá-

rakra vonatkozó szabványkészleten (X.500), illetve (mivel azok az OSI hálózati modellre lettek kifejlesztve) a TCP/IP protokollveremre elkészült a könnyűsúlyú címtár hozzáférési protokollon (Lightweight Directory Access Protocol – LDAP) alapulnak. A továbbiakban címtáron mindig ilyen típusú címtárat értünk.

A címtár egyik fő jellemzője a hierarchikus felépítés, amely leginkább egy - a gráfelméletből ismert - fa struktúrának feleltethető meg. A fa struktúra kitüntetett pontja a „gyökér” (Root) elem (csomópont), amelyhez több „ág” kapcsolódhat, összekötve a gyökeret a leszármazott (vagy gyerek) csomópontokkal. A fában minden csomópontnak egyedi, ún. megkülönböztetett neve van (Distinguished Name – DN), amely a csomóponttól a gyökérig az összes csomópont relatív megkülönböztetett nevének (Relative Distinguished Name – RDN) felsorolásával kaphatunk meg, úgy mintha a kérdéses csomóponttól a gyökérig tartó útvonalat írnánk le. A csomóponthoz attribútumok tartozhatnak, amelyek az adott csomópont tulajdonságait, jellemzőit írják le. Különböző csomópontokhoz különböző attribútumok is tartozhatnak, ilyen formán teljesen különböző típusú csomópontokat is tárolhatunk egy fában. Lehetne úgy is mondani, hogy a csomópontok objektumokat reprezentálnak, és ilyen módon többféle típusú erőforrás objektum is eltárolható. Alapvetően kétféle objektumot különböztetünk meg. Az egyik levél objektum, amely csak saját attribútumait tartalmazza, a másik a konténer vagy tároló objektum, amely a saját attribútumain kívül más objektumokat is tartalmazhat.

Természetes elvárás egy címtártól, hogy a szervezet (vállalat, cég, intézmény stb.) szervezeti felépítését, struktúráját meg lehessen jeleníteni a címtáron keresztül. Ennek elsődleges eszközei az olyan konténer objektumok, mint az ország (Country – C), a szervezet (Organization – O) és a szervezeti egység (Organizational Unit – OU), de gyakran használt objektum a tartomány komponens (Domain Component – DC).

A címtár önmagában még nem sokat ér, azonban a hozzá szervesen kapcsolódó címtárszolgáltatások (Directory Services) révén olyan alapvető feladatokat tud ellátni, mint pl. az erőforrás-objektumok azonosítása (pl. felhasználók azonosítása). Ezenkívül sok címtár segít a hálózatot is átláthatóvá tenni, akár protokoll szinten is, így a felhasználóknak nem kell tudniuk arról, hogy egyes hálózati szolgáltatások, hol találhatóak meg valójában és hogyan kell hozzájuk kapcsolódni.

4.3 AZ ACTIVE DIRECTORY (AD)

Az Microsoft az AD-ra támaszkodva olyan újításokat hozott a Windows operációs rendszert futtató számítógépekből álló helyi hálózatokban, amelyek mind a felhasználást, mind az üzemeltetést jelentősen megkönnyítik a szerverektől egészen a végpontokig. Az AD segítségével például lehetővé vált a fel-

használók szabad, de ellenőrzött vándorlása (roaming) a hálózat számítógépei között, miközben munkakörnyezetük „követi" őket. Ezt úgy kell elképzelni, hogy amikor a felhasználó átül egy kollégájának számítógépéhez (és ez lehet egy másik épületben, vagy akár a világ másik végén is), akkor is ugyanazt a munkakörnyezetet kapja meg. Azaz, miután ugyanazzal a felhasználó névvel és jelszóval jelentkezett be egy másik számítógépre, ott ugyanazt az **asztalt** (Desktop) látja, ugyanott találja meg dokumentumait, leveleit és nyomtatóit, mintha a saját számítógépe előtt ülne. Az üzemeltetés számára óriási jelentőségű, hogy az AD segítségével a hálózat számítógépei távolról telepíthetők és konfigurálhatók, akár csoportosan is. Ilyen lehetőségek közepette a rendszergazdának gyakorlatilag fel sem kell állnia asztalától, mindent egy helyről meg tud csinálni.[20]

A biztonság kérdése mindig is kulcsfontosságú egy hálózat esetében. Az AD segítségével konfigurált biztonsági beállítások és jogosultságok is egyformán jutnak érvényre a hálózatban. A központosított beállítások révén garantálja a rendszergazda a rendszer folyamatos működőképességét és biztonságát.

Az AD szolgáltatásai a következők:

- Nyilvántartja a hálózat és a szervezet erőforrásait, többek között a szervezet felépítését reprezentáló különböző objektumokat; a felhasználói fiókokat, a csoportokat, a fájlokat és a megosztásokat, a jogosultságokat, a szolgáltatásokat, a perifériákat, a számítógépes kapcsolatokat, az adatbázisokat, egyéb erőforrás rekordokat stb.
- A fent említett erőforrásokat jól kereshető formában tárolja, ezenkívül lehetővé teszi az erőforrások tulajdonságainak beállítását, új erőforrás objektumok létrehozását, régiek törlését, illetve a fa struktúrában való mozgatását.
- Az egyben elosztott, de mégis akár egy helyről is kezelhető adatbázis mind a centralizált és mind a decentralizált felügyeletet lehetővé teszi. Az igen összetett csoportházirenddel (Group Policy – GP) pedig a bonyolult hálózatfelügyelet is könnyen kezelhetővé válik.
- Egyszeri azonosítással (Single Sign On – SSO) biztosít hozzáférést a hálózat összes erőforrásához.
- Használata a legtöbb szerver szolgáltatás eléréséhez elengedhetetlen. Pl.: Exchange, RRAS, ISA Server, Certificate Services stb.

Az AD ügyesen integrálódik a Windows operációs rendszerek biztonsági modelljébe úgy, hogy az azonosítási és hozzáférés vezérlési feladatokat átveszi a kliens gépektől, de az olyan szerver alkalmazások esetében is elvégzi a fel-

[20] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

használói azonosítást, mint az IIS, vagy az SQL Server. Az AD-nek alapvetően két feladata van: az azonosítás és a hozzáférés szabályozása.

4.3.1 Az AD címtárszolgáltatás

Az AD címtára, több rendszerhez hasonlóan szintén az X.500 szabványon és az LDAP protokollon alapul, amely lehetővé teszi, hogy a címtár jól skálázható és rugalmas legyen, és le tudjon kezelni egy pár gépes irodai hálózatot, de akár több tízezer számítógépből álló, kontinensek fölött elhelyezkedő multinacionális vállalati hálózatot.

Az AD felépítése

Az Active Directory felépítése – más címtárakhoz hasonlóan – szintén a már korábban említett fastruktúrát követi, sőt több fa struktúrát is össze tud fogni. A legmagasabb szintű tárolónak erdő (Forest) a neve, az erdőt pedig fák (Tree) alkotják. Ez utóbbi tároló (konténer) objektumtípus a hierarchikus felépítésben a következő. Nem úgy, mint a természetben, itt létezik egy fából álló erdő is. Talán ez a leggyakoribb, főleg kisebb hálózatok esetében lehet találkozni vele. Több fából álló erdővel inkább olyan esetben fordulhat elő, amikor a különböző vállalatok, vállalat részek egyesülésénél az eltérő vállalati hálózatokat kell összekapcsolni. Az itt felmerülő problémák megoldására nagyon hasznos, hogy különböző fák egy erdőbe integrálhatóak.

A fa tartományokból (Domain) áll, amely az Active Directory alapvető szervezeti és biztonsági egysége. Az erdő (és így a fa) első tartománya a gyökértartomány. Egy tartomány ugyanis olyan hálózati erőforrások gyűjteménye, amelyek egy címtáradatbázisban találhatóak meg. Ez a közös címtáradatbázis lesz a címtárreplikáció alapegysége is.[21]

Az Active Directory tartományt egy DNS-beli tartománynév azonosítja. Egy ilyen tartományban legalább egy ún. tartományvezérlő (Domain Controller – DC) kiszolgálónak kell lennie. Ajánlott azonban kettő vagy több tartományvezérlő kiszolgálót üzemeltetni a redundancia biztosítása végett, hiszen az azonosítást és hozzáférés-vezérlést végző tartományvezérlő meghibásodása esetén a hálózati szolgáltatások nem állhatnak meg. Ilyen esetben a többi tartományvezérlő átveszi a kiesett tartományvezérlő szerepét. A tartományok egy tartományfában foghatók össze, ha neveik összefüggő DNS-beli nevekkel, azaz egymás szülő és gyerek tartományaiként vannak megadva. Az erdőben a különböző fák így különböző DNS névtereket alkotnak.

[21] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

Egy tartományon belül tovább osztható a fa struktúra a DNS-től függetlenül. Ennek lényege az adott szervezet (vállalat, intézmény) címtárban való reprezentálása, illetve a különböző erőforrások szétválasztva történő tárolása, amely áttekinthetőbb, könnyebben konfigurálható rendszert eredményez. A szervezeti egység (Organizational Unit – OU) objektum konténer ennek az osztásnak az alapvető egysége, mivel a különböző csoportházirendek és jogok delegálása ezeken az egységeken keresztül történik.

Magyarországon ritkán lehet találkozni több tartományból álló hálózattal. Hazánkban inkább az egy tartományos hálózatok a jellemzőek, a tartományon belül pedig a szervezeti egységek tárolókkal fedik le a szervezet felépítését.

A címtárpéldányok szinkronizációja

Az ilyenképpen felépülő AD adatbázisa több, egymással automatikusan szinkronizáló tartományvezérlő kiszolgálón tárolódik, ezt a szinkronizációt hívják replikációnak. Az adatbázis elosztott, de minden adatbázispéldány (címtárpéldány – replika) egyenértékű, a címtár módosításai bármelyik tartományvezérlőn elvégezhetők, köszönhetően a több főkiszolgálós (multimaster) replikációnak. Ilyen típusú replikáció esetén minden tartományvezérlő fogad módosításokat, melyek automatikusan átterjednek a tartomány többi tartományvezérlőjére úgy, hogy egy több ponton történő módosítás esetén is konzisztens marad az adatbázis. Ha ilyen módosítás esetén két különböző objektum kerül módosításra, az nem okozhat nagyobb problémát a különböző replikák „összefésülésénél". Azonban ugyanazon objektum, pl. egy felhasználói fiók (akár ugyanazon) tulajdonságainak egyszerre több tartományvezérlőn történő módosítása már egy kicsit nehezebb eset. Az AD multimaster replikációja szerencsére az ilyen eseteket is kiválóan kezeli, ugyanis a replikáció nem az objektumok szintjén, hanem az objektumok tulajdonságainak (attribútumainak) szintjén történik. Abban az esetben pedig, amikor több helyen történik egy azon objektum egy azon tulajdonságának módosítása, akkor mindig a későbbi módosítást tekinti a rendszer érvényesnek.

Ez a replikációs modell ún. laza konzisztenciát tart fenn a címtáron belül. Ez azt jelenti, hogy a címtárpéldányok ideiglenesen tartalmazhatnak a teljes konzisztens állapotnak nem megfelelő adatokat, de ezek a teljes replikáció során feloldásra kerülnek.[22]

[22] Gál Tamás – Szabó Levente – Szerényi László: Rendszerfelügyelet rendszergazdáknak, Bicske, Szak Kiadó, 2007

A címtárpartíciók

A tartományvezérlőkön található címtárpéldányok mindegyike legalább három, de általában négy vagy több különálló részből, az ún. címtárpartícióból áll. Ezek a partíciók az AD-ben külön részfaként jelennek meg és egységként replikálódnak az erdő olyan tartományvezérlőire, amelyek tartalmaznak példányt az adott részfából. A három címtárpartíció a következő:

- **Séma partíció** (Schema Partition): A címtárban tárolt objektumok és tulajdonságaik meghatározását az ún. osztály és attribútum definíciókat tartalmazza. Az AD erdő szintjén minden tartományvezérlőn (és globális katalóguson is) ugyanaz.
- **Konfigurációs partíció** (Configuration Partition): Az AD topológiájára, a tartományokra, a fákra és az egész erdőre vonatkozó adatok tárhelye. Itt tárolódnak továbbá a replikációval kapcsolatos adatok és meta adatok. Az egész címtár erdőre nézve azonos és az erdő összes tartományvezérlőjén megtalálható.
- **Tartomány partíció** (Domain Partition): A hálózati erőforrások (felhasználók, csoportok, számítógépek, egyéb erőforrás objektumok stb.) tárolásának helye. Tartomány szinten minden tartományvezérlőn azonos.
- **Alkalmazás partíció** (Application Partition): Windows Server 2003-től a Windows Serverek legalább egy ilyen partíciót tartalmazhatnak.[23]

Egyedi főkiszolgáló műveletek (Flexible Single Master Operations – FSMO)

A Windows Server 2003 óta a tartományvezérlői szerepkörök nagyrészt elosztottan működnek, és az összes tartományvezérlőn elérhetők, használhatók. Ez alól kivételt képez öt funkció, melyek elosztott megvalósítása nem lehetséges. Ezek a funkciók csak a tartomány, illetve a teljes erdő egyetlen tartományvezérlőjén helyezkedhetnek el, de nem feltétlenül ugyanazon az egy tartományvezérlőn kell mind azt öt főkiszolgáló műveletnek működnie. Alapértelmezésben a tartományi szintű szerepkörök a tartomány, míg az erdő szintű szerepkörök az erdő legelső tartományvezérlőjére lesznek feltelepítve. Utólag ez természetesen megváltoztatható, a szerepkörök más kiszolgálókra átvihetők. Itt kell megjegyezni, hogy ha egy adott szerepkört megvalósító tartományvezérlőt valamiért el kell távolítani a tartományból, akkor az adott szerepkör áthelyezéséről mindenképpen gondoskodni kell. A szerepkörök a következők:

[23] Gál Tamás – Szabó Levente – Szerényi László: Rendszerfelügyelet rendszergazdáknak, Bicske, Szak Kiadó, 2007

- **RID főkiszolgáló** (Relative Identifier Master – RID Master): A tartományban egy létrehozandó új objektum esetén a funkcióval felvértezett tartományvezérlő más tartományvezérlők, vagy saját maga kérésre kiad egy **relatív azonosítót** (Relative Identifier – RID). A tartományban minden objektumot egy **biztonsági azonosító** (Security Identifier – SID) azonosít, amelynek része a RID. Ahhoz, hogy az objektumok létrehozása zökkenőmentes legyen a RID főkiszolgáló a tartomány minden tartományvezérlőjének 200db-os RID csomagokat oszt ki. Így a tartományvezérlők pl. hálózati leállás esetén is tudnak új objektumokat is létrehozni, persze csak míg ki nem fogynak a RID-ekből. Mivel minden RID-nek csak a tartományon belül kell egyedinek lennie, ezért ez csak tartomány szintű szerepkört kíván, azaz minden tartományban legfeljebb egy lehet belőle.
- **PDC emulátor** (PDC Emulator): A Windows 2000 előtti kliensek úgy illeszthetők be a modernebb tartományi környezetbe, hogy a szerepkörrel bíró tartományvezérlő feléjük a Windows NT-ben használt **elsődleges tartományvezérlőnek** (Primary Domain Controller, PDC) mutatja magát. Ez azt jelenti, hogy többek között kezeli a felhasználók bejelentkezéseit, jelszóváltoztatásait és a változásokat a többi tartományvezérlő felé replikálja. További feladata a többi tartományvezérlő az idő automatikus szinkronizálása a Windows Time szolgáltatás segítségével. Tulajdonságaiból adódik, hogy szintén tartomány szintű szerepkörről van szó.
- **Infrastruktúra főkiszolgáló** (Infrastructure Master): Erre a szerepkörre igazán csak akkor van szükség, ha a hálózat több tartományból áll. Ebben az esetben ugyanis minden tartományban lehetnek olyan objektum-hivatkozások, amelyek más tartományok objektumaira mutatnak. A szerepkörrel bíró tartományvezérlők kezelik és frissítik ezeket a kapcsolatokat és a rájuk vonatkozó kéréseket. Mivel ilyen főkiszolgáló tartományonként csak egy lehet, kiesése esetén a más tartományokhoz tartozó objektumok nem lesznek elérhetőek.
- **Tartománynév-nyilvántartási főkiszolgáló** (Domain Naming Master): Ugyan az erdőben a tartományok és fák közötti kapcsolatok adatai minden tartományvezérlőn megtalálhatók, csak a szerepkörrel bíró tartományvezérlőn módosíthatóak. Feladata továbbá az erdőben az új tartományok hozzáadásának illetve régiek törlésének szabályozása. Erdőszintű szerepkör, az erdőben kizárólag egy ilyen lehet. Ha a szerepkörrel bíró tartományvezérlő elérhetetlen, akkor a tartományfákkal kapcsolatos változások lépnek érvényre.

- **Séma főkiszolgáló** (Schema Master): Mivel a séma az egész erdő szintjén írja le a címtáradatbázis szerkezetét, azaz az objektum-osztályokat és a hozzájuk tartozó attribútumokat, ezért nyilván ennek a szerepkörnek is erdő szintűnek kell lennie. A séma ugyan az egész erdő tartományvezérlőit tekintve mindenhol azonos, a módosítással járó ütközések elkerülése végett azonban célszerű, ha van egy séma főkiszolgáló, amelyen a kérdéses módosításokat el lehet végezni. A változások pedig replikáció útján jutnak el a főkiszolgálótól a többi tartományvezérlőre.[24]

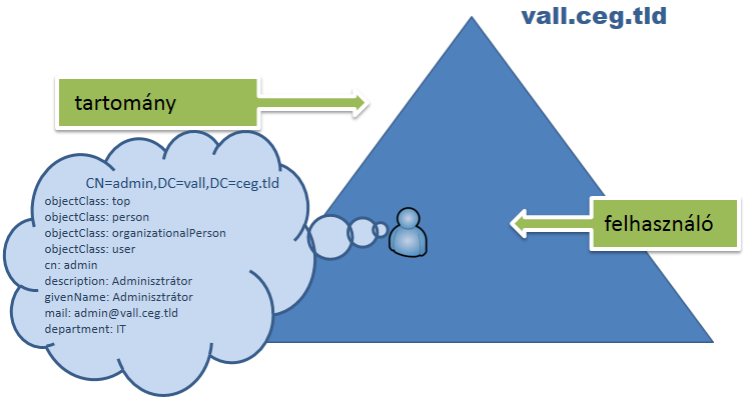
A sémáról

A séma, tulajdonképpen az Active Directory adatbázis szerkezetét írja le oly módon, hogy definiálja az adatbázis által tárolt objektum-osztályokat, illetve azok tulajdonságait, az attribútumokat. Ezzel olyan dolgokat is meghatároz egy objektum-osztály esetén, minthogy mely attribútumok használata kötelező, és melyeké opcionális, vagy mely objektum osztályok szerepelhetnek szülő objektumként.

Az alapértelmezett séma általában teljesen megfelel a hálózat üzemeltetéséhez, és nincs szükség módosításra, hiszen rengeteg objektum-osztályt és számtalan attribútumot tartalmaz. Például egy felhasználó objektumnak rengeteg a működéshez szükséges tulajdonságán kívül (felhasználó név, jelszó, csoporttagság, logon szkript) számos olyan egyéb adatokat is eltárolhatunk, mint a telefonszám, vagy a cím stb.

Ritkán előfordulhat, hogy mégsem elég az alapséma nyújtotta objektumtár, akár azért mert olyan alkalmazásokat kell fejleszteni vagy használni, amelyek más típusú objektumokat használnak, vagy egyszerűen csak azért, mert olyan adatokat is el kell tárolni a címtárban, amelyekhez saját objektumosztályt kell definiálni. Persze lehet módosítani is egy létező objektumtípust, de ez nagy körültekintést igényel, és nem is mindig célszerű. A megváltozott séma ugyanis gyorsan replikálódik az erdő összes tartományvezérlőjére, és ezzel az egész hálózatra hatással van, a módosítás visszavonására pedig nincs lehetőség (esetleg mentésből történő visszaállítással). Vannak olyan alkalmazások, melyek „intenzív” AD használatuk miatt komolyabb sémabővítést is elvégeznek. Ilyen pl. az Exchange Server teleptője, de pl. amikor Windows Server 2003-ról kell migrálni Windows Server 2008 R2-re, akkor is történik sémabővítés.

[24] Gál Tamás – Szabó Levente – Szerényi László: Rendszerfelügyelet rendszergazdáknak, Bicske, Szak Kiadó, 2007



64. ábra: Objektumosztályok és tulajdonságaik

A címtárban található objektumok (címtárobjektumok) tehát a címtárban tárolt objektum-osztály példányok, az attribútumok pedig ezeknek a címtárobjektumoknak a tulajdonságait tárolják. Az attribútumok egyébként nem feltétlenül csak egy objektum-osztályhoz köthetők. Előfordulhat, hogy több objektum-osztály definíció is ugyanazt az attribútumot tartalmazza.

Globális katalógus (Global Catalog – GC)

Fentebb már említésre került a globális katalógus fogalma, amely tulajdonképpen egy tartományvezérlői szerepkör. Ha egy tartományvezérlő globális katalógus is egyben, akkor a saját tartományi objektumain kívül, erdő szinten a címtár összes objektumának alapadatait, elérhetőségeinek információit tárolja. A globális katalógus ez által egy olyan kereshető adatbázist tart fent az erdő objektumairól, amelyben az objektumoknak azon tulajdonságai kerülnek be, amelyek alapján a leggyakrabban keresik őket. Ezt a saját tartományából teljes, más tartományokból részleges objektummásolatok tárolásával teszi lehetővé. Alapértelmezésben az erdő első tartományvezérlője bírja ezt a szerepkört, de több tartományvezérlő esetén más kiszolgálókra is áthelyezhető, sőt érdemes több ilyen tartományvezérlőt is üzemeltetni az erdőben.[25]

4.3.2 Active Directory működési szintek

A Windows szerverek és így az Active Directory fejlődése törvényszerűen újabb és újabb címtárszolgáltatások megjelenését hozza magával. Meglévő,

[25] Gál Tamás – Szabó Levente – Szerényi László: Rendszerfelügyelet rendszergazdáknak, Bicske, Szak Kiadó, 2007

régebbi rendszereket is tartalmazó, folyamatos működést igénylő hálózat esetén nem is olyan egyszerű ezeknek az újabb szolgáltatásoknak az integrálása. Hogy az integráció folyamata lehetőleg zökkenőmentes legyen lehetőség van arra, hogy a különböző tartományokban használt rendszerek, valamint a frissített rendszerek verzióit figyelembe véve lehessen megválasztani a tartományok, illetve az erdő működési szintjét. A működési szintek közötti legfontosabb különbség a támogatott szolgáltatások köre. Ezenkívül oda kell figyelni arra, hogy a működési szint emelésével kizárható a régebbi verziójú tartományvezérlők tartományhoz csatolása. Ez azonban nem jelenti azt, hogy maga a kiszolgáló tagkiszolgálóként ne lehetne továbbra is a tartomány tagja.

Külön működési szintek vannak meghatározva tartományokra és erdőkre is. Jelenleg, amikor is a Windows Server 2008 R2 a legújabb verzió tartományi szinten hat, erdő szinten öt működési szint van definiálva. A tartományi működési szintek a következők: Windows 2000 vegyes (mixed), Windows 2000 natív (native), Windows Server 2003 átmeneti (interim), Windows Server 2003, Windows Server 2008 és Windows Server 2008 R2.

Ha van igény a tartomány működési szintjének emelésére, akkor a szint emelés műveletét a tartományvezérlőkön kell végrehajtani. A legfontosabb, hogy számolni kell azzal, hogy a folyamat általában nem vonható vissza. Ez alól bizonyos korlátokkal kivétel a Windows Server 2008 szintről Windows Server 2008 R2 szintre emelés, ahonnan vissza lehet lépni a sima 2008-as szintre.[26]

Windows 2000 vegyes

Ezt a működési módot azért találták ki, hogy a régi Windows NT tartalék tartományvezérlők (Backup Domain Controller – BDC) addig is működhessenek a tartományban, mint tartalék tartományvezérlők, amíg nincsenek Windows 2000-re frissítve. Ebben a működési módban Windows NT, Windows 2000 és újabbak tartományvezérlők támogatottak. Kivételt képez ez alól a Windows Server 2008 sima és R2 változata. A Windows NT szerverek 2000-re történő frissítése vagy migrálása után célszerű működési szintet emelni, hogy a Windows 2000 natív működési szint plusz szolgáltatásait ki lehessen használni, arról nem is beszélve, hogy ebben az üzemmódban maximum 40000 objektumot tartalmazhat a címtár. Meg kell még említeni, hogy Windows Server 2003-ban ez az alapértelmezett működési szint.

[26] Gál Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

Windows 2000 natív

Ebben a működési módban a Windows NT kivételével az összes Windows Server verzió használható tartományvezérlőként. Ez a működési szint pedig olyan további szolgáltatások nyújt az előzőhöz képest, mint az univerzális csoportok, a csoportok egymásba ágyazhatósága, biztonsági és terjesztési csoportok közötti konverzió, biztonsági azonosító történetkövetés (SID history), távoli hozzáférés házirendek támogatása (RAS policy), valamint megoldja a 40000 objektum korlátból adódó méretezési problémákat.

Windows 2003 átmeneti

Windows NT-ről Windows Server 2003-ra történő migrációkor, az erdő első NT tartományának frissítésekor használatos átmeneti jelleggel. Tartományvezérlők lehetnek Windows Server 2003-tól felfelé.

Windows 2003 natív

Csak Windows Server 2003 és magasabb verziójú tartományvezérlőket lehet használni. Az előző szinthez képest természetesen bővül a szolgáltatások köre. A legfontosabbak közé tartozik a tartományvezérlő átnevezése a **netdom.exe** eszközzel, a Users és a Computers konténerek átirányíthatósága, újdonság két bejelentkezési időbélyeg attribútum kezelésében a felhasználók (Users) és a számítógépek (Computers) objektumoknál; frissíti a LastLogonTime attribútumot, illetve képes replikálni a LastLogonTimeStampet, igaz nem túl nagy pontossággal. Ezenkívül olyan egyéb szolgáltatások jelennek meg, mint a Kerberos Secure Delegation az alkalmazások Kerberos hitelesítéséhez, illetve az engedélyezéskezelő (Authorization Manager) Active Directoryban történő házirend tárolása.[27]

Windows 2008

A használható tartományvezérlők köre a Windows Server 2008 (sima és R2) verziókra korlátozódik. Az ezzel a verzióval megjelenő extra szolgáltatások közül mindenképpen meg kell említeni a csak olvasható tartományvezérlő (Read-only Domain Controller – RODC) támogatást, a SYSVOL megosztás RDC algoritmussal és különbségi replikációs módszerrel támogatott DFS-R replikációját, a Kerberos AES 128/256 támogatását. De ide kell sorolni az utolsó interaktív bejelentkezés információinak (Last Interactive Logon Information) rögzítését (utolsó belépés ideje, honnan történt a belépés, sikertelen belépések száma), valamint a finomított (vagy alternatív) jelszóházirendet (Fine-Grained Password Policies),

[27] GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

melynek segítségével akár szervezeti egységenként különböző jelszóházirendet adhatunk meg a felhasználókra.

Windows 2008 R2

Természetesen ebben az esetben csak Windows Server R2-es tartományvezérlők használhatók, és csak tisztán ezt a működési szintet alapul véve olyan további szolgáltatások jelennek meg, mint a biztosított hitelesítési mechanizmus (Authentication Mechanism Assurance – AMA), amely multifaktoros bejelentkezés esetén több jogosultságot nyújt, illetve a kibővített szolgáltatásfiók kezelés (Managed Service Accounts – MSA), amely automatikusan kezeli a szolgáltatások egyszerű neveit (Service Principal Name – SPN).[28]

Ezenkívül meg kell említeni azokat a szolgáltatásokat is, amelyek nem csak tiszta Windows 2008 R2 működési szinten érhetők el, hanem már akkor is, amikor Windows Server 2008 R2 pl. tagi kiszolgálóként vagy tartományvezérlőként kerül a Windows 2008-as tartományba. Már az előbbi esetében használható a fizikai kapcsolat nélküli tartományba léptetés (Offline Domain Join) és az alap szolgáltatásfiók kezelés (Managed Service Accounts). Utóbbi esetben pedig olyan extrák érhetők el, mint az Active Directory felügyeleti központ (Active Directory Administrative Center – ADAC), az Active Directory PowerShell modulja (Powershell for Active Directory Module), az ajánlott eljárásokat kezelő eszköz (Best Practices Analyzer – BPA) és a címtárszolgáltatások helyreállító módjának jelszó szinkronizálás funkciója (Directory Service Restore Mode – DSRM, Password Sync).[29]

Sokkal körültekintőbben kell eljárni az erdő működési szintjének meghatározásával, ugyanis az erdő a tartományok feletti fogalom. Az öt működési szint a következő: Windows 2000, Windows Server 2003 átmeneti (interim), Windows Server 2003 natív (native), Windows Server 2008 és Windows Server 2008 R2. A megfelelő szint megválasztásánál figyelembe kell venni, hogy az adott verziónál alacsonyabb verziójú tartományvezérlő többé nem léptethető be az erdőbe. Azaz ha nem cél az, hogy tartományvezérlők essenek ki az erdőből, akkor a szint megválasztásánál általában az erdő legalacsonyabb működési szintű tartományának szintjét kell alapul venni. Természetesen a tartományok működési szintjének emelésével az erdők működési szintjét is érdemes emelni. Az erdő működési szintjei részletesen:

[28] GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

[29] Kovács Attila: Active Directory alapfogalmak dióhéjban, Online cikk, KF GAMF Info, 2011, <http://gamfinfo.hu/halozatok/201103/active-directory-alapfogalmak-diohejban>, 2012.09.19>

Windows 2000

Ebben a működési módban Windows NT tartományvezérlő kivételével mindenféle verziójú Windows Server megengedett tartományvezérlőként. A teljes erdőben használhatók lesznek a címtár Windows 2000 natív működési szintű tartományban használható szolgáltatások. Windows Server 2003 és 2008 esetén ez az alapértelmezett működési szint.

Windows 2003 átmeneti

Ez a működési szint – ahogyan a tartományok esetében is – a Windows NT-ről Windows Server 2003-ra való közvetlen áttérés támogatása miatt létezik. Ilyenkor csak Windows NT és Windows 2003 tartományvezérlők csatlakozhatnak az erdőhöz. A Windows NT tartományvezérlők frissítése illetve migrációja után tiszta Windows 2003 natívra emelhető az erdő működési szintje.

Windows 2003 natív

A tartományvezérlők természetesen a Windows Server 2003 és attól magasabb verziójú Windows Serverekből lehetnek ilyen működési szintű erdőben. Mindenképpen érdemes emelni a szintet, ha nincs akadálya, mert szolgáltatások köre szemmel láthatóan bővül. Megjelenik többek között a tartomány átnevezésének lehetősége, az erdők közötti bizalmi kapcsolat kialakításának (Cross Forest Trust) lehetősége, amelyet nagyrészt cégek összeolvadásánál lehet leginkább kihasználni, vagy a csak olvasható tartományvezérlő (RODC) használata, amelyre azonban minden attribútum replikálódik, ezért nem tekinthető teljesen biztonságosnak. Mindenképpen meg kell említeni a finomított replikációt (Link Valued Replication), amely tekintettel a sávszélességre, csak a változott elemet replikálja, továbbá a séma elemek inaktiválási lehetőségét, amelynek segítségével már nem használt vagy sérült osztályokat, attribútumokat lehet használaton kívül helyezni törlés nélkül.

Windows Server 2008

Az azonos tartományi működési szint extra szolgáltatásain kívül csak egyet lehet megemlíteni, amely miatt érdemes is lehet az erdő szintjét emelni, már ha ez lehetséges. Ez a szolgáltatás pedig a csak olvasható tartományvezérlőkre replikálódó attribútumok szűrésének lehetősége (RODC Filtered Attribute Set – RODC FAS), amelyet a kérdéses attribútum searchFlags értékének növelésével lehet elérni. Ez a szűrés azonban csak Windows Server 2008 globális katalógus tartományvezérlő replikációjáról működik megfelelően, 2003-éról nem. Tartományvezérlőként egyébként Windows Server 2008 sima és R2 is használható.

Windows Server 2008 R2

Itt csak a Windows Server 2008 R2 tartományvezérlők használhatóak, a plusz szolgáltatás pedig az Active Directory lomtár (AD Recycle Bin – AD RB) erdőszintű használata, amely nagyon hasznos dolog, hiszen egy (pl. véletlenül) törölt címtárobjektum online, azonnali és teljes körű visszaállítási lehetőségét nyújtja. Mellesleg talán a leggyakoribb hibák az Active Directory esetében az ilyen véletlen törlésekből adódnak.[30]

4.3.3 A címtár fizikai tárolása

Általában nem szükséges az Active Directory adatbázisát fájl szinten manipulálni, de mindenképpen érdemes tudni, hogy mely fájlokban milyen adatok tárolódnak, valamint ezek a fájlok pontosan hol is helyezkednek el a fájlrendszerben.

A fájlok helye a **%systemroot%\NTDS** mappa, ahol a %systemroot% a rendszerpartíción elhelyezkedő Windows mappát jelenti és alapértelmezésben a **C:\Windows**.

A legfontosabb fájl az **Ntds.dit**, amely tulajdonképpen az Active Directory adatbázist tárolja. A fájlnév kiterjesztése is ezt jelzi. (Directory Information Tree – DIT)

Az **Edb.log** fájl az Active Directory adatbázis tranzakciós naplója található, amelyben minden címtárban történt változás azonnal tárolódik, ahonnan később az **Ntds.dit** fájlba kerülnek. A fájl mérete 10MB. Ha ez a fájl megtelik, akkor a további aktív tranzakciók az **Edb00001.log** fájlba kerülnek, amely szintén 10MB-os. Ha az is megtelik, akkor az **Edb00002.log**-ba és így tovább. Az összes tranzakciós naplót tartalmazó fájlnak 10MB a maximális mérete.

Az **Edb.chk** fájl a címtárba még be nem került adatok állapotát tárolja.

Edbres00001.jrs és **Edbres00002.jrs** (korábban **Res1.log** és **Res2.log**) fájlok kétszer 10MB helyet foglalnak le a későbbiekben esetlegesen létrehozandó Edbxxxxx.log fájloknak, más funkciójuk nincs.

Temp.edb fájl a tranzakciós adatok ideiglenes helye.

Itt kell megemlíteni a SYSVOL megosztott mappát, amelyet az Active Directory telepítő programja hozza létre tartományvezérlőkön a **%systemroot%\SYSVOL\sysvol** mappa megosztásával. Ebben a mappában olyan fájlok találhatók, amelyeket a kliens számítógépek indítás, illetve bejelentkezés közben letöltenek (pl. csoportházirend fájlok, bejelentkezési

[30] GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

szkriptek). A mappa tartalmát a fájlreplikációs szolgáltatás (File Replication Service – FRS) komponens automatikusan szinkronizálja a tartományvezérlők között.[31]

4.4 ÖSSZEFOGLALÁS, KÉRDÉSEK

4.4.1 Összefoglalás

Ebben a leckében a címtár és a címtárszolgáltatások alapvető tulajdonságai kerültek ismertetésre. Kiderült, hogy a címtár tulajdonképpen egy objektum orientált adatbázis, amely különösen alkalmas felhasználói és egyéb erőforrások tárolására, hogy aztán pl. azonosításra vagy hozzáférés-vezérlésre lehessen használni.

A Microsoft által nyújtott címtár, az Active Directory (AD), a tartomány modell és a központosított adminisztráció alapja, így muszáj valamilyen módon védeni. Az címtáradatbázis a tartományvezérlő számítógépeken tárolódik és a címtárszolgáltatásokat is ez a számítógép nyújtja. A gyártó ajánlása, hogy megbízhatósági szempontok miatt egy tartományban legalább két tartományvezérlő működjön, amelyek között az adatok a replikációnak nevezett eljárással szinkronban legyenek.

A címtáradatbázis ún. címtárpartíciókból áll, amelyeknek különböző szerepük van. A séma partíció a sémákat, a konfigurációs partíció az AD és a replikáció konfigurációit, a tartományi partíció az erőforrásokat, az alkalmazás partíció különböző alkalmazások beállításait tartalmazza.

Több tartományi fa összefogása az erdő, amelyben bár a legtöbb szolgáltatás elosztott működésű, az egyedi főkiszolgálói műveletek (FSMO) azonban egyszerre csak egy tartományvezérlőn működhetnek. Ilyen funkciók a RID főkiszolgáló, a PDC emulátor, az infrastruktúra főkiszolgáló, a tartománynév-nyilvántartási főkiszolgáló valamint a séma főkiszolgáló. Ezek után ismertetésre került a globális katalógus szerepe is, melyből szintén egy lehet az erdőben.

A lecke második felében ismertetésre kerültek az AD működési szintjei és azok jellemzői, mind tartományi, mind erdő szinten. Tartományi működési szintek a Windows 2000 vegyes (mixed), Windows 2000 natív (native), Windows Server 2003 átmeneti (interim), Windows Server 2003, Windows Server 2008 és Windows Server 2008 R2. Az erdő működési szintjei a következők: Windows

[31] Gál Tamás – Szabó Levente – Szerényi László: Rendszerfelügyelet rendszergazdáknak, Bicske, Szak Kiadó, 2007

2000, Windows Server 2003 átmeneti (interim), Windows Server 2003 natív (native), Windows Server 2008 és Windows Server 2008 R2.

Általánosságban elmondható, hogy a tartomány működési szintjét mindig az szerint kell megválasztani, hogy legalább milyen képességű (verzójú) tartományvezérlők működnek a tartományban. Ugyanez elmondható az erdőre is, de ott a tartományok működési szintjét kell figyelembe venni.

A címtáradatbázis helye a merevlemezen a %systemroot%\NTDS mappa. Itt található meg maga az adatbázis fájl, valamint a tranzakciós napló- és egyéb fájlok.

4.4.2 Önellenőrző kérdések

1. Mi a címtár? Mik a jellemzői?
2. Melyek AD logikai felépítésének jellemzői?
3. Mi a szervezeti egység?
4. Hogyan szolgálja ki az AD a tartományi hálózati modellt?
5. Mit jelent az FSMO? Jellemezze az egyedi főkiszolgáló műveleteket!
6. Melyek címtárpartíciók szerepei?
7. Mire jó a séma?
8. Jellemezze a globális katalógus szerepkört!
9. Ismertesse az AD tartományi működési szintjeit!
10. Ismertesse az AD erdő működési szintjeit!

5 DNS ÉS CÍMTÁR KONFIGURÁCIÓ

5.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Az Active Directory (AD) címtár a tartományi névszolgáltatás (DNS) nélkül nem létezik. Ebben a leckében e két szolgáltatás összefonódásáról lesz szó. Ismertetésre kerül, hogy hogyan épül fel a tartományfa, illetve példán keresztül is bemutatásra kerül egy-két tartományfából álló erdő felépítése.

A tananyag második részében ismertetésre kerül a tartományvezérlői szerepkör, valamint az AD telepítése. A két tartományvezérlő multimaster replikációval szinkronizálja egymást.

A tananyag feldolgozása után a hallgató képes lesz akár több tartományfából álló erdők tervezésére, a tartományfák és erdő létrehozására tartományvezérlői szerepkör telepítéssel.

5.2 TANANYAG

5.2.1 Az Active Directory és a DNS szolgáltatás

Az előző leckében már említésre került, hogy a címtár a hálózatban lévő objektumokat hierarchikus struktúrába szervezi, amelynek alapja az objektumok elnevezésében jelenik meg. Ez az elnevezés egyrészt a felhasználók számára teszik az objektumokat azonosíthatóvá, másrészt pedig jelzi az objektumok helyét a struktúrában.

A hálózati szolgáltatások jórészt ezzel a névvel azonosítják a címtár objektumait. Abban az esetben, ha például egy felhasználó el akarja érni ezeket a szolgáltatásokat, ahhoz a szolgáltatást igénybe venni akaró számítógépnek a szolgáltatást nyújtó számítógéppel kell kommunikálnia. Mint ismeretes, a Windows alapértelmezett hálózati protokollja a TCP/IP protokollcsalád, amelynél a hálózat csomópontjai közötti kommunikáció az IP protokoll címzésén (IP címek) alapul. Azaz a szolgáltatást nyújtó számítógép nevét valamilyen úton-módon le kell „fordítani” IP címre. Erre a legmegfelelőbb eszköz, a TCP/IP protokollcsaládon alapuló, internetes **tartományi névrendszer** (Domain Naming System – DNS) szolgáltatás, amelyben **névkiszolgálók** (Name Server) segítségével történik az említett név-cím konverzió, a folyamatot pedig **névfeloldásnak** (Name Resolution) nevezik. A rendszer működése egy elosztott adatbázison alapul, amely a névkiszolgálókon található, és a nevek és IP címek összerendeléseit

tartalmazza. Amikor a kliens azzal a kéréssel fordul a névkiszolgálóhoz, hogy az adja meg neki az adott névhez tartozó IP címet, akkor a kiszolgáló az adatbázisból kikeresi a kérdéses címet és válaszában visszaküldi a kliensnek.[32]

Az Active Directoy működéséhez elengedhetetlen, hogy a hálózatban működjön DNS kiszolgáló, amely mind a kiszolgáló és kliens számítógépek számára elérhető. A DNS kiszolgálóra egyetlen kritérium létezik, az hogy támogassa a **szolgáltatás meghatározó** (Service Locator Record – SRV Record) **rekordtípust**. (A rekordokat gyakran erőforrásrekordoknak, vagy bejegyzéseknek is nevezik.) A gyártó azonban azt ajánlja, hogy ha lehet, akkor a használt DNS kiszolgáló a következő tulajdonságokkal mindegyikével rendelkezzen:

- Szolgáltatás meghatározó rekordok támogatása (SRV rekordok): A DNS adatbázisában nem csak DNS beli név – IP cím megfeleltetésre használt bejegyzések, rekord típusok találhatóak. A DNS ezenkívül sok más típust is használhat. Ilyen típus a szolgáltatás meghatározó SRV rekord is, amely olyan adatokat tárol el, mint a szolgáltatás szimbolikus neve (pl.: _kerberos vagy _ldap), a használt protokoll (_tcp vagy _udp), illetve a tartománynév, ahova a szolgáltatás tartozik. Ezenkívül tárolja még a prioritást, amely a használandó kiszolgálók sorrendjét határozza meg, egy súlyozási értéket, amelyet a terheléselosztásnál lehet használni, a portot, amelyen a szolgáltatás elérhető, valamint a kiszolgáló DNS nevét, ahol a szolgáltatás elérhető. Az AD működése során a kliens számítógépek lekérdezikaz adott tartományban, adott szolgáltatáshoz tartozó adatokat, amelyek segítségével tudni fogja, melyik kiszolgálóhoz forduljon pl. egy felhasználó beléptetéshez.

Service.Protocol.Name	TTL	Class	Type	Priority	Weight	Port	Target
_ldap._tcp.vall.ceg.tld	600	IN	SRV	0	100	389	dc1.vall.ceg.tld

6. *Egy tipikus SRV rekord*

- Dinamikus DNS frissítés támogatása: Korábban a DNS kiszolgálókon csak kézzel lehetett újabb rekordokat felvenni, illetve a meglévőket módosítani, az adatbázis pedig gyakorlatilag egy szövegfájlban tárolódott. Azaz a rekord felvétel, illetve módosítás nem jelentett mást, mint szöveg fájlok szerkesztését. Az újabb kiszolgálók már támogatják a dinamikus DNS frissítéseket. Az újabb kiszolgálók esetében a dinamikus IP konfigurációt (DHCP) használó kliensek IP címe és neve automatikusan frissül a DNS kiszolgálón, ha azokban változás történik.

[32] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

- Az AD telepítése közben a telepítő szintén a dinamikus frissítést képességét használja ki ahhoz, hogy tartományvezérlőnként előforduló számos SRV rekordot automatikusan bejegyezze a DNS adatbázisába. Ennek hiányában kézzel kéne ezeket a bejegyzéseket létrehozni, amely elég időigényes és sok hibalehetőséget is rejt magában.

A gyártó természetesen a Windows Server 2008 saját DNS kiszolgáló szoftverét ajánlja, amely teljesíti a kívánt feltételeket. Ettől függetlenül előfordulhat, hogy a hálózatban már létezik más típusú DNS kiszolgáló. Ekkor arra kell odafigyelni, hogy az támogassa a fent említett szolgáltatásokat. Windows alapú kiszolgáló esetén ez legalább a Windows 2000 Server DNS kiszolgálóját jelenti, míg UNIX alapú rendszereknél a BIND legalább 8.1.2-es verzióját

5.2.2 A DNS névkiszolgálók

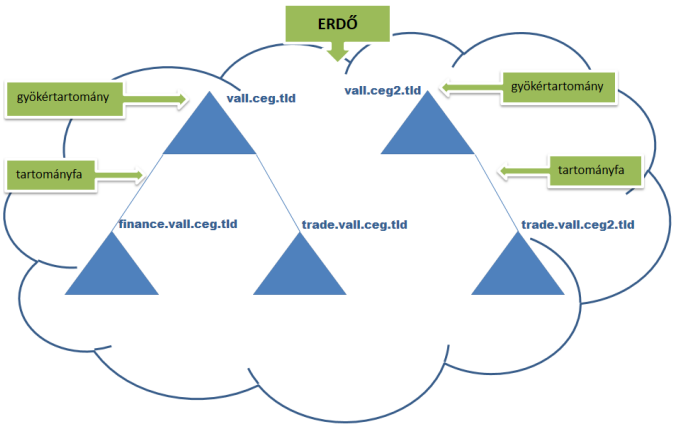
Az előbbiekben már említésre került, hogy az Active Directory működéséhez elengedhetetlen egy DNS névkiszolgáló a hálózatban, mivel a címtár tartomány-hierarchiáját a DNS névtér-struktúrájában tárolja, amely teljesen megfeleltethető neki. A DNS névkiszolgálónak tehát az internetes névfeloldáson túl feladata lesz az is, hogy tárolnia kell a hálózatban az adott tartományra vonatkozó adatokat is.

A DNS névkiszolgálók a tartományokat ún. zónákban (Zone) tárolják, amelyek legalább egy, de akár több tartomány adatait is tartalmazhatják. (Ezek közé tartozhat egy tartomány akár összes altartománya is.) Az adott kiszolgáló hatáskörébe ezek a tartományok tartoznak. Más szóval ezekért a tartományokért az adott névkiszolgáló felel.

Egy zónában kezelhetők például az alábbi DNS-tartományok: vall.ceg.tld, marketing.vall.ceg.tld, ertekesites.vall.ceg.tld. (ábra)

Összefoglalva a zóna egy összefüggő névhierarchiát, vagy annak egy összefüggő részét tartalmazza. Így akár egyetlen zónában is tárolható egy AD tartományfa teljes névtere.

Abban az esetben, ha az AD tartománystruktúra egy erdő, azaz több gyökértartományt tartalmaz, akkor minden gyökértartományhoz külön zóna szükséges.



65. ábra: Két tartományfából álló erdő, minden gyökértartományhoz, külön zóna szükséges

A DNS névkiszolgálókon minden zónának egy adatbázis felel meg, amelyet a kiszolgáló az ún. zónaállományban tárol. Ezekből több is lehet egy kiszolgálón. Az adatbázisban a zónához tartozó számítógépek bejegyzései találhatók. Azaz pl. az **IPv4 cím típusú rekord** (IPv4 Address – A), amely az IPv4-es címet és a hozzátartozó nevet tárolja.

Minden zónának lehetnek **elsődleges** (Primary zone) és **másodlagos** (Secondary zone) példányai. Az elsődleges zóna az adatbázis eredeti példánya. Az elsődleges zónát kezelő névkiszolgáló a zóna elsődleges, míg a másodlagos zónát kezelő a zóna másodlagos DNS névkiszolgálója. A zóna módosításai minden esetben az elsődleges névkiszolgálón történnek, míg a másodlagos kiszolgáló a zónafájl átmásolásával rendszeresen frissíti saját példányát.

Ugyan minden tartomány tartozhat külön zónába és minden zóna tárolható külön DNS névkiszolgálón, azaz minden tartománynak lehet saját névkiszolgálója, ez azonban a teljesítmény és a kihasználtság szempontjából vizsgálva nem feltétlenül a legjobb megoldás. Abban az esetben, ha pl. az AD tartományfa minden tartománya azonos telephelyen található és nagysebességű helyi hálózaton van összekapcsolva, akkor teljesen felesleges minden tartományhoz külön kiszolgáló.

Általános esetben az mondható el, hogy érdemes a lehető legkevesebb zónát használ. Ez azt jelenti, hogy minden tartományfát lehetőleg egy zónában kell tárolni. Ebből következik, hogy ha az erdő egy tartományfát tartalmaz, akkor akár az egész AD címtárat kiszolgálhatja egy DNS névkiszolgáló. Ez azonban megbízhatósági szempontokat figyelembe véve nem a legjobb választás, hiszen

az egyetlen névkiszolgáló bármilyen okból történő elérhetetlensége az egész címtár működésképtelenségét vonja maga után. Célszerű lehet a DNS azon tulajdonságát kihasználni, hogy az elsődleges névkiszolgáló mellett egy automatikusan frissülő másodlagos névkiszolgáló is működhet, azonban a Microsoft DNS névkiszolgálóját használva még ennél is jobb megoldás létezik. Az ajánlott konfiguráció ebben az esetben az, hogy mivel a gyártó tanácsai szerint úgyis legalább két tartományvezérlőre van szükség tartományonként, ezért az ezekre a tartományvezérlőkre az AD-ba integrálva telepített DNS névkiszolgálók elsődleges névkiszolgálóként fognak működni, elsődleges zónáik szinkronban tartásáról pedig az AD replikációs folyamata gondoskodik. Összefoglalva: egy tartományfa esetén két darab, AD-ba integrált, elsődleges DNS névkiszolgáló biztosítja a DNS megfelelő működését a fenti esetben említett hálózatban.

Amennyiben az AD tartományfa egy több olyan helyi hálózatból álló hálózatot fed le, melyeket alacsony sávszélességű vonalak kapcsolnak össze, akkor érdemes lehet ezekre a telephelyekre másodlagos DNS névkiszolgáló kihelyezése, amely nagyban meggyorsítaná a DNS kérésekre történő válaszadást. A másodlagos DNS automatikus frissítése pedig jóval kevesebb sávszélességet fog le, mint a kliensek lekérdezései. Ha az adott helyi hálózat ráadásul egy nagyobb vállalat nagyobb telephelye, akkor a korábban ismertetett módszerrel telepített, külön DNS kiszolgálóval felvértezett tartományvezérlő is kihelyezhető.

Sok esetben az vállalat már rendelkezik DNS névkiszolgálókkal, és ha ezek megfelelnek a korábban említett követelményeknek, akkor használhatók is. Az AD használata miatt azonban célszerű a Microsoft DNS névkiszolgálók használata. A létező névkiszolgálók általában az internetről is láthatóak, hiszen a publikus internetes (pl. WWW, FTP) kiszolgálók máskülönben nem lennének elérhetőek az internet felől. Felvetődik a kérdés, hogy akár Microsoft DNS névkiszolgáló, akár más névkiszolgáló van használatban, az AD struktúra is olyan kiszolgálón legyen tárolva, amely kívülről is elérhető? Az is kérdés, hogy az AD struktúra gyökértartományának a neve, megegyezzen-e a vállalat internetes tartománynevével?

Ezen a szempontokat figyelembe véve a következő lehetőségekre kell odafigyelni:

A külső (az internet felől is látható) és belső (csak a belső hálózatról látható) névkiszolgálóknak különbözőknek kell lennie. Ha volt már létező DNS névkiszolgáló, amelynek feladata az internetes névfeloldás volt, akkor az maradjon is meg ebben a funkciójában. Ha nem volt ilyen, de szükség van rá, akkor telepíteni kell. Az belső hálózatban található számítógépek kéréseit a belső névkiszolgálók szolgálják ki, még akkor is, ha azok külső címekre irányulnak. Utóbbi eset

akkor működhet megfelelően, ha a belső kiszolgálók a külső címekre irányuló kéréseket **továbbítják** (Forward) a külső kiszolgálónak.

A belső tartományok zónáinak különböznie kell az internetes DNS tartományok zónáitól. Feltehető, hogy az intézménynek van internet kapcsolata és internetes gyökértartomány neve is, amelyet használ internetes szolgáltatásainál. Ebben az esetben célszerű egy másik DNS gyökértartomány nevet is beregisztrálnia, amely különbözik a használttól (pl.: cegnev.tld az eredetileg használt, a belső használatra szánt pedig a rovidcegnev.tld), vagy megoldás lehet az eredeti gyökértartomány egy altartományát külön zónába tenni, és azt rendszeresíteni belső használatra. Utóbbi esetben hiába összefüggő a névtér a külsőleg használt tartománnyal, mivel külön zónában (és az előző szempont szerint külön kiszolgálón) van, nem keveredhet össze a két zóna. Nagyon fontos, hogy valóban ne legyenek átfedések a két zóna között.

Elképzelhető olyan helyzet is, hogy a hálózat nincs összekapcsolva az internettel, de nem túl gyakori, és ha elő is fordul igen ritka, hogy azt a jövőben sem tervezik. Ilyen esetekben lehet használni olyan gyökértartományokat, mint a régebbi ajánlásokban szereplő **.intra** vagy a **.local** (ceg.intra vagy ceg.local). Ilyen gyökértartományokkal gyakran lehet találkozni, mert évekkel (és Windows Server verziókkal) ezelőtt ez volt az ajánlás a tartománynévtér kialakítására.

A belső DNS névkiszolgálót célszerű tartományvezérlőre telepíteni, méghozzá a korábban ismertetetteknek megfelelően címtárba integráltan. Az ezzel kapott plusz szolgáltatás segítségével, az AD replikáción keresztül történik a zóna példányok szinkronbantartása. Itt kell megjegyezni azonban azt is, hogy az integrált DNS zónák nem terjednek át az erdő más tartományainak tartományvezérlőire, ezért a zóna másodpéldánya miatt mindenképpen szükséges lesz a tartományban egy újabb tartományvezérlő és DNS kiszolgáló elhelyezése, amelynek használata amúgy is erősen ajánlott.

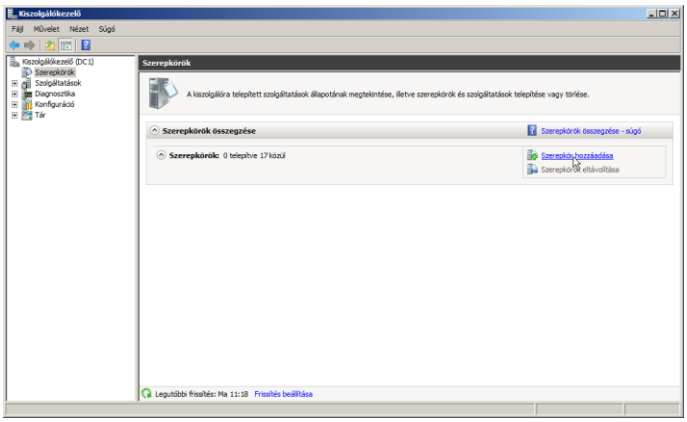
5.2.3 Az Active Directory telepítése

Amennyiben az AD és így a tartománystruktúra telepítése előtt nincs a hálózatban DNS névkiszolgáló, úgy a címtár elsőként telepített tartományvezérlőjére automatikusan települ egy DNS névkiszolgáló és az AD működéséhez elengedhetetlen (ebben az esetben az AD-ba integrált) zóna is létre lesz hozva. A többi tartományvezérlő telepítése előtt gondoskodni kell arról, hogy a már telepített DNS névkiszolgáló elérhető legyen. Abban az esetben, ha az újabb tartományvezérlő DNS névkiszolgáló is egyben, nem szabad elfeledkezni a DNS szerepkör telepítéséről. Ez szerencsére nehezen maradhat ki, mivel majd látszik, hogy az AD telepítése közben a telepítővarázsló felkínálja a DNS kiszolgáló telepítését.

A későbbiekben tárgyalásra kerülő témák bemutathatósága miatt, most különösebb részletezés nélkül tárgyalásra kerül a Windows Server 2008 R2 tartományvezérlői és az azokkal összefüggő szerepkörök telepítése.

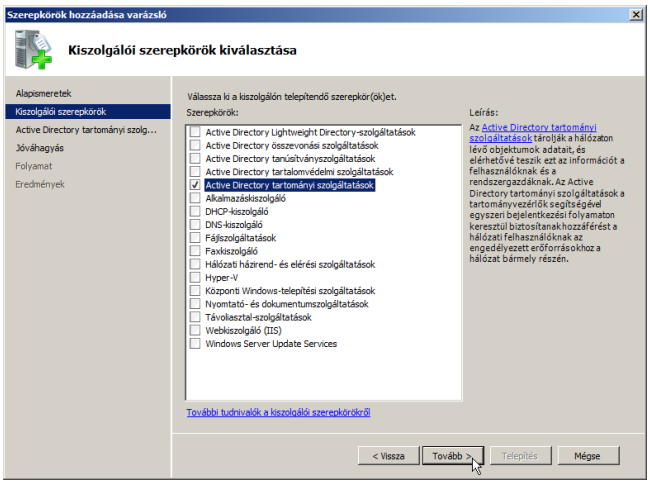
5.2.4 Tartományvezérlő szerepkör telepítése

A telepítés két lépésből áll. Először magát a szerepkört kell hozzáadni, majd futtatni kell a tartományi szolgáltatások telepítővarázslóját. Az első lépéshez vagy a **kezdeti konfigurációs feladatok** (Initial Configuration Tasks) ablakban, vagy a **kiszolgálókezelőben** (Server Manager) a **szerepkör hozzáadása** (Add Roles) elemre kell kattintani.



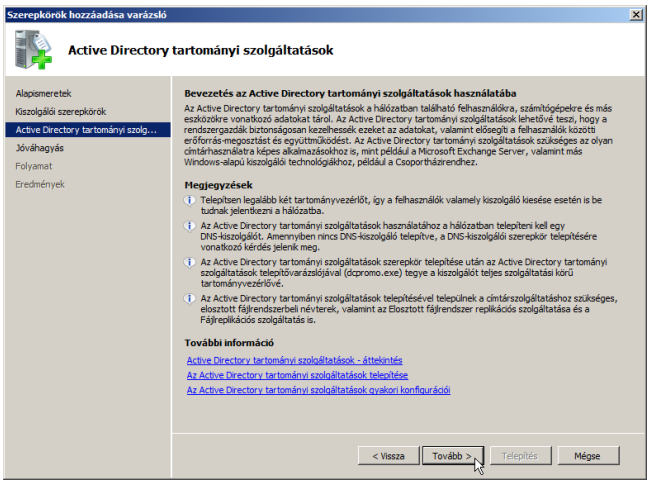
66. ábra: Szerepkör hozzáadása

A megjelenő **szerepkörök hozzáadása varázsló** (Add Roles Wizard) első lapján a varázsló tájékoztatást nyújt, hogy szerepkörök telepítése előtt mire érdemes figyelni. A tájékoztató szöveg figyelmes elolvasása után a **tovább** (Next) gombra kattintva megjelennek a telepíthető szerepkörök. A szerepkörök neve előtti kijelölőnégyzetre kattintva kiválasztható a kívánt szerepkör. (A már telepített szerepkörök itt elszürkülve jelennek meg.) A tartományvezérlő szerepkör hozzáadásához az **Active Directory tartományi szolgáltatások** (Active Directory Domain Services) szerepkört kell kiválasztani, majd a **tovább** (Next) gombra kell kattintani. Az ezek után megjelenő ablak szintén egy tájékoztató szöveget tartalmaz, de itt már specifikusan a kiválasztott szerepkörről lehet olvasni általános információkat, valamint jó tanácsokat is. A **tovább** gombra kattintva egy összegzés jelenik meg a telepítendő szerepkörről, amelyet a **telepítés** (Install) gombra kattintva lehet jóváhagyni. Ez után elindul a telepítési folyamat, melynek végén a **bezárás** (Close) gombra kell kattintani.



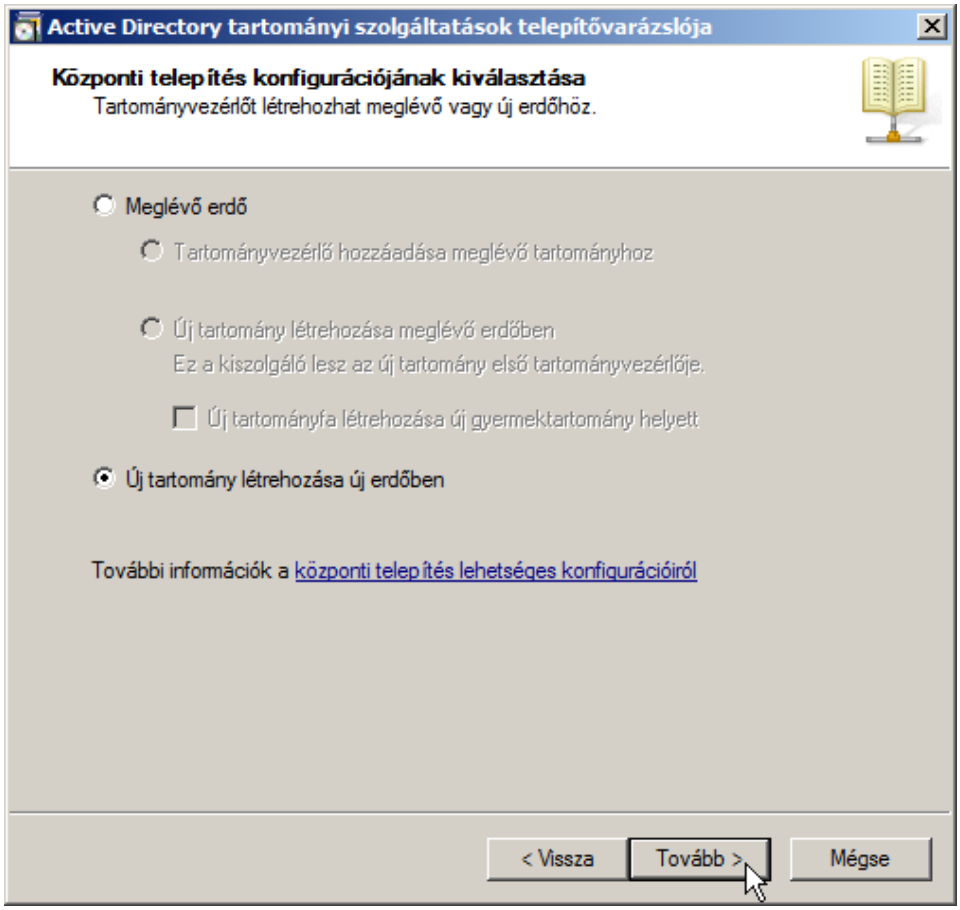
67. ábra: Active Directory tartományi szolgáltatások kiválasztása

A szerepkör telepítésének második lépéseként a **kiszolgálókezelőben** (Server Manager), a **szerepkörök** (Roles) alatt található **Active Directory tartományi szolgáltatások** (Active Directory Domain Services) **összegzés** (Summary) mezőjében található **futtassa az Active Directory tartományi szolgáltatások telepítővarázslóját** (Run the Active Directory Domain Services Installation Wizard (dcpromo.exe)) mezőre kattintva futtatni kell a telepítő varázslót. A varázsló úgy is futtatható, hogy parancssort (cmd) indítva a **dcpromo** parancsot kell kiadni (C:\%systemroot%\System32\dcpromo.exe).



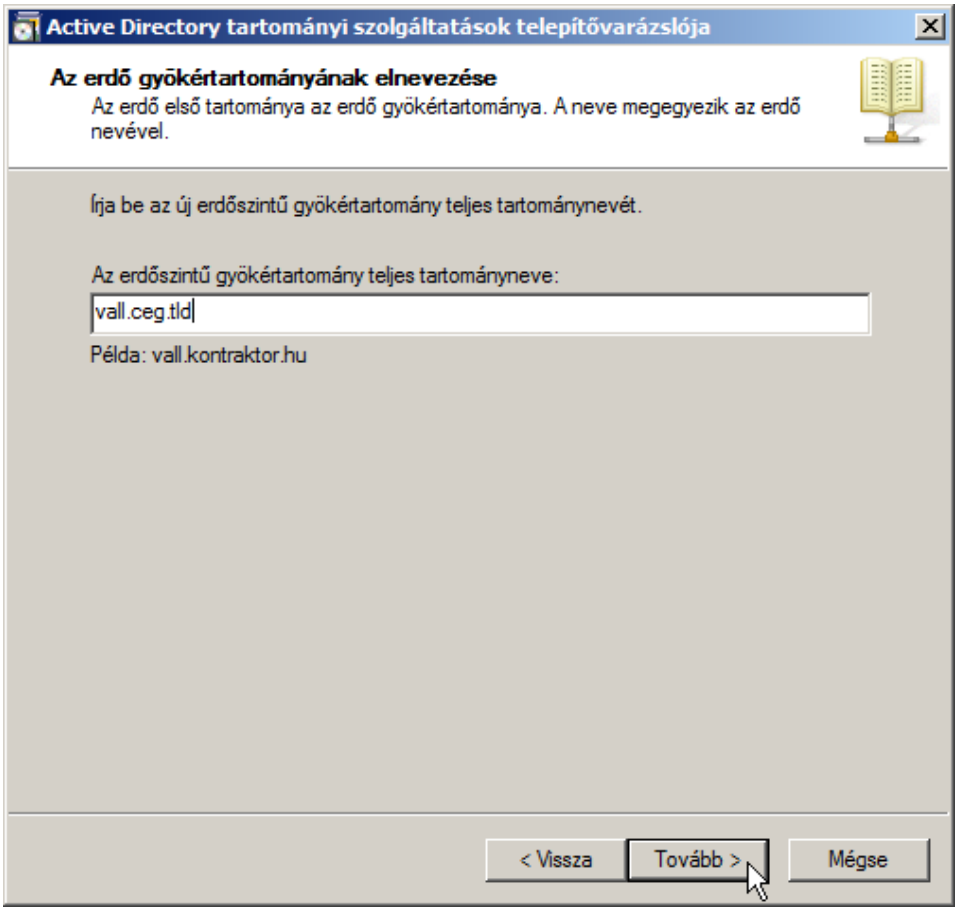
68. ábra: Érdemes a tanácsokat is elolvasni

Az elinduló varázsló ablakbának először a **tovább** (Next) gombra kell kattintani, amelynek hatására a következő ablakban egy tájékoztató szöveg olvasható, amely már létező, Windows Server 2008-tól régebbi verziójú AD kiszolgálókra és Windows Vista SP1 kliensekre vonatkozik. Ez a jelenlegi tesztkörnyezetet nem érinti, hiszen itt csak Windows Server 2008 R2 és Windows 7 operációs rendszerek vannak és lesznek telepítve. A **tovább** gombra kattintva, a következő ablakban azt kell kiválasztani, hogy a telepítendő tartományvezérlőt új, vagy meglévő erdő, új vagy meglévő tartományához kell létrehozni. Mivel ez az első tartományvezérlő ezért az **új tartomány létrehozása új erdőben** (Create a new domain in a new forest) lehetőséget kell választani.



69. ábra: Új tartomány létrehozása új erdőben

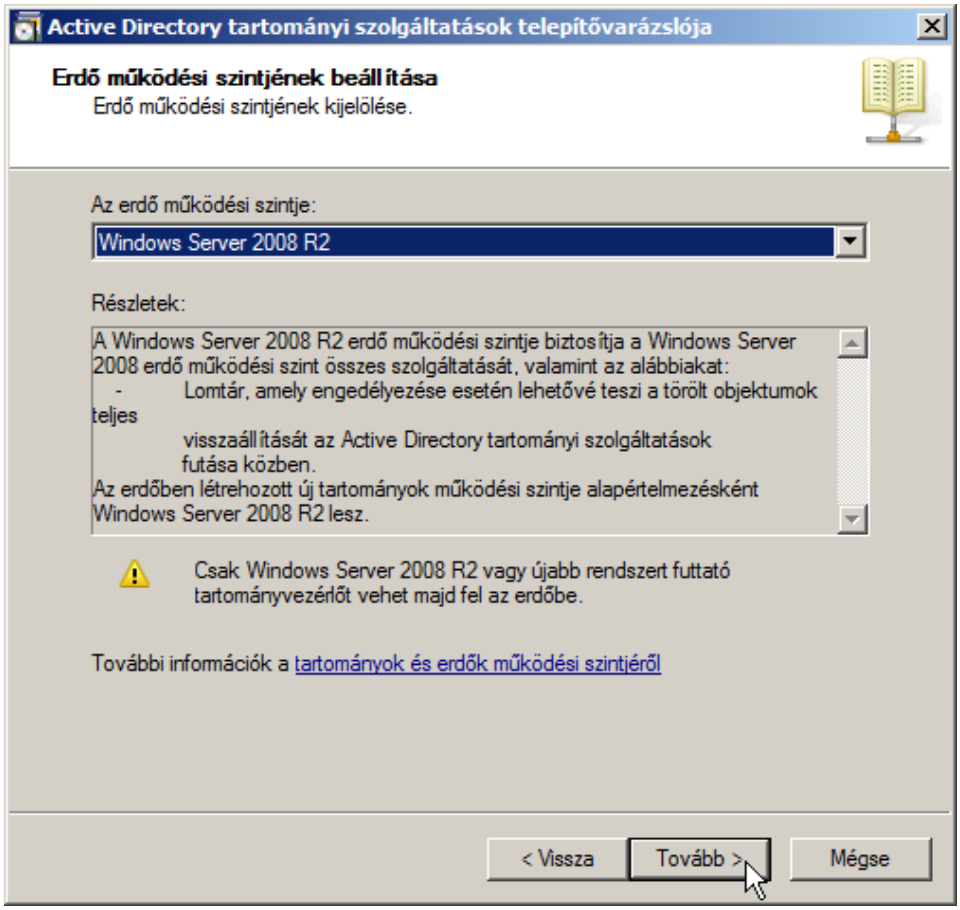
A **tovább** (Next) gombra kattintva meg kell adni **az erdőszintű gyökértartomány teljes tartománynevét** (FQDN of the forest root domain), amely itt a vall.ceg.tld lesz. A **tovább** gombra kattintva a varázsló ellenőrzi a NetBIOS típusú nevet, amelyet a teljes tartománynévből állít elő automatikusan a varázsló. Ebben az esetben ez a **tartomány NetBIOS neve** (Domain NetBIOS name) mezőben elhelyezkedő VALL lesz, amelyet a **tovább** gombra kattintva lehet nyugtázni.



70. ábra: A gyökértartomány teljes nevének beállítása

A következő ablakban az **erdő müködési szintjét** (Forest functional level) lehet beállítani. A különböző működési szintek már bemutatásra kerültek az előző fejezetben, és ott kiderült, hogy akkor van igazából jelentőségük, ha különböző operációs rendszer verziójú tartományvezérlők működtetik a tartományokat és az erdőt. Ebben a tesztkörnyezetben jelenleg csak Windows Server

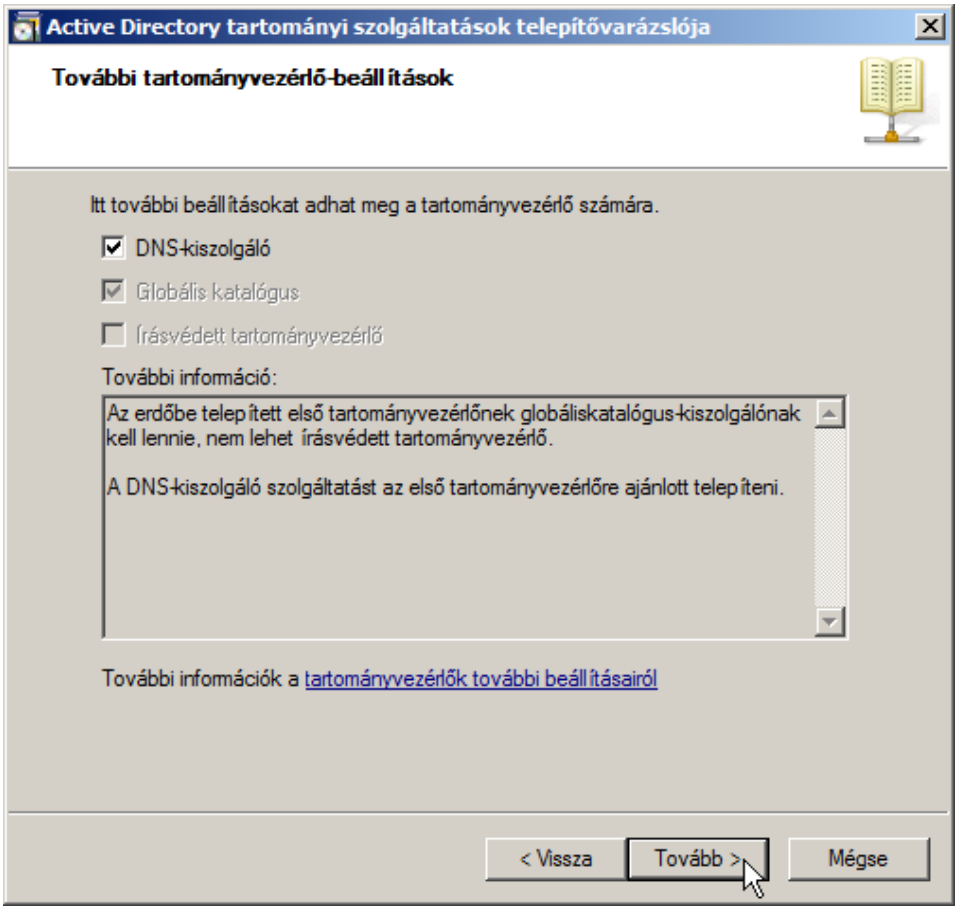
2008 R2 verzójú tartományvezérlők fognak működni ezért a működési szintet is Windows Server 2008 R2-re célszerű állítani. Így az összes létező előnyét ki lehet használni a Windows Server 2008 R2 kiszolgáló nyújtotta tartományi szolgáltatásoknak.



71. ábra: Az erdő működési szintjének beállítása

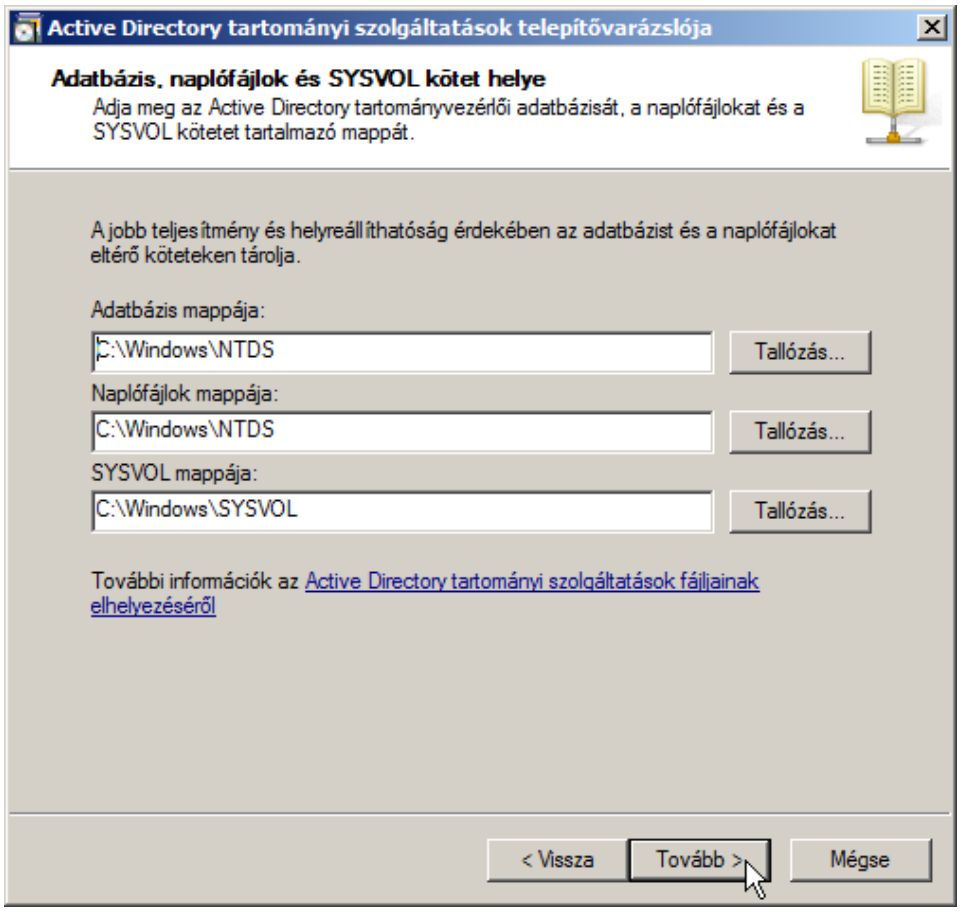
A **tovább** (Next) gombra kattintva a további tartományvezérlő-beállítások ablak jelenik meg, ahol **DNS-kiszolgáló** (DNS server), **globális katalógus** (Global Catalog) és **írásvédett tartományvezérlő** (Read-only domain controller (RODC)) telepítéséről lehet dönteni. A DNS kiszolgáló kiválasztása a korábban ismertetett tulajdonságok miatt célszerű (a tesztkörnyezethez pedig elengedhetetlen), továbbá a varázsló is erősen ajánlja a tartomány első tartományvezérlőjéről lévén szó. A másik két lehetőség választása ugyanezen ok, valamint az erdő első tartománya és tartományvezérlője miatt korlátozott. **Globális katalógust** min-

denképpen, **írásvédett tartományvezérlőt** pedig semmiképpen sem lehet telepíteni ilyen feltételek mellett. A választásokat a **tovább** gombra kattintva kell nyugtázni.



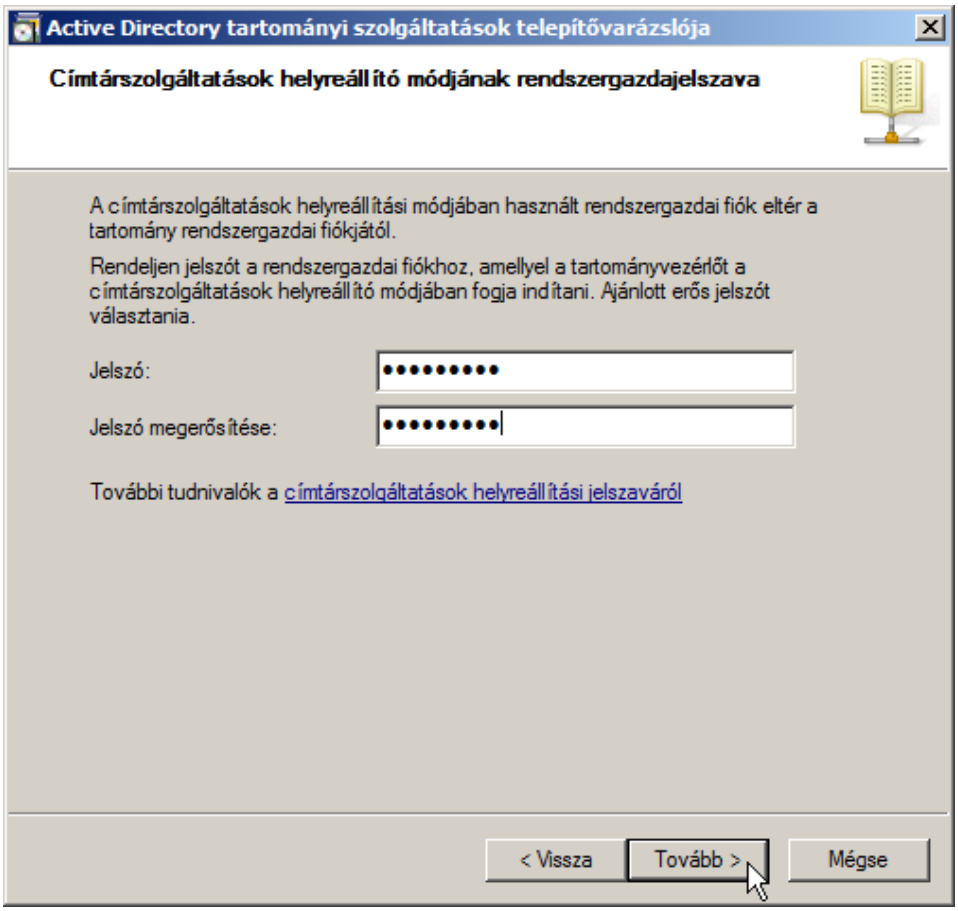
72. ábra: DNS kiszolgálóra is szükség lesz

A következő ablakban az **AD adatbázisfájljainak** (Location for Database), **naplófájljainak** (Log Files), valamint a **SYSVOL** kötet helyét, **mappáit** (folder) lehet megadni. A változtatáshoz a megfelelő mezőkbe meg kell adni a mappák elérési útját, vagy a **tallózás** (Browse) gombra kattintva lehet azokat kiválasztani. Célszerű itt, hacsak nincsen valami különös indoka a dolognak, az alapértelmezett értékeket elfogadni.



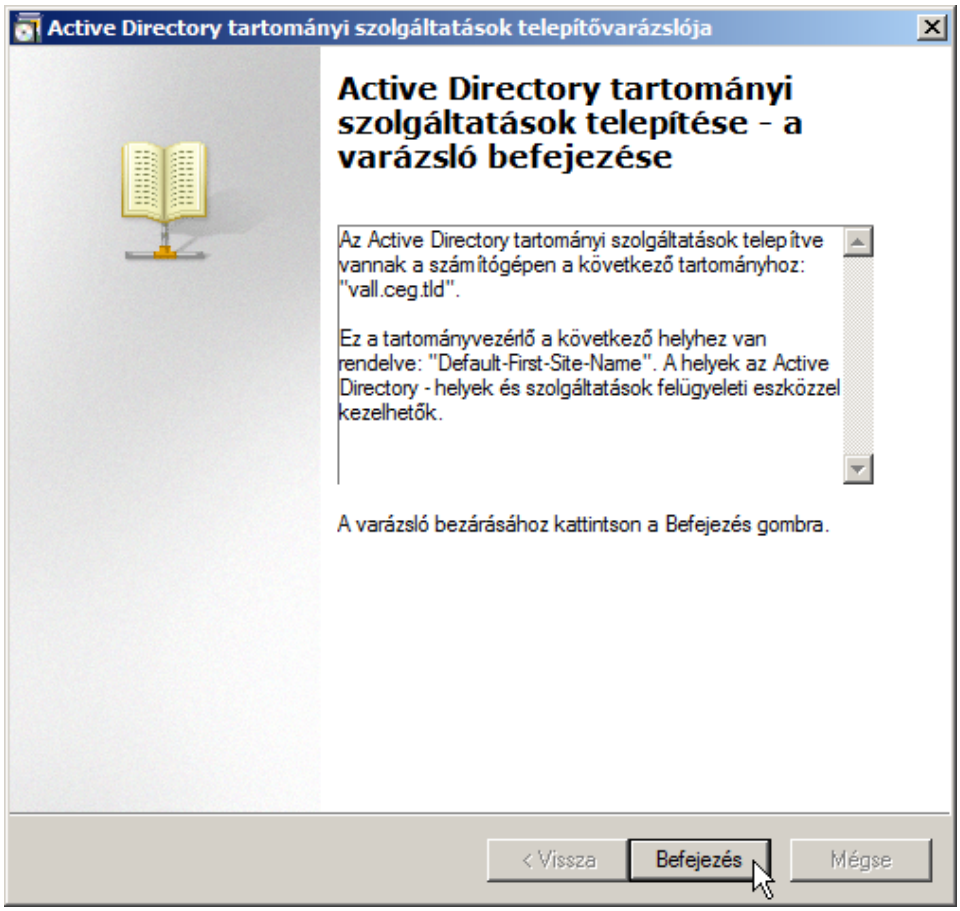
73. ábra: Célszerű az alapértelmezett értékeket elfogadni

A **tovább** (Next) gombra kattintva a **címtárszolgáltatások helyreállító módjának rendszergazdajelszavát** (Directory Services Restore Mode Administrator Password) kell kétszer megadni. A tájékoztató alapján érdemes erős jelszót választani és megőrizni azt egy biztonságos, mások által hozzá nem férhető helyen. Ezek után a **tovább** gombra kell kattintani, melynek hatására megjelenik egy összegző ablak, ahol az eddig megadott beállítások jelennek meg. Ezek ún. **válaszfájlba** (answer file) **exportálhatók** (Export settings), ha ugyanezen beállításokkal felügyelet nélküli telepítés segítségével kell tartományvezérlőket telepíteni.



74. ábra: Címtárszolgáltatások helyreállító módjának rendszergazdajelszava

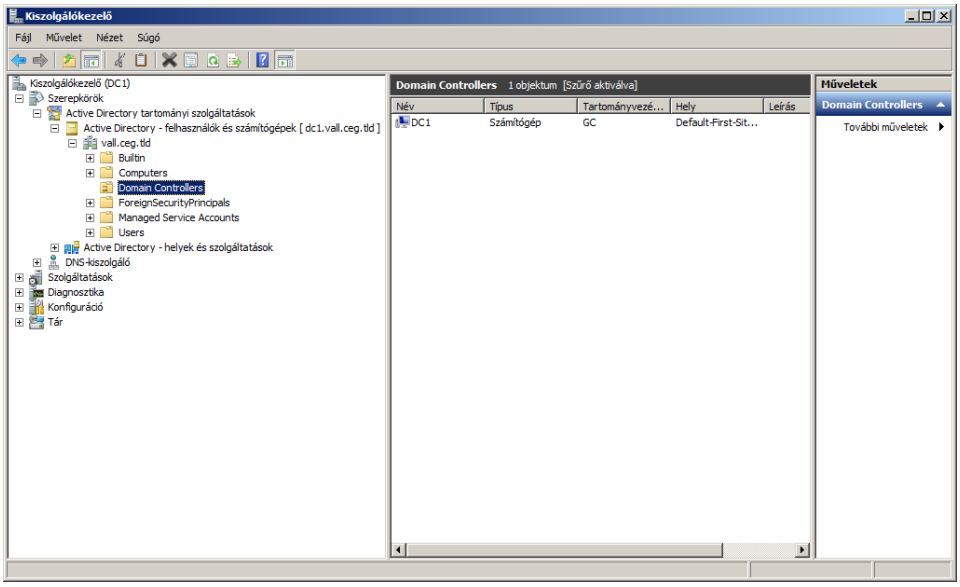
A **tovább** gombra kattintva megkezdődik a tartományvezérlő telepítése, amelynek a végén a **befejezés** (Finish) gombra kell kattintani, majd a változások érvénybelépéséhez **újra kell indítani** (Restart Now) a számítógépet.



75. ábra: A telepítés befejezése

Az újraindítás után a **rendszergazda** (Administrator) felhasználó jelszavát meg változtatni. Itt oda kell figyelni, hogy a tartományi jelszóházirend erősebb jelszót ír elő a nem tartományi Windows kiszolgálónál.

A **kiszolgálókezelőben** (Server Manager), a **szerepkörök** (Roles) és az **Active Directory tartományi szolgáltatások** (Active Directory Domain) alatt megjelenik az **Active Directory – felhasználók és számítógépek** (Active Directory Users and Computers) bejegyzés, valamint utána a tartományvezérlő neve szögletes zárójelekben (itt: [dc1.vall.ceg.tld]). A bejegyzés alatt látható a vall.ceg.tld gyökértartomány alatt megjelenő különböző típusú és nevű tárolókból álló fa struktúra. Megjelenik továbbá az **Active Directory – helyek és szolgáltatások** (Active Directory Sites and Services) bejegyzés, valamint önnálóan a szerepkörök alatt a **DNS-kiszolgálót** (DNS Server) szimbolizáló elem.

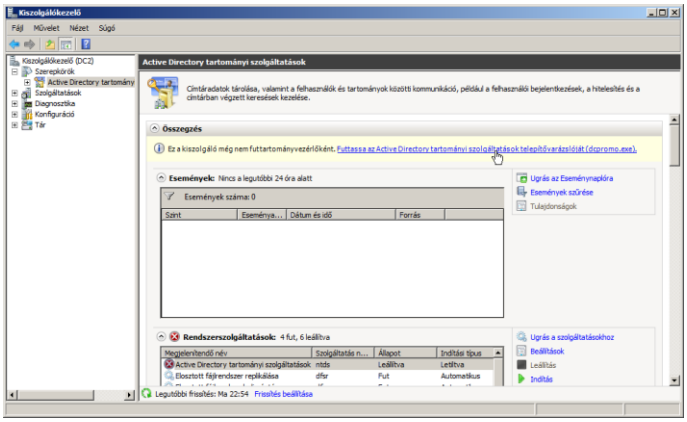


76. ábra: Telepített szerepkörök a kiszolgálókezelőben

1.1.4 Második tartományvezérlő telepítése a tartományban

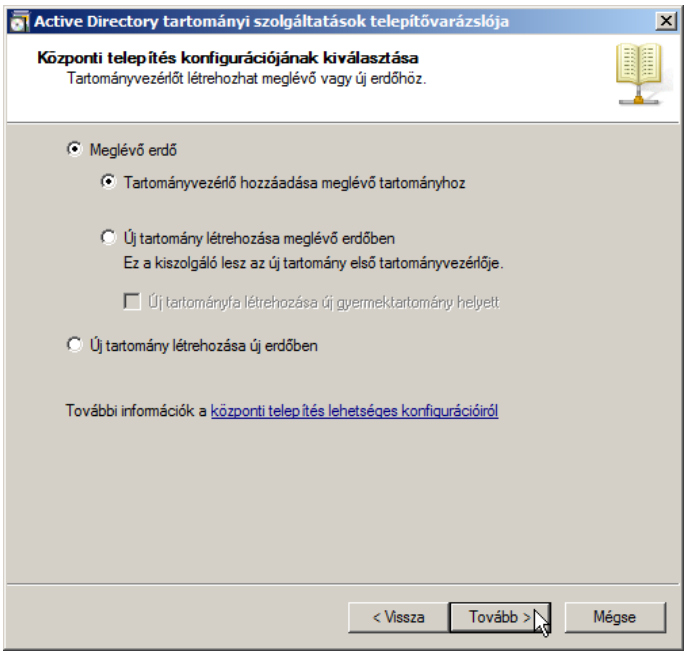
Ahogy az előző leckében már említésre került, egy tartomány esetében ajánlott legalább még egy tartományvezérlő telepítése. Ezzel a lehetőséggel, és azzal, hogy ebből a tartományvezérlőből is DNS kiszolgáló lesz, egyszerre teljesül a „legalább két tartományvezérlő” feltétel, valamint a másodlagos DNS kiszolgáló jelenléte a hálózatban. Mindkettő a megbízható működés alapfeltétele Active Directory hálózati környezetben.

A telepítés első lépése ugyanúgy zajlik, mint az előző esetben. Egy új szerepkört kell hozzáadni a kiszolgálóhoz, ugyanúgy az **Active Directory tartományi szolgáltatásokat** (Active Directory Domain Services), például a **kiszolgálókezelőn** (Server Manager) keresztül. Második lépésként itt is az **Active Directory tartományi szolgáltatások telepítővarázslóját** (Run the Active Directory Domain Services Installation Wizard (dcpromo.exe)) kell futtatni a kiszolgálókezelőből, vagy parancssorból (dcpromo.exe).



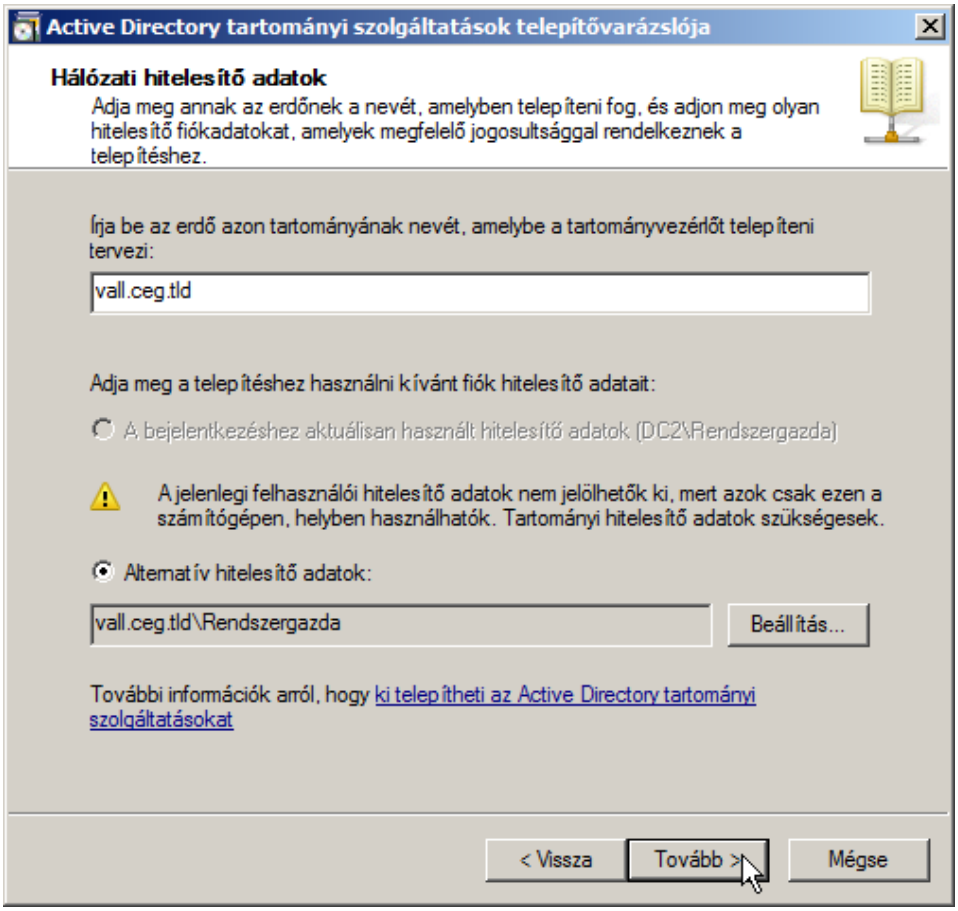
77. ábra: A dcpromo.exe futtatása a kiszolgálókezelőből

A telepítővarázsló nyitólapján először a **tovább** (Next) gombra kell kattintani, majd a megjelenő ablakban a **meglévő erdő** (Existing forest), valamint a **tartományvezérlő hozzáadása meglévő tartományhoz** (Add a domain controller to an existing domain) opciókat kell kiválasztani.



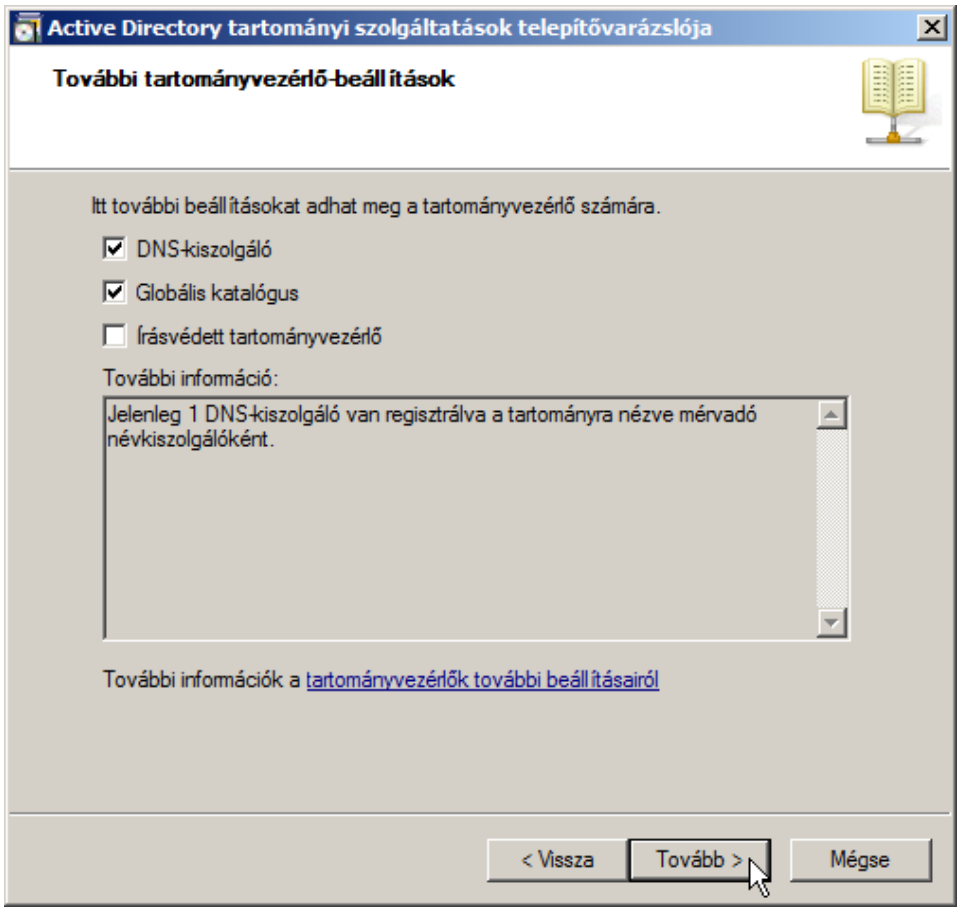
78. ábra: Tartományvezérlő hozzáadása meglévő tartományhoz

A **tovább** gombra kattintva, a megjelenő ablakban meg kell adni a létező tartomány nevét (itt: vall.ceg.tld), valamint a tartományi rendszergazda felhasználói nevét (itt: vall.ceg.tld\Rendszergazda). A **tovább** gombra kattintva a megjelenő listából **ki kell választani a megfelelő tartományt** (Select a domain for this additional domain controller), majd a **tovább** gombra kattintva a **hely kiválasztása** (Select a Site) következik. Itt az **alapértelmezett első hely nevét** (Default-First-Site-Name) kell megadni.



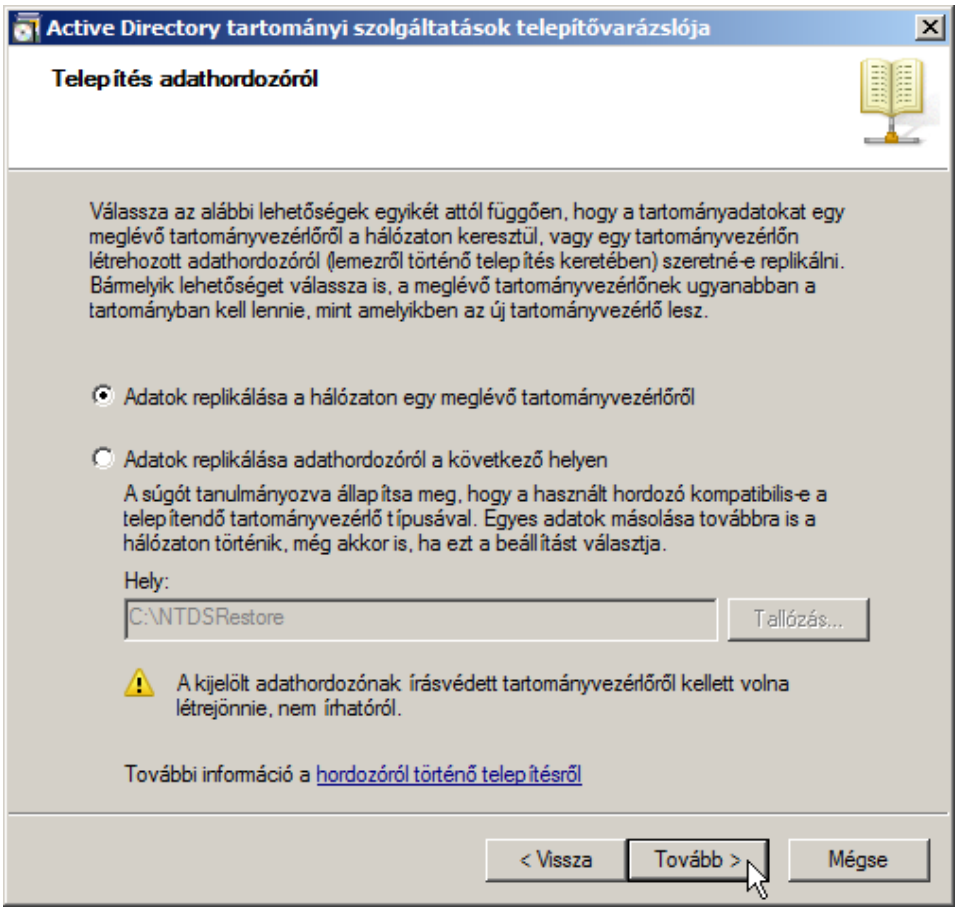
79. ábra: Hitelesítő adatok megadása

A következő lapon lehet kiválasztani, hogy településön-e **DNS-kiszolgáló** (DNS server), **globális katalógus** (Global catalog), illetve **írásvédett tartományvezérlő** (Read-only domain controller (RODC)). Az előbbi kettőt ki kell választani a tesztkörnyezet megfelelő telepítéséhez.



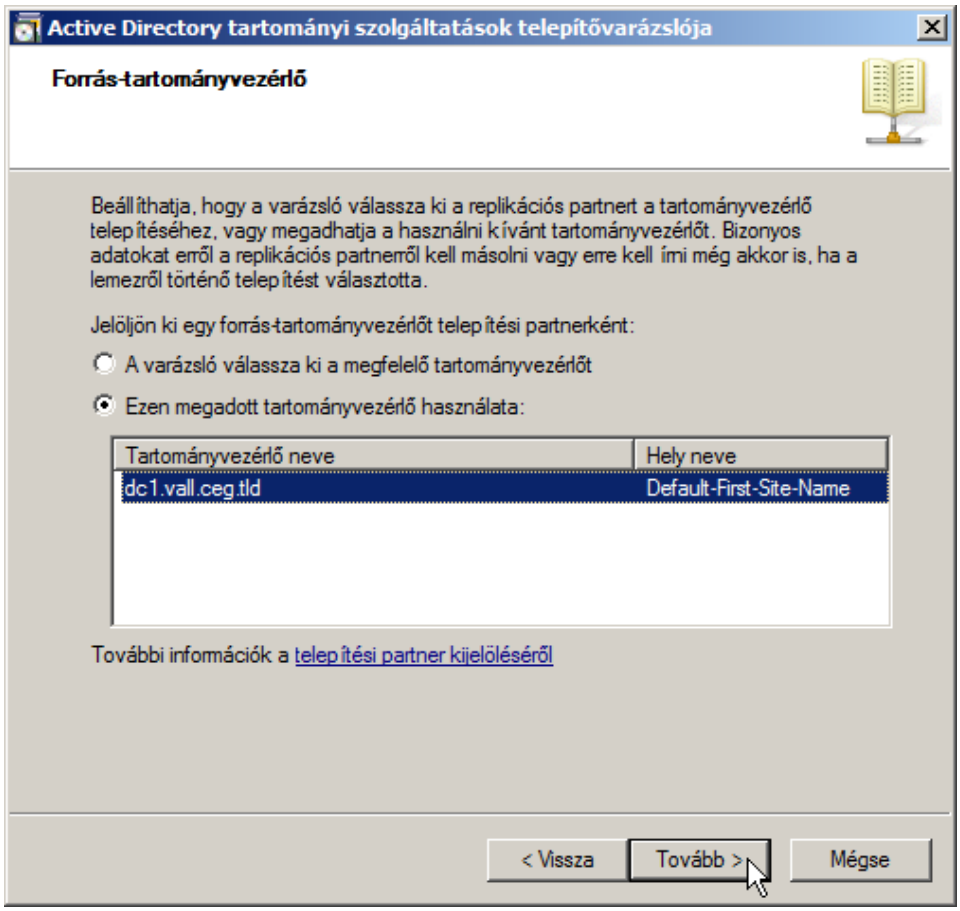
80. ábra: Szükség lesz még egy DNS kiszolgálóra is

A **tovább** (Next) gombra kattintva egy figyelmeztető ablak ugrik fel, amely arról tájékoztat, hogy a DNS-kiszolgálóhoz nem található mérvadó szülőzóna és így nem hozható létre delegálás. A folytatáshoz az **igen** (Yes) gombra kell kattintani, majd a következő megjelenő lapon az **adatok replikálása a hálózaton egy meglévő tartományvezérlőről** (Replicate data over the network from an existing domain controller) opciót kell választani, a következő lépésben pedig a tartományvezérlőt kell megadni (itt: dc1.vall.ceg.tld).



81. ábra: Replikáció beállítása

A **tovább** (Next) gomb választása után már minden lépés ugyanaz, mint az első tartományvezérlő telepítése esetén. A telepítés végén a tesztkörnyezet már egy egytartományos erdőből áll, amelyet két, DNS kiszolgálót az AD-ban integrált tartományvezérlő kiszolgáló működtet.



82. ábra: Forrás tartományvezértlő

5.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

5.3.1 Összefoglalás

A leckében tárgyalásra került az Active Directory (AD) címtár és a tartományi névszolgáltatás (DNS) összefonódása, illetve az, hogy az AD nem tud meglenni a DNS nélkül, tulajdonképpen arra épül. A DNS szolgáltatás az internet működésének is az alapja, így működését más tanulmányok alapján is jól ismerheti a hallgató. Az IP protokollban alkalmazott IP címek és nevek összerendelésében nem a DNS volt az első próbálkozás, de mindenképpen az a legsikeresebb.

A leckéből kiderült, hogy nem szükséges DNS-t telepíteni az AD-t kezelő Windows kiszolgálóra, ha már van DNS kiszolgáló a hálózatban és az megfelel

bizonyos feltételeknek, azonban célszerű mégis a gyártó által ajánlott és a Windows kiszolgálóhoz adott DNS kiszolgálót telepíteni a különböző problémák és kényelmetlenségek végett.

A tartományfák felépítésénél figyelembe kell venni a gyökértartományt, amelyet nagy körültekintéssel kell megválasztani, követve az aktuális gyártói ajánlásokat.

A tartományvezérlői szerepkör telepítésével új tartományi környezet hozható létre, vagy a kiszolgáló integrálható egy már létező tartományi környezetbe.

5.3.2 Önellenőrző kérdések

1. Ismertesse a DNS működését!
2. Miért nem tud működni az AD DNS nélkül?
3. Milyen jellemzőkkel kell bírnia a DNS kiszolgálónak, hogy alkalmas legyen az AD-vel való együttműködésre?
4. Mire jó a SRV rekord?
5. Mire kell figyelni a gyökértartomány nevének megválasztásánál?
6. Hogyan kell a tartományvezérlői szerepkört telepíteni?
7. Ismertesse tartomány második tartományvezérlőjének telepítését!

6 CÍMTÁR OBJEKTUMOK LÉTREHOZÁSA ÉS KEZELÉSE

6.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Ebben a leckében az Active Directory objektumai kerülnek ismertetésre, különös tekintettel az olyan biztonsági objektumokra, mint a felhasználói, számítógép és csoportfiókok. Ismertetésre kerülnek a felhasználói fiók legfontosabb jellemzői, valamint a felhasználói csoportok szerepe, előnyei és típusai.

Tárgyalásra kerülnek a beépített, és az alapértelmezett tartományi helyi, globális és univerzális csoportok. Említésre kerülnek a hozzáférés-vezérlés szempontjából lényeges csoport egymásbaágyazások és használatuk előnyei. A tananyag végén a szervezeti egységek szerepéről, valamint használatuk előnyeiről lesz szó.

A tananyag elsajátítása után a hallgató meg tudja különböztetni az AD információs és biztonsági objektumait, ismerni fogja a közöttük lévő különbségeket, mind tulajdonságaikban, mind felhasználásukban. A hallgató képes lesz a csoportképzés alapszabályait alkalmazva a célnak megfelelő csoportok kialakítására. Ismerni fogja és tudja majd alkalmazni az A-G-DL-P elvet. Meg fogja érteni a felhasználói csoportok és a szervezeti egységek és más tároló objektumok közötti különbséget.

6.2 TANANYAG

6.2.1 Az AD objektumai

Ahogy az a 4. fejezetben már bemutatásra került, az AD nem más, mint egy objektum orientált adatbázis. Elemei, mint például a felhasználói fiókok, számítógépfiókok, a szervezeti egységek vagy akár a megosztott erőforrások, mindmind objektumok, melyeket tulajdonságaik jellemeznek. Ezeknek a tulajdonságoknak attribútum a nevük. Egy felhasználói fiókot vizsgálva, a fiókot reprezentáló felhasználó fiók objektum legfontosabb attribútumai pl. a következők: **globálisan egyedi azonosító** (Globally Uniq Identifier – GUID), **biztonsági azonosítószám** (Security Identifier - SID), bejelentkezési név, teljes név, e-mail cím, jelszó, csoporttagságok, vagy a fiók olyan beállításai, mint például a jelszó lejáratára és megváltoztatására vonatkozó lehetőségek.

Az objektumok típusait azok attribútumai határozzák meg, amelyeket a séma definiál, melyek egy külön címtárpartíción találhatók az AD-ben. Az objektumoknak két alaptípus létezik. Az egyik tartalmazhat további objektumokat, a másik nem. Az előbbinek **levél** objektum (Leaf), az utóbbinak tároló vagy **konténer** (Container) objektum a neve. Mindkettőből többféle létezik. A levél típusúból már jó pár fel lett sorolva az imént (pl. felhasználói fiók objektum, vagy számítógép fiók objektum).

A tároló típusú objektumok közül a legfontosabb a **szervezeti egység** (Organizational Unit – OU), amelynek fontos tulajdonsága, hogy azon kívül, hogy a levél típusú objektumokon kívül további szervezeti egység objektumokat is tartalmazhat. Segítségével a címtár áttekinthetőbbé, strukturáltabbá tehető, sőt akár az intézmény szervezeti felépítése is leképezhető rá. Ez utóbbi azért lehet hasznos, mert segítségével különféle biztonsági és egyéb beállítások lesznek ráhúzhatók az adott szervezeti egység felhasználóira, számítógépeire, meghozzá az ún. **csoportházirend** (Group Policy – GP) szolgáltatáson keresztül. A tartomány tervezésénél, létrehozásánál ezért is tanácsos a „kevesebb tartomány, helyette szervezeti egységek” elvet követni.[33]

Tulajdonképpen azt lehet mondani, hogy a szervezeti egység objektumok segítségével a tartomány logikai egységekre osztható, mely egységek önálló biztonsági és más beállításokkal rendelkezhetnek.

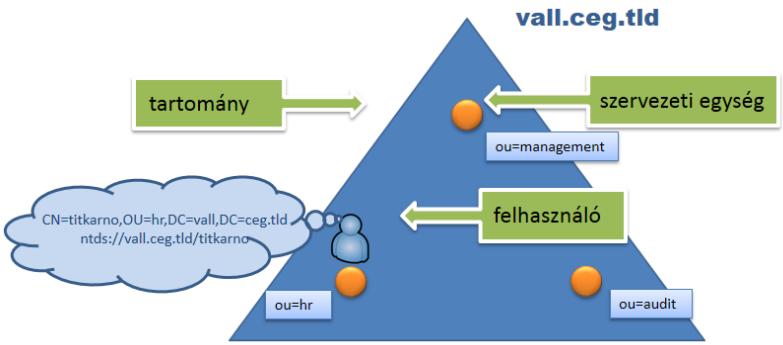
A címtárban több beépített tároló is található, amelyek a tartományi objektumok alapértelmezett helyei. Közülük csak a **Domain Controllers** (tartományvezérlők) tároló objektum szervezeti egység. A legfontosabbak:

- **Domain Controllers** (tartományvezérlők) szervezeti egység: alapértelmezés szerint ebbe a szervezeti egységbe kerülnek bele a tartomány tartományvezérlői.
- **Builtin** (beépített) tároló: alapértelmezés szerint itt tárolódnak a beépített helyi felhasználócsoportok.
- **Computers** (számítógépek) tároló: alapértelmezés szerint itt tárolódnak a tartományban található, valamint az újonnan a tartományhoz adott számítógép fiókok.
- **Users** (felhasználók) tároló: alapértelmezés szerint itt tárolódnak a tartomány felhasználói és csoportjai. Az ún. golbális és univerzális csoportok is itt találhatóak.

[33] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

Az utolsó három tároló nem szervezeti egység, így nem lehet bennük újabb tároló objektumot létrehozni, valamint nem is képeznek külön logikai egységet a tartományban, ezért nem vonatkozhatnak rájuk külön beállítások.

Például a Domain Controllers szervezeti egységbe kerülnek bele alapból a tartomány tartományvezérlői és ez biztosítja, hogy a tartományvezérlőkre más beállítások vonatkozzanak, mint a tartomány többi számítógépére. A többi számítógépre ugyanis a tartományhoz rendelt házirend, míg a tartományvezérlőkre a tartományvezérlők szervezeti egységhez rendelt házirend vonatkozik.



83. ábra: Alapértelmezett tárolók a kiszolgálókezelőben

6.2.2 Biztonsági és információs objektumok

Az AD alapszolgáltatásai, mint korábban a 4. leckében említésre került, az azonosítás, valamint a hozzáférés vezérlés. Ehhez a címtár kétféle típusú objektumot tart nyilván. Az egyik a biztonsági objektum, vagy **biztonsági fiók** (Security Principal), a másik az **információs objektum** vagy egyszerűen csak objektum (Object). Nagy vonalakban az AD a biztonsági fiókokat azonosítja, és vezérli ezen fiókoknak a különböző (pl. információs objektumokban nyilvántartott) erőforrásokhoz való hozzáférését. A lényeges különbségek a két objektum típus között a következők:

- A **biztonsági fiókok** leglényegesebb ismertetője, hogy van **biztonsági azonosítójuk** (Security Identifier – SID). A Windows ezzel az azonosítóval azonosítja a biztonsági objektumokat a különböző hozzáférési engedélyek tárolásakor. Tehát az ilyen objektumoknak hozzáférési engedélyek adhatók a tartományi számítógépek erőforrásaihoz. Ilyen biztonsági fiókokat pl. a tartomány(ok) felhasználóinak és számítógépeinek lehet létrehozni.

- Az **információs objektumok** (gyakorlatilag vagy egyátalán) nem rendelkeznek biztonsági azonosítóval, ezért nekik nem lehet hozzáférési engedélyeket adni. Nagyrészt különböző erőforrások (megosztott mappa, megosztott nyomtató) és egyéb infromációk, tájékoztató jellegű adatok nyilvántartására használja a rendszer. Utóbbiak közé tartoznak pl. a **névjegyek** (Contact) és a **terjesztési csoportok** (Distribution Group) is. Ezek kizárólag nyilvántartási, informatív céllal tárolódnak az adatbázisban. A különböző erőforrásokhoz való hozzáférés ezért rajtuk keresztül nem lehetséges.[34]

6.2.3 Felhasználók

Az előzőekben tárgyalt biztonsági fiók objektumok legjellemzőbb reprezentánsai a felhasználói fiókok, melyek a hálózat kezelés és a hozzáférés vezérlés szempontjából is kiemelt szerepet kapnak. A tartomány erőforrásai és a felhasználói fiókok a már említett hozzáférési engedélyekkel történő összerendelésének alapja az AD felhasználói nyilvántartása. Ez alapján a nyilvántartás alapján történik többek között a felhasználó azonosítása is, amely a tartományba történő bejelentkezés során történik meg.

A klasszikus (vagy hagyományos) felhasználói azonosítás esetében a bejelentkező felhasználó egy felhasználói név, jelszó párossal azonosítja magát. Ezenkívül számos azonosítás létezik, a biometrikus azonosító eljárásoktól a különböző elektronikus, intelligens rendszerekig, ezekkel azonban e tankönyv nem foglalkozik részletesebben.

A Windows operációs rendszerek önmagukban is többfelhasználós rendszerek, mert rendelkeznek helyi felhasználói fiókokkal és csoportokkal is. Egy ilyen rendszerbe történő belépés esetén nem jelent problémát, ha a felhasználó csak a felhasználói névvel és a hozzátartozó jelszóval azonosítja magát, majd ezen a felhasználói fiókon keresztül éri el a számítógép helyi erőforrásait.

Tartományi környezetben, ahol több számítógép erőforrásai is megtalálhatók, az azonosításhoz ez a két alapvető adat már nem elég. Az AD-ban tárolt felhasználói fiókok adatai közül már több említésre került a lecke elején. Ezek közül több is egyértelműen tudja azonosítani a felhasználót a tartományban, de ha kell, akkor az erdőben is, hiszen ebben az esetben az sem mindegy, hogy melyik felhasználó melyik tartomány, vagy akár tartományfa tagja. Ilyen azonosítók többek között a **biztonsági azonosító** (SID), a **globálisan egyedi azonosító** (GUID), de ide lehet sorolni akár a **megkülönböztető neve** (DN) is.[35]

[34] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

[35] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

Bejelentkezéskor tehát a felhasználói név és jelszó pároson kívül meg kell adni a tartomány nevét is, amelyben a felhasználó található. Egy tartományos rendszerben ennek csak annyi jelentősége van, hogy a Windowsnak ezzel lehet jelezni, hogy a felhasználó a tartományba és nem csak az adott számítógépre kíván bejelentkezni. Ezzel szemben több tartományos rendszerben gyakran előfordul, hogy a bejelentkezni kívánó felhasználó nem a saját tartományában található számítógépről akar bejelentkezni, hanem az erdő egy másik tartományának számítógépéről. Így érthető, hogy meg kell adni a felhasználót tartalmazó tartomány nevét is, hiszen ilyen esetben a számítógép annak a tartományvezérlőnek küldi az azonosítási kérését, amelyik a megadott tartományért felelős. Azt sem szabad elfelejteni, hogy a felhasználói neveknek ugyan egyedieknek kell lenniük, de csak tartományon belül. Azaz az egyértelmű azonosításhoz mindenképpen szükséges a tartomány megadása.

A felhasználói név mellett a tartomány megadás kétféle formában történhet, attól függően, hogy a tartomány Windows 2000 előtti vagy utáni rendszert használ. A felhasználói név és a tartomány együttes megadására a bejelentkezési név, két fajtája pedig az **elsődleges felhasználói név** (User Principal Name – UPN) és a **biztonsági fiókkezelő név** (Security Account Manager – SAM). Az előbbi a felhasználói fiók nevéből és a tartomány DNS nevéből áll (UPN utótag), amelyeket a „@” karakter választ el egymástól, az utóbbi pedig a tartomány NetBIOS nevéből (Windows 2000 előtti rendszerben) és a felhasználói fiók nevéből áll, és a „\” karakter az elválasztó jel. Az újabb rendszerekben szinte már csak az UPN név van használatban, de jó tudni, hogy a SAM is működik. A továbbiakban bejelentkezési név mindig az elsődleges UPN felhasználónevet fogja jelenteni.

A bejelentkezési neveknek a leglényegesebb tulajdonságuk, hogy az egész erdőre nézve egyediek, az utótagjuk pedig alapértelmezés szerint a fiókot tartalmazó tartomány, vagy a gyökértartomány teljes DNS nevének valamelyike.

*Legyen például a szervezet, melynek tartományi erdője egy tartományfából áll. A tartományfa gyökértartománya a **vall.ceg.tld**, ennek pedig gyermeke a **marketing.vall.ceg.tld**.*
*A **marketing.vall.ceg.tld** tartományban létrehozott user felhasználói fiók elsődleges felhasználói neve (UPN) a **user@marketing.vall.ceg.tld** vagy a **user@vall.ceg.tld** lehet. Érdemes ezért odafigyelni az UPN név megválasztásánál, ha két különböző, de azonos nevű felhasználó van a szervezetben, hogy semmiképpen se legyenek összekeverve.*

A példából is látszik, hogy az UPN utótag nem feltétlenül azonosítja a fiókot tartalmazó tartományt, a tartományvezérlő mégis tudja azonosítani. Ennek oka, hogy az elsődleges (UPN) felhasználónév szerepel a globális katalógusban,

ahonnan már kiderül, hogy melyik tartományhoz tartozik az adott felhasználói fiók.

A számítógépre történő bejelentkezés esetén tehát a **felhasználói név** (User name) mezőbe az elsődleges felhasználói nevet kell megadni (már ha a cél a tartományba és nem csak az adott számítógépre való bejelentkezés a cél). Az elsődleges felhasználói név megadása esetén a **tartomány** (Domain) mező kitöltése nem szükséges.[36]

6.2.4 Felhasználócsoportok

Egy több felhasználós rendszerben a felhasználók felügyelete elképzelhetetlen **felhasználói csoportok** (Group), röviden csoportok nélkül. A csoportok használata azért hasznos, mert azt veszi alapul, hogy sok felhasználónak hasonló (vagy ugyanaz) a feladata és ezért hasonló (vagy ugyanaz) a jogosultság szükséges ahhoz, hogy bizonyos feladatokat el tudjon látni. Ezek a jogosultságok vezérelhetik a különböző fájlokhoz, mappákhoz, nyomtatókhoz való hozzáférést, de szabályozhatják különböző feladatok végrehajthatóságát is a számítógépen. Az előbbi jogosultságokat a Windows **engedélyeknek** (Permissions) nevezi, és a Windows operációs rendszerek fájlrendszerében, az NTFS fájlrendszerben tárolódnak, ún. **hozzáférés-vezérlési listák** (Access Control List – ACL) formájában. Minden fájlrendszerbeli objektumhoz (pl. fájl, mappa) több ACL kapcsolódhat, és minden ACL egy adott felhasználó vagy csoport engedélyeit tárolja az adott objektumhoz. (Az NTFS engedélyek ismertetése nem képezi a tananyag részét, a témáról bővebben a Kerecsendi András: Hálózati Operációs Rendszerek tankönyvében lehet olvasni.)

Az utóbbi jogosultságokat **jogoknak** (Rights) hívja a Windows, és a rendszer használatához fűződő olyan műveletek szabályozhatóak vele, mint a számítógép elérése hálózatról, a rendszeridő megváltoztatása vagy akár a rendszer távolról történő leállítása.

A felhasználók csoportokban való kezelése több előnnyel is jár, melyek közül a legfontosabb talán az, hogy felhasználók attól függően kaphatnak vagy veszíthetnek el jogokat és engedélyeket, hogy benne vannak-e egy csoportban, vagy sem. Mivel a felhasználók csoport tagsága egyszerűen kezelhető, így egyszerűvé, átláthatóvá és könnyen kezelhetővé válik a felhasználókra vonatkozó NTFS engedélyek és jogok kezelése. Egy másik előnye a csoportok alkalmazásának az engedélyek tekintetében, hogy relatíve kevesebb ACL bejegyzés fog készülni és így tárolódni egy adott objektumhoz, amely egyrészt a tárterület gazdaságosabb kihasználását eredményezi, másrészt az engedélyek vizsgálata is

[36] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

kevesebb időt vesz igénybe, amelynek következménye, hogy gyorsabb lesz az objektumok elérése.

Mivel a Windows egy többfelhasználós operációs rendszer, ezért a felhasználók csoportosíhatósága nem függ össze az AD-val, azaz címtár nélkül is létezhetnek ún. **helyi csoportok** (Local Groups), amelyek között sok alapértelmezett helyi csoport már az operációs rendszer telepítése közben létrejön. A legfontosabb két ilyen csoport, melyekkel gyakran lehet találkozni a **Felhasználók** (Users) és a **Rendszergazdák** (Administrators). (A témáról bővebben Kerecsendi András: Hálózati Operációs Rendszerek tankönyvében lehet olvasni.)

Active Directory telepítése esetén kicsit módosul a helyzet. A tartományvezérlőkön többé nem lesznek elérhetőek a helyi felhasználók és csoportok. Helyettük több felhasználói csoport is létrejön alapértelmezetten. Ezeknek egy része ún. **beépített** (Bultin) csoport, amelyek főleg a **helyi csoportok** AD-ba történő átemelései **tartományi helyi csoportok** (Bulintin local) néven a Builtin tárolóban, másrészük pedig a Users tárolóban létrejövő alapértelmezett csoportok és felhasználók. Az előbbi csoportok olyan „beépített” jogosultságokkal (innen a nevük) rendelkeznek, amelyeket nem lehet tőlük elvenni, illetve más csoportoknak vagy felhasználóknak adni. A tartományi helyi csoport jelentése pedig az, hogy a tartomány összes számítógépén kaphatnak jogosultságokat, azonban az erdő többi tartományában nem, azaz hatókörük a tartományra terjed ki. A beépített csoportok a következők:

- **Fiókfelelősök** (Account Operators): A csoport tagjai jogosultak arra, hogy a tartományban felhasználókat és felhasználócsoportokat hozzanak létre, illetve a nyilvántartásukat kezeljék, de náluk magasabb szintű jogosultságokkal rendelkező csoportokba nem vehetnek fel tagokat. A rendszergazda feladatai megoszthatóvá válnak, ha ebbe a csoportba tagok kerülnek felvételre, mert így másokra bízható a egyszerű, „közönséges” felhasználók nyilvántartásának kezelése, anélkül, hogy más rendszergazda jogokat kapnának.
- **Rendszergazdák** (Administrators): Ennek a csoportnak tagjai a tartomány minden számíógépén rendszergazda jogokkal rendelkeznek. Gyakorlatilag ez a legmagasabb szintű hozzáférés.
- **Biztonságimásolat-felelősök** (Backup Operators): Ezek a felhasználók – biztonsági mentés céljából - hozzáférhetnek minden állományhoz a tartomány minden számítógépén, még azokhoz is, amelyektől különben el vannak tiltva. A jogosultság más állományműveletekre nem terjed ki, az állományok csak a biztonságimásolat-készítő programon keresztül érhetők el számukra.

- **Vendégek** (Guests): A csoport tagjai korlátozott jogosultságú felhasználók. A tartomány egyetlen számítógépén sem rendelkezhetnek felhasználói profillal.
- **Bejövő erdőszintű bizalmi kapcsolat építői** (Incarning Forest Trust Builders): Ebbek a csoportnak a tagjai létrehozhatnak egyirányú, bejövő, erdők közötti meghatalmazásos kapcsolatokat.
- **Hálózatbeállítási felelősök** (Network Configuration Operators): Ennek a csoportnak a tagjai a hálózati beállítások módosítására és paraméterezésére jogosultak.
- **Teljesítménynapló felhasználói** (Performance Log Users): A csoport tagjai elvégezhetik az adott kiszolgáló teljesítménynaplózását és elemzésének ütemezését.
- **Teljesítményfigyelő felhasználói** (Performance Manitor Users): a felhasználóknak joguk van megfigyelni és naplózni a rendszer terhelési és teljesítményszámlálóit, helyben, de akár távolról is.
- **Windows 2000 előtti rendszerekkel kompatibilis hozzáférés** (Pre-Windows 2000 Compatible Access): A tagok a Windows NT 4.0 módján is hozzáférhetnek a tartományi felhasználók és csoportok nyilvántartásához. Minden hitelesített felhasználó (Authenticated Useres) tagja ennek a csoportnak, hiszen nem lehet tudni, hogy mely felhasználók csatlakoznak a rendszerhez Windows 2000 előtti rendszert használó számítógépekről. Elvileg elég lenne csak az ilyen felhasználóknak tagnak lenni.
- **Nyomtatófelelősök** (Printer Operators): A csoport tagjai a tartomány számítógépein szabályozhatják a nyomtatókhoz való hozzáférést, illetve a nyomtatási sarok tartalmát, új nyomtatót nem telepíthetnek.
- **Asztal távoli felhasználói** (Remote Desktop Users): A felhasználóknak joguk van a távoli asztalon bejelentkezni az adott kiszolgálóra.
- **Kiszolgálófelelősök** (Server Operators): Tagjai a tartomány minden, legalább Windows 2000 verziójú operációs rendszerrel működő számítógépén megoszthatnak mappákat, és szabályozhatják az azokhoz való hozzáférést.
- **Windows-hitelesítés hozzáférési csoport** (Windows Authorization Access Group): A tagok jogosultak arra, hogy a felhasználóosztály (Users) meghatározott, számított értékű attribútumát (tokenGroupsGlobalAndUniversal) lekérdezhessék.[37]

[37] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

A Users tárolóban már nem csak tartományi helyi csoportok találhatók alapértelmezetten, hanem ún. globális (Global) és univerzális (Universal) hatókörű csoportok is. A csoportok használata már nagyban függ a szervezet méretétől, a használt tartományok számától és struktúrájától. A mindenekfelett működő univerzális csoportok alapértelmezés szerinti fontosabb csoportjai a következők:

- **Vállalati rendszergazdák** (Enterprise Admins): A csoport tagjai a többtartományos erdők összes tartományában rendszergazda jogokkal rendelkeznek. Az egyes tartományok feletti műveleteket, mint az új tartományok felvétele, vagy a globáliskatalógus-kiszolgálók kijelölése stb. csak e csoport tagjaként lehet elvégezni. A csoportnak kezdetben csak a gyökértartomány **rendszergazda** (Administrator) nevű felhasználó a tagja.
- **Sémafelelősök** (Schema Admins): A tagok módosíthatják a címtáradatbázis struktúráját leíró sémát. A séma erdő szinten egyedi, azaz egy erdőben minden tartomány ugyanazt a sémát használja. Ennek módosítása tartományok feletti művelet, mivel az erdő minden tartományát érinti. A séma módosítására a **vállalati rendszergazdák** csoport tagjai is jogosultak.[38]

A Users tárolóban található alapértelmezett globális csoportok között olyan felhasználócsoport is található, amelybe mindenféle biztonsági fiók felvehető, illetve megtalálható, így a tagok között a felhasználói fiókok mellett szerepelhetnek akár számítógépfiókok és csoportfiókok is. A csoportfiókok egymásba ágyazására meghatározott szabályok vonatkoznak, amelyről később lesz szó. A Users tárolóban alapértelmezés szerint jelen levő fontosabb globális csoportok a következők:

- **Tartománygazdák** (Domain Admins): A tagok a tartomány címtára és számítógépei fölött rendszergazda-jogosultságokkal rendelkeznek. Ez úgy lehetséges, hogy a csoport szerepel a tartomány **rendszergazdák** (Administrators) nevű tartományi helyi csoportjában.
- **Tartományi számítógépek** (Domain Computers): A tartományvezérlőkön kívül a tartományba felvett összes számítógép fiókját tartalmazza. Segítségével egységes hozzáférési engedélyek adhatók azoknak a folyamatoknak, amelyek a számítógépfiók nevében nyitnak meg erőforrásokat.

[38] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

- **Tartományvezérlők** (Domain Controllers): Működésében hasonló a **tartományi számítógépek** csoporthoz azzal a különbséggel, hogy a tartomány tartományvezérlőihez tartozó számítógépfiókokat tartalmazza.
- **Tartományi vendégek** (Domain Guests): A csoport a tartományba vendégszintű jogosultságokkal felvett felhasználókat tartalmazza. A tagok jogait a rendszer azáltal korlátozza a vendégszintre, hogy a csoportot alapértelmezés szerint felveszi a **vendégek** nevű tartományi helyi csoportba.
- **Tartományfelhasználók** (Domain Users): Ebbe a csoportba minden, a tartományba felvett új felhasználó bekerül. Alapértelmezés szerint nem távolíthatók el a tagok ebből a csoportból, amely úgynevezett alapértelmezés szerinti elsődlegescsoport (primary group). Az elsődleges csoport csak akkor változtatható meg, ha a tartományban Macintosh-, illetve UNIX-rendszereket kiszolgáló hálózati szolgáltatások is működnek. Ekkor az egyes felhasználói fiókok elsődleges fiókja megváltoztatható. A szabály az, hogy minden felhasználónak szerepelnie kell a hozzá tartozó elsődleges csoportban.
- **Csoportházirend-létrehozó tulajdonosok** (Group Policy Creator Owners): A tagok jogosultak a tartományban csoportházirend-objektumok létrehozására és azok szervezeti egységekhez rendelésére.
- **DnsUpdateProxy**: A csoport olyan számítógépek fiókjait tartalmazza, amelyek más számítógépek nevében küldenek dinamikus bejegyzéseket a DNS-kiszolgálóknak. Az ilyen számítógépre tipikus példa a DHCP-kiszolgáló, amely IP-címeket oszt szét a hálózatban, és eközben bejegyzi a DNS-kiszolgálónál azokat a számítógépeket, amelyeknek címet osztott.[39]

A Users tárolóban található néhány tartományi helyi csoport is. Ezek közül kettő:

Tanúsítványközzétevők (Cert Publishers): A tagok későbbi felhasználásra szánt tanúsítványokat tehetnek közzé a címtárban.

DNS Admins: A csoport tagjai a DNS kiszolgálón bármilyen telepítési vagy karbantartási műveletet végrehajthatnak.[40]

[39] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

[40] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

6.2.5 A felhasználócsoportok kezelése

Az AD felhasználócsoportjainak megfelelő kezeléséhez meg kell érteni működésüket, tulajdonságaikat. A csoport objektumok két fontos jellemzője a csoport típusa (Type), illetve hatóköre (Scope). Típus szerint kétféle csoport létezik. Az egyik típus esetében a csoportfiók egy biztonsági objektum, ekkor a típust **biztonsági csoportnak** (Security Group) hívják. A másik típus esetén a csoport egy információs objektum, ilyenkor **terjesztési csoport** (Distribution Group) a neve. Ahogy korábban is említésre került, az információs objektumok és így a terjesztési csoport sem kaphat hozzáférési engedélyeket a különböző erőforrásokhoz, azaz mint ahogy a nevében is benne van, csak információs funkciója van. Ez tulajdonképpen azt jelenti, hogy a csoport típusa azt szabályozza, hogy kaphat-e a csoport a különböző erőforrásokhoz hozzáférési engedélyeket.

A terjesztési csoport egyik fő felhasználási területe, hogy csoportos levélküldéshez felhasználható. Ezenkívül a felhasználók valamilyen szempont szerinti csoportosítási funkcióját használják. Az, hogy a terjesztési csoportnak nincs hozzáférési engedélye a különböző erőforrásokhoz, nem azt jelenti, hogy nincs biztonsági azonosítószám (SID). Ebből kifolyólag a terjesztési csoportok és a biztonsági csoportok közötti átalakítás lehetősége adott és működik is.

Egy biztonsági csoportot terjesztési csoporttá alakítva nem veszíti el biztonsági azonosítóját, az csak inaktívvá válik a művelet során. Ennek következménye, hogy a hozzáférési engedélyek ekkor nem érvényesülnek, így a csoport tagjai az átalakítást követően nem rendelkeznek azokkal a jogosultságokkal valamint korlátozásokkal, amelyekkel a csoport tagjaiként rendelkeztek volna. Visszaalakítva a terjesztési csoportot biztonsági csoporttá, a korábbi jogosultságok ismét érvényesek lesznek.

Érdekes, hogy a felhasználói fióknak, mint biztonsági objektumnak is létező információs objektum párja, a névjegy (Contact – kapcsolattartó) nem alakítható felhasználói fiókká és ezért nem kaphat hozzáférési engedélyeket. Azonban bármilyen felhasználói csoportba (biztonsági és terjesztési) felvehető, de csak csoportos adatkezelési, vagy levélküldési céllal.

A csoport másik tulajdonsága a hatókör (Scope) tulajdonképpen azt jelenti, hogy a csoport mely tartományokból kaphat tagokat, illetve mely tartományokban lehet másik csoportoknak eleme, és mely tartományokban kaphat hozzáférési engedélyeket. A hatókör alapján háromfelé bonthatók a csoportok:

- **Tartományi helyi csoportok** (Domain Local Groups): Ezek a csoportok, csak az őket tartalmazó címtárban vehetők fel más csoportokba, illetve biztonsági csoportok esetében csak saját tartományuk számítógépein kaphatnak hozzáférési engedélyeket. Természetesen ennek igazából

több tartományos rendszerben van jelentősége, amikor egy csoport felhasználása a saját tartományán kívül esik. Ebből következik, hogy más tartományok tartományi helyi csoportjai nem lehetnek az adott tartomány tartományi helyi csoportjának tagjai. Azonban univerzális és globális csoportok, valamint az adott tartomány tartományi helyi csoportjai tagjai lehetnek a tartományi helyi csoportnak. Ennek következménye, hogy azonos tartományban található tartományi helyi csoportok tetszés szerint ágyazhatók egymásba olyannyira, hogy a körkörös egymásbaágyazás is lehetséges, hacsak nem egy csoport önmagába történő felviteléről van szó. Ennek ellenére a körkörös egymásbaágyazás nem túl célszerű dolog, ezért jobb kerülni. Kerülni érdemes a tartományi helyi csoportok (főleg többszörös) egymásba ágyazását is, mert a csoporttagságok kiszámítása lelassulhat és megnőhet a bejelentkezési idő.

- A tartományi helyi csoportok a Windows NT Server 4.0 helyi csoportjaihoz képest abban jelentenek újdonságot, hogy nemcsak a tartományvezérlőkön használhatók fel (kaphatnak hozzáférési engedélyeket), hanem a tartomány összes legalább Windows 2000 verziójú operációs rendszert futtató számítógépén. Ha a tartomány működési üzemmódja vegyes, a tartományi helyi csoportok nem ágyazhaták egymásba.

- **Globális csoportok** (Global groups): Ebben az esetben a globális szó arra utal, hogy a csoport a tartományi erdőn belül bármelyik tartományban használható. Azaz tagjai lehetnek az erdő összes tartományában található tartományi helyi csoportjainak, illetve az összes tartományban kaphatnak hozzáférési engedélyeket. Vannak azonban olyan megkötések, amelyek szerint ezek a csoportok csak saját tartományukból tartalmazhatnak tagokat (felhasználókat, globális csoportokat), illetve más tartományok felhasználói és csoportjai, továbbá univerzális és tartományi helyi csoportok nem vehetők fel egy ilyen globális csoportba. A globális csoportok natív üzemmódban a tartományon belül egymásba ágyazhatók (bár ez nem túl célszerű, mert lassíthatja a bejelentkezést), míg ez vegyes üzemmódban nem megengedett.
- **Univerzális csoportok** (Universal groups): Ezek a csoportok onnan kapták a nevüket, hogy tartományi helyi csoportok kivételével bármilyen tartomány felhasználója és csoportja lehet a tagja, valamint maga a csoport is bármilyen tartományban lehet tagja tartományi helyi csoportnak, illetve kaphat hozzáférési engedélyeket. Ez azt jelenti, hogy az univerzális csoportoknak tetszőleges tartományok felhasználói fiókjai, globális csoportjai, továbbá univerzális csoportok lehetnek tagjai. Tartományi helyi csoportok ebben az esetben azért nem lehetnek tagok,

> mert – ahogy már korábban említésre került – a tartományi helyi csoportok nem használhatók fel saját tartományukon kívül. Fordítva viszont mindez lehetséges, azaz univerzális csoport tetszőleges tartomány tartományi helyi csoportjába felvehető, és tetszőleges tartományban kaphat hozzáférési engedélyeket is. Mivel az univerzális csoportok nem köthetők az AD egyetlen tartományához sem, ezért azok. tagságukkal együtt a globális katalógusban tárolódnak. Ezt azért fontos megjegyezni, mert minden egyéb csoport is helyet kap a globális katalógusban, de csak az azonosító adataik erejéig, pl. tagsági adataik továbbra is az adott tartományban tárolódnak.[41]

A hatókörök természetesen megváltoztathatók, persze csak a megadott szabályok szerint. Az alapelv az, hogy a tartományi helyi és globális csoportok univerzálissá az univerzális csoportok pedig tartományi helyi és globális csoporttá alakíthatók. Ebből következik, hogy ha pl. egy globális csoportot tartományi helyi csoporttá kell alakítani, akkor azt a csoportot először univerzálissá kell tenni, majd univerzálisból tartományi helyi csoporttá kell alakítani. Ha az átalakítandó csoport olyan tagot tartalmaz, amelyet az új hatókörrel nem tartalmazhatna, az átalakítás nem végezhető el. (Pl.: ha egy tartományi helyi csoport egy másik helyi csoportot tartalmaz, nem alakítható univerzális csoporttá, vagy egy univerzális csoport másik univerzális csoportot tartalmaz, nem alakítható globálissá stb.)

A felhasználói csoportok a korábban már ismertetett módokon ágyazhatók egymásba (lehetnek egymás tagjai). A hozzáférési engedélyek optimális kiosztásához elengedhetetlen a megfelelő egymásbaágyazás használata. Ezt az egymásbaágyazást csoporttagsági láncnak, vagy röviden csoportok láncának is nevezik.

A csoporttagsági lánc többféle elvet is követhet, melyek közül a leggyakrabban használt és egyben legegyszerűbb az ún. A-G-DL-P elv. Az elnevezés rövidítésekből áll, ahol az „A” a felhasználói fiókot (Account), a „G” a globális csoportot (Global group), a „DL” a tartományi helyi csoportot (Domain local group), a „P” pedig a hozzáférési engedélyeket (Permissions) jelenti. Az A-G-DL-P elv jelentésének lényege az, hogy az azonos, vagy hasonló szerepben dolgozó felhasználókat („A”) egy globális csoportba („G”) fogva már nem szükséges a tartományi erőforrás eléréséhez annyi hozzáférési engedélyt eltárolni, mint amennyi felhasználó van, ilyenkor elegendő egyetlen, a csoporthoz rendelt hozzáférési engedély. Abban az esetben azonban, ha több tartományból álló erdő a helyszín, minden tartományba létre kell hozni az ottani felhasználók egy-egy globális csoportját. Így ugyanahhoz az erőforráshoz már minden csoport hozzáférési engedélyeit létre kéne hozni, ezáltal megint csak megnő az erőfor-

[41] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

ráshoz tartozó hozzáférési engedélyek száma. A megoldást az jelenti, hogy az erőforrás tartományában létre kell hozni egy tartományi helyi csoportot („DL"), amelybe fel kell venni a szóban forgó globális csoportokat, majd a tartományi helyi csoporthoz hozzá kell rendelni a kívánt hozzáférési engedélyeket („P").

Látszik, hogy a teljes lánc alkalmazásának csak több tartományos erdőben, vagy olyan egy tartományos rendszerben van létjogosultsága, amelynek várható több tartományossá történő bővítése. Ha nem várható ilyen jellegű bővítés, akkor kihagyhatók a „fölösleges" elemek a láncból (pl.: A-G-P, A-DL-P, A-P). Érdemes azonban használni a teljes láncot, mert áttekinthetőbbé teszi a kezelést. A csoportok kialakításához egy másik ajánlás szerint érdemes a tartományi helyi csoportokat inkább a meghatározott erőforrásigények szerint, míg a globális csoportokat a munkaköri szerepek szerint kialakítani.

Az A-G-DL-P elvnél léteznek komplexebb egymásbaágyazások is, amelyek pl. olyan esetben fordulnak elő, mint amikor az elérni kívánt erőforrások is több tartományban helyezkednek el. Ilyenkor érdemes lehet létrehozni, majd felvenni egy univerzális csoportot az erőforrás tartományokban az erőforrások hozzáférési engedélyeihez létrehozott tartományi helyi csoportokba. Valamint a globális csoportokat ebbe az univerzális csoporthoz hozzá kell adni (A-G-U-DL-P elv).[42]

*A következő példában a **vall.ceg.tld** gyökértartományú erdő **marketing.vall.ceg.tld** és **sales.vall.ceg.tld** tartományainak vezető beosztású felhasználói a gyökértartomány egyik kiszolgálóján elhelyezkedő megosztott mappákat és megosztott nyomtatót kell elérniük azonos hozzáférési engedélyekkel. A megoldás, hogy mindkét tartományban létre kell hozni egy-egy globális csoportot pl. **MarketingManager** és **SalesManager** néven. A gyökértartományban letre kell hozni egy tartományi helyi csoportot pl. **ManagerFilesAndPrinter** néven. Ehhez a csoporthoz hozzá kell rendelni a megfelelő hozzáférési engedélyeket, majd fel kell venni tagként a két globális csoportot. Végül a két tartományban fel lehet venni a globális csoportokba a kívánt felhasználókat.*

6.2.6 Szervezeti egységek

Korábban már többször szóba került az AD szervezeti egység (OU) tároló objektuma, mint a tartományon belüli objektumok jobban áttekinthető logikai struktúrába szervezésének az eszköze. Fontos azt is megjegyezni, hogy a szervezeti egység, mint adminisztratív egység is megjelenik, azaz akár ún. alárendelt

[42] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

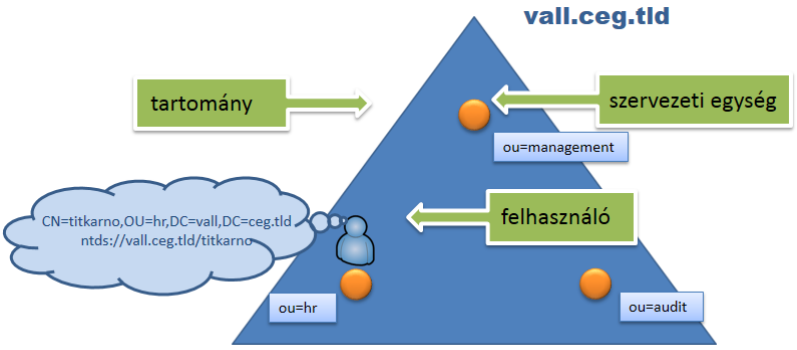
„rendszergazda” is elláthatja egy ilyen egység adminisztratív teendőit, de nem szabad elfelejteni a már korábban szintén említett, és majd a következő leckében tárgyalandó csoportházirendeket sem, melyek szervezeti egységek szintjén juttathatók érvényre.

Ajánlott a szervezeti egységeket használni a szervezet (vállalat, intézmény) szervezeti struktúrájának leképezésére is. Ha nem szükséges a tartományok további altartományokra bontása, akkor e helyett inkább a szervezeti egység használata a célszerű a logikai struktúra kialakítására. Mivel a címtár egy adott objektuma (felhasználói fiók, számítógép fiók, csoport fiók) egyszerre csak egy szervezeti egységben helyezkedhet el, előfordulhat néha, hogy nehéz leképezni a szervezeti struktúrát. Elég a különböző szervezeti egységek fölötti projektmunkákra gondolni. Ilyen esetekben is célszerű mindig a szervezet legstabilabbnak tűnő szervezeti egységeit ábrázolni a címtárban.

A szervezeti egységek által alkotott tartományon belüli logikai struktúra tulajdonképpen tekinthető a címtár tartományi hierarchia egyfajta tartományon belüli kiterjesztésének, folytatásának. Több szolgáltatás esetében is az adott objektumok elérése miatt a hivatkozási neveknek muszáj illeszkednie a címtár által használt hivatkozási névtérhez. A hivatkozási nevek, mint elérési utak megadására alkalmas az LDAP szintaxis, de a Windows 2008-tól bizonyos esetekben lehetőség van URL-ként is megadni egy adott objektumot.[43]

*Legyen például egy titkarno nevű felhasználó a **vall.ceg.tld** tartomány **hr** szervezeti egységében. Az LDAP szintaxis szerint a felhasználó elérési útja a **CN=titkarno, OU=hr, DC=vall, DC=ceg.tld** hivatkozási név. Ugyanez URL-ként **ntds://vall.ceg.tld/hr/titkarno** hivatkozással adható meg.*

[43] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008



84. ábra: A titkárnő a szervezetben

6.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

6.3.1 Összefoglalás

Az Active Directory (AD) nem más, mint egy objektum orientált adatbázis, melyben a különböző objektumokat többek között biztonsági objektumok és erőforrásobjektumok teszik ki. A biztonsági objektumok közül a felhasználói, a számítógép és a felhasználócsoportok kerültek ismertetésre. Ezenkívül szó esett az információs objektumok és biztonsági objektumok közötti különbségekről, valamint a kettejük közötti konverzió lehetőségéről.

A felhasználók csoportokba szervezése egy régi, de nagyon hatékony technika a felhasználói adminisztrációval járó munka és hozzáférés-vezérlés áttekinthetőbbé tételére. A felhasználók alapértelmezett jogosultságai is ezen keresztül oszthatók ki a legegyszerűbben. Ehhez állnak rendelkezésre a beépített, és alapértelmezett tartományi helyi, globális és univerzális csoportok.

Az A-G-DL-P elv jelentése az, hogy a felhasználói fiókot (Account) egy globális (Global) csoporttagságon keresztül kell felvenni, egy tartományi helyi (Domain Local) csoportba, hogy azon keresztül kaphasson hozzáférési engedélyeket (Permissons) a kért tartományi erőforrásokhoz.

A szervezeti egységet több dolog is megkülönbözteti más tároló objektumoktól. Az egyik pl. az hogy a szervezeti egység tartalmazhat újabb tároló objektumokat, míg a többi nem. A másik lényeges különbség az, hogy a szervezeti egységhez hozzárendelhető csoportházirend-objektum, mellyel felhasználói jogok és a felhasználói munkakörnyezet kezelhető. A szervezeti egység és a csoport közötti különbség az, hogy míg az előbbi a tartományi logikai struktúra

állandó és ilyen formán csoportosító része, az utóbbi inkább egy feladatok alapján szerveződik.

6.3.2 Önellenőrző kérdések

1. Mi a különbség a levél objektum és a tároló objektum között?
2. Mi a különbség a biztonsági objektum és az információs objektum között?
3. Soroljon fel 2-2 biztonsági és információs objektumot!
4. Soroljon fel a felhasználói fiókhoz tartozó attribútumokat!
5. Melyek a csoportszervezés előnyei?
6. Mi az A-G-DL-P elv és mire jó?
7. Hasonlítsa össze a szervezeti egységet és a biztonsági csoportokat!

7 CÍMTÁRSZOLGÁLTATÁSOK

7.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Ebben a leckében olyan címtárszolgáltatások kerülnek ismertetésre, mint a tanúsítványkezelés vagy a csoportházirend.

A tanúsítványkezeléshez és a nyilvános kulcsú infrastruktúra kialakításához szükséges fogalmak tárgyalása után egy vállalat típusú hitelesítésszolgáltató telepítésének ismertetése következik, majd a kiszolgáló használata a leggyakrabban előforduló webkiszolgáló típusú tanúsítvány kiállításának folyamatán keresztül bemutatva.

Említésre kerülnek a csoportházirend segítségével szabályozható beállítások, valamint a csoportházirend-objektumok tárolási jellemzői és a csoportházirend-objektumok replikációjáért felelős szolgáltatás is.

Ismertetésre kerül a csoportházirend kezelése felügyeleti konzol (GPMC) kezelése, valamint a házirendekkel végezhető műveletek. A lecke ezen részében szó lesz még arról, hogy mi történik több csoportházirend-objektum egyszerre történő alkalmazása esetén, illetve a csoportházirend érvényre juttatásának folyamatában. A csoportházirend-objektumok szerkesztése témakörben ismertetésre kerülnek a főbb házirend beállításcsoportok.

A tananyag áttanulmányozása után a hallgató képes lesz egyszerűbb PKI infrastruktúra tervezésére, építésére, telepítésére, valamint tud üzemeltetni tanúsítványkiszolgálót.

A lecke végén a hallgató képes lesz a csoportházirendek kezelésére, a GPMC megfelelő használatára. Képes lesz megtervezni a tartományban alkalmazni kívánt a csoportházirend-objektumokat, hogy azok együttes alkalmazása esetén is minden megfelelően működjön.

7.2 TANANYAG

7.2.1 A megbízható hálózati kommunikáció

Amikor két számítógép kommunikál a hálózaton keresztül, az emberek sokszor bele sem gondolnak abba, hogy ez a kommunikáció akár le is hallgatható. A hálózati kommunikáció biztonságossá tételéhez több összetevő is szükséges. A kérdés az, hogy hogyan biztosítható a hálózaton átmenő adatok hiteles-

sége és titkossága? Azaz hogyan lehet biztonságosan azonosítani az üzenetek küldőjét, illetve, hogyan lehet garantálni, hogy az üzeneteket más ne tudja elolvasni, vagy módosítani? Ezek a felvetett problémák a **nyilvános kulcsú infrastruktúra** (Public Key Infrastructure - PKI) segítségével orvosolhatók.

7.2.2 A nyilvános és a szimmetrikus kulcsú titkosítás

A **nyilvános kulcsú titkosítás** (Public Key Encryption) lényege, hogy a kommunikáció mindkét résztvevője két kulccsal rendelkezik. Az egyik egy **privát**, vagy **személyes kulcs**, amely csak a tulajdonosnak áll rendelkezésére. Ezt a kulcsot úgy kell védeni, hogy senki másnak nem kerülhet a birtokába. A másik kulcs egy **publikus**, vagy **nyilvános kulcs**, amely bárki számára hozzáférhető. Ennek a titkosításnak a jellemzője, hogy a privát kulccsal titkosított üzenet csak a publikus kulccsal fejthető vissza és fordítva, a publikus kulccsal kódolt üzenet, csak a privát kulcs segítségével dekódolható.

Amikor pl. egy e-mail feladójának hitelesítése a feladat, akkor a feladó privát kulcsával titkosítja, majd a címzett a mindenki által rendelkezése bocsátott nyilvános kulccsal visszafejtheti az üzenetet. Ha ez sikerül neki, akkor biztos lehet benne, hogy a feladó küldte az üzenetet.

Ha az üzenet titkosítása a feladat, akkor ugyanez történik, azzal a különbséggel, hogy a küldő a címzett publikus kulcsával kódolja el az üzenetet, amit a címzett a saját privát kulcsával dekódol. Ez utóbbi esetben a privát kulcs tulajdonságai miatt, illetve mert a címzettől máshoz feltételezhetően nem kerül a privát kulcs, csak a címzett tudja a titkosított üzenetet visszafejteni.

A nyilvános kulcsú titkosítási eljárás eléggé erőforrásigényes, ebből kifolyólag lassú is ahhoz, hogy valós idejű, vagy akár interaktív kommunikációhoz megfelelő legyen. Ezért az egyszerűbb, és önmagában nem elég biztonságos **szimmetrikus**, vagy **osztott kulcsú** (Pre-Shared Key) **titkosítás** segítségét kell igénybe venni a nyilvános kulcsú eljárás mellé a probléma megoldása végett. A trükk az, hogy a **nyilvános kulcsú titkosítást** nem az egész kommunikáció titkosítására, hanem csak a kommunikációt majd valójában titkosító, szimmetrikus kulcsú titkosítás kulcsának titkosítására használják. Ez a gyakorlatban azt jelenti, hogy a nyilvános kulcsú titkosítással leggyakrabban osztott kulcsokat, digitális aláírásokat és tanúsítványokat titkosítanak, mivel ezek kis terjedelműek és így a nagy erőforrásigényű nyilvános kulcsú titkosítás rövid ideig terheli a rendszert. A nyilvános kulcsú titkosítások legismertebbjei az RSA (Rivest-Shamir Algorithm) algoritmus különböző változatai.[44]

[44] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

Általánosságban a titkosítási folyamat lépései a következők:

- A feladó előállítja az osztott kulcsot, majd titkosítja a címzett nyilvános kulcsával. Ez biztosítja, hogy a titkosított osztott kulcsot majd csak a címzett tudja visszafejteni.
- A feladó elküldi a címzettenek a titkosított osztott kulcsot, amelyet a címzett saját privát kulccsával visszafejt.
- A feladó megkezdi a kommunikációt a címzettel, a titkosítást az osztott kulcs biztosítja.

A felhasználónak vagy számítógépnek a biztonságos kommunikációhoz szüksége van egy nyilvános kulcsra, amelyet egy ún. tanúsítványkiszolgálótól tud beszerezni. A kapott tanúsítvány tartalmazza publikus kulcsot, de a privát kulcsot nyilván nem. Ez utóbbi biztonságos helyen van tárolva. Tároló lehet egy mappa a fájlrendszerben, de akár egy külön hardvereszköz, pl. USB-kulcs, vagy intelligens kártya.

7.2.3 A nyilvános kulcsú infrastruktúra (PKI)

A PKI legfontosabb összetevői az **elektronikus tanúsítványok** (Certificate), amelyek a számítógépes rendszer valamely elemének azonosítására szolgálnak, a **hitelesítésszolgáltatók** (Certification Authority - CA), amelyek a tanúsítványok kiadásával és hitelesítésével foglalkoznak, és egyéb a tanúsítványok regisztrációjába és a **hitelesítésbe bevont szervezetek** (Registration Authority – RA). A PKI további részei azok az eljárások, szolgáltatások, amelyekkel a számítógépes rendszerek elemeinek kilétét lehet ellenőrizni, digitális aláírást vagy valamilyen titkosítást lehet velük végezni.

A PKI tulajdonképpen egy olyan nyílt szabványokra épülő szoftverkörnyezet, amelyhez a jogi környezet is szorosan kapcsolódik, kiegészülve és a helyi szabályozásokkal. A szoftverkörnyezet a tanúsítványok, a publikus és privát kulcsok felhasználását szabályozza, az egységes tanúsítványkezelést pedig az X.509 szabvány biztosítja. A PKI ezek segítségével a következő funkciókat tudja ellátni egy számítógépes rendszerben:

- **Adatvédelem**, amely magába foglalja a biztonságosabb felhasználó hitelesítést (pl. intelligens kártyákkal), a tárolt vagy a hálózaton átvitt adatok titkosítását, hitelességének és sérthetetlenségének biztosítását.
- **Egyszerűsödhet a rendszerfelügyelet**, hiszen a publikus kulcsú hitelesítés valamilyen formájával szükségtelenné válhat a jelszavak használata. A tanúsítványokkal folytatott azonosítás segítségével megszűnhetnek azok a problémák, amelyeket a jelszavak több felhasználó általi felhasználásából fakadtak.

- **További alkalmazások titkosítására is alkalmas**, mert számos olyan alkalmazási rétegbeli protokoll támogatja a nyilvános hálózatokon történő adatok titkosított illetve hitelesített átvitelét. A leggyakoribb felhasználási terület a webkiszolgálók hitelesítése és adatforgalmának titkosítása a **biztonságos csatlakozó réteg** (Secure socket Layer – SSL) és a **szállítási rétegbeli adatvédelem** (Transport Layer Security – TLS) protokollok segítségével. De meg kell említeni az e-mail küldés **biztonságos többcélú internetes levelezési kiterjesztések** (Secure Multipurpose Internet Mail Extentions – S/MIME) szabvány által támogatott titkosítását is.[45]

A PKI által támogatott legfontosabb alkalmazások:

- felhasználó és kiszolgáló (web, imap, pop, smtp) hitelesítés az interneten
- bejelentkezés intelligens kártyával
- titkosított levélküldés
- hitelesítés vezeték nélküli hálózatokban
- saját fejlesztésű programok egyedi aláírása
- IP-alapú hálózat forgalmának titkosítása
- mappák tartalmának titkosítása

Látható, hogy a PKI rendszere megfelelő biztonságot nyújt összetevői révén. Megvalósított funkciói a következők:

- **Titkosság**: biztosítja a hálózati kommunikáció titkosságát, védelmet nyújt a lehallgatással szemben.
- **Hitelesség**: lehetővé teszi minden olyan személy azonosságának ellenőrzését, aki kapcsolatba kíván lépni a rendszerrel, vagy a rendszer felhasználóival.
- **Bizonyíthatóság**: segítségével igazolható a kommunikáló felek kiléte, és nem lehet letagadni a kommunikáció tényét.
- **Az adatok integritása (sérthetetlensége)**: garantálja, hogy a feladó és a címzett között a kapcsolat sértetlen, vagyis azok az adatok érkeznek meg, amelyeket a feladó elküldött.

[45] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

7.2.4 A PKI elemei

A PKI rendszer sok elemből épül fel, melyek nagy részére már történt hivatkozás. Most ezen elemeknek egy valamivel részletesebb ismertetése következik.

A **tanúsítvány**, **elektronikus tanúsítvány** (Digital Certificate, Certificate) a számítógépes rendszer olyan elemeinek azonosítására szolgál, mint a felhasználó személye, számítógép, intézmény, szolgáltatás vagy egy program. A tanúsítvány által tartalmazott azonosító adatok az elemek típusától függően változhatnak.

Az **aláírt tanúsítvány** (vagy digitálisan aláírt tanúsítvány) hitelesítésre is használható, hiszen ekkor a kommunikációban részt vevő másik félnek sem marad kétsége a felől, hogy a tanúsítványt a jogos tulajdonosa használja. A tanúsítványkezelés az X.509 szabvány alapján működik.

A **digitális aláírás** (Digital Signature) gyakorlatilag egy olyan kivonat, amely a feladó titkos kulcsával van aláírva. A másik fél a titkosított kivonatot visszafejtheti a feladó publikus kulcsával, majd a maga által készített kivonattal össze tudja hasonlítani. A digitális aláírás így biztosítja hitelességet és a sértetlenséget. (Digitális pecsétnek is nevezik.)

A **hitelesítésszolgáltató** (Ceritficate Authority – CA) feladata a tanúsítványok kibocsátása. Ha több ilyen kiszolgáló van a rendszerben üzemeltetve, akkor azok hierarchikus kapcsolatban állnak egymással.

A **tanúsítványlánc** (Certificate Chain) a CA-k által alkotott olyan láncolat, amely azon az elven alapul, hogy a CA-k is rendelkeznek tanúsítvánnyal, amelyet arra használnak, hogy segítségükkel aláírják az általuk kibocsátott tanúsítványokat. Egy CA tanúsítványának egy másik tanúsítvány kiszolgálótól kell származnia, amelynek szintén van tanúsítványa, amely tanúsítvány szintén egy másik CA-tól kell, hogy származzon és így tovább. A CA-k ilyen láncolata végén az ún. gyökér hitelesítésszolgáltató áll. Gyökér CA lehet helyi hálózatban, azonban sok rendszerben a helyi (relatív) gyökér CA hitelesítésére is, külső, nyilvános CA-tól származó tanúsítványt használ. Az utóbbi esetben a tanúsítványlánc végén a nyilvános tanúsítványkiadási lánc gyökér CA-ja áll.

Megbízható tanúsítványok listája (Certificate Trust List – CTL) a tanúsítvány felhasználási helyén (pl. egy számítógépen) tárolt megbízható CA-k listája. Ezek által a CA-k által kiállított tanúsítványokat a rendszer hitelesnek fogadja el. **Tanúsítványvisszavonási lista** (Certificate Revocation List – CRL) pedig a visszavont tanúsítványok listája.

A tanúsítványkezelés olyan folyamatok összességéből tevődik össze, mint a tanúsítványok közzététele, amely során a tanúsítványok a rendszer elemei (fel-

használói, számítógépei stb.) számára elérhetővé válnak. Amíg ez nem működik, addig a rendszer elemei nem igényelhetnek tanúsítványokat. Egy másik folyamat, a tanúsítványok **igénylésének** folyamata (enrollment), amely során a rendszer elemei még mielőtt a nyilvános kulcsú adatvédelmet alkalmaznák, tanúsítványt kell igényelniük egy CA-tól, valamint fogadniuk is kell a megfelelő tanúsítványokat.

Amikor a kliensprogramok (böngésző, levelező stb.) felhasználják tanúsítványukat a rendszernek előbb ellenőriznie kell azt, nem lett-e már visszavonva. A tanúsítványok nem csak visszavonás miatt érvénytelenítődhetnek, hanem azért is, mert pl. lejártak. A tanúsítvány menedzsment a PKI-ban mind a tanúsítvány megújításban, mind a visszavonásban fontos szerepet játszik.[46]

7.2.5 A PKI megvalósítása Windows Server 2008 R2 alatt

A nyilvános kulcsú infrastruktúra megvalósítása nagyrészt azt jelenti, hogy a hálózatban ki kell alakítani a CA-knak egy alkalmas hierarchiáját, és e szerint telepíteni kell őket. Kisebb rendszerek esetén azonban bőven elegendő egy CA telepítése a hálózatban.

A CA szerepkört a **kiszolgáló-kezelőben** (Server Manager) elérhető szerepkör hozzáadása funkcióval lehet telepíteni. Ehhez a kiszolgáló kezelőt elindítva, majd annak bal oldalán található **szerepkörök** (Roles) elemre jobb gombbal kattintva, a megjelenő helyi menüből pedig a **szerepkör hozzáadása** (Add Roles) menüpontot választva, elindul a **szerepkörök hozzáadása varázsló** (Add Roles Wizard).

A **tovább** (Next) gombra kattintva a megjelenő szerepkörök közül ki kell választani az Active Directory tanúsítványszolgáltatásokat (Active Directory Certificate Services), majd a tovább gombra kattintás után egy figyelmeztetés jelenik meg, mely szerint a telepítés után már nem lehet megváltoztatni a számítógép nevét és tartománybeállításait, ezért ezeket ha lehet, akkor inkább a telepítés előtt kell elvégezni. Ezután a tovább gombra lehet választani a szerepköri szolgáltatások közül.

Az alapértelmezetten kiválasztott szolgáltatás a **hitelesítésszolgáltató** (Ceritficate Authority – CA), ez az esetek többségében (és most is) elegendő. Ezenkívül lehet még választani a **hitelesítés szolgáltató webes igénylése** (Certificate Authority Web Enrollment) szolgáltatást is, amelyre akkor van igazából szükség, ha pl. a felhasználóknak az engedélyezett otthoni munkavégzés

[46] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

céljából saját számítógépeiknek a belső hálózatra engedéséhez céges tanúsítványt igényelhessenek. Ehhez egy webes igénylőfelület egy igen kényelmes megoldás. A webes igénylés telepítése most nem kerül ismertetésre, azonban az mindenképpen megjegyzendő, hogy telepítéséhez szükség van a Windows **internetes információs szolgáltatásaira** (Internet Information Services – IIS), azon belül is a **webkiszolgálóra** (Web Server) és a **kezelőeszközökre** (Management Tools), valamint a **távoli kiszolgálófelügyelet eszközei** (Remote Server Administration Tools) szerepkör, **szerepkör-felügyeleti eszközök** (Role Administration Tools) moduljára. Erre a szerepkör-szolgáltatás kijelölése közben figyelmezet is a telepítő varázsló, valamint felajánlja a szolgáltatások telepítését.

Maradva az alapértelmezett kiválasztásnál (hitelesítésszolgáltató) a **tovább** (Next) gombra kattintva a megjelenő képernyőn a telepítés típusát kell megválasztani. Itt kétféle lehetőség közül lehet választani. Az egyik az **önálló** (StandAlone), a másik a **vállalat** (Enterprise) típus. A kettő között a lényeges különbség az, hogy míg a **vállalat** típusú CA sablonok alapján dolgozik, támogatja az AD-ba integrált automatikus tanúsítványigénylést, továbbá felhasználói tanúsítványok kibocsátására alkalmas, addig az **önálló** típus ezeket nem támogatja, és elsősorban csak **gyökér CA** (Root CA) feladatkörben használják, és valamint ha a címtár jelenléte nem várható el. A **vállalat** típus kiválasztása után a **tovább** (Next) gombra kattintva a **hitelesítésszolgáltatók típusának megadása** (Specify CA Type) lapon választani kell a **legfelső szintű hitelesítésszolgáltató** (Root CA), illetve az **alárendelt hitelesítésszolgáltató** (Subordinate CA) típus között. Az előbbit akkor kell választani, ha ez lesz az egyetlen hitelesítés szolgáltató a hálózatban, illetve ha ez lesz először telepítve, az utóbbit pedig olyan esetben, ha a telepítendő hitelesítés szolgáltató a hierarchiában fölötte álló hitelesítésszolgáltatótól kapott tanúsítvánnyal fog rendelkezni. Itt a legfelsőbb szintűt választva, majd a **tovább** (Next) gombra kattintva a következő lépésben a **személyes kulcs** megadásának mikéntjéről kell dönteni.

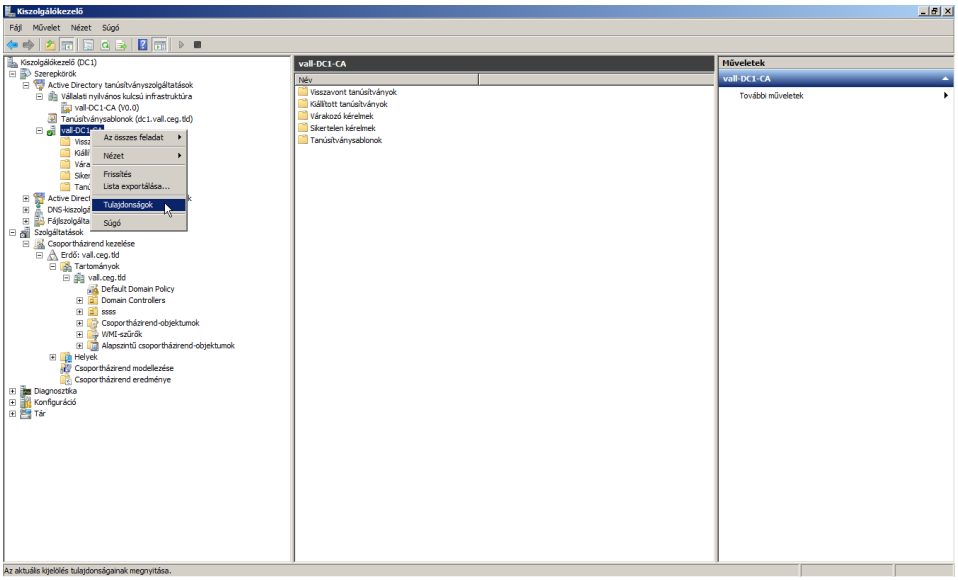
Itt az **új titkos kulcs létrehozását** (Create a new private key) kell választani, hacsak nem már létező CA újratelepítése történik éppen. A következő ablakokban a generálandó kulcs tulajdonságait lehet megadni. Ilyen tulajdonság a **kulcs bithossza**, a **hitelesítésszolgáltató kanonikus neve**, a **gyökértanúsítvány érvényességi ideje**. A kriptográfiai részben, hacsak nincs különösebb oka, érdemes meghagyni az alapértelmezett értékeket. A **kanonikus név** megadásánál érdemes olyat választani, amelyből egyből kiderül a felhasználók számára, hogy ki is a tanúsítvány kiállítója (pl. Cégnév Root CA). **Érvényességi időtartamhoz** egy olyan időhosszt kell megadni, amely pl. az adott rendszer maximális üzemhosszánál valamivel több (pl. 20 év).

A **tanúsítvány-adatbázis beállítása** (Configure Certificate Database) lapon lehet módosítani az adatbázis fájljainak elérési útját. Ezeket a beállításokat is érdemes az alapértelmezett értékeken hagyni. A **tovább** (Next) gombra kattintva egy összegzés látható az elvégzendő műveletekről, amelyeket a **telepítés** (Install) gombra kattintva lehet nyugtázni.

7.2.6 Tanúsítványkezelés

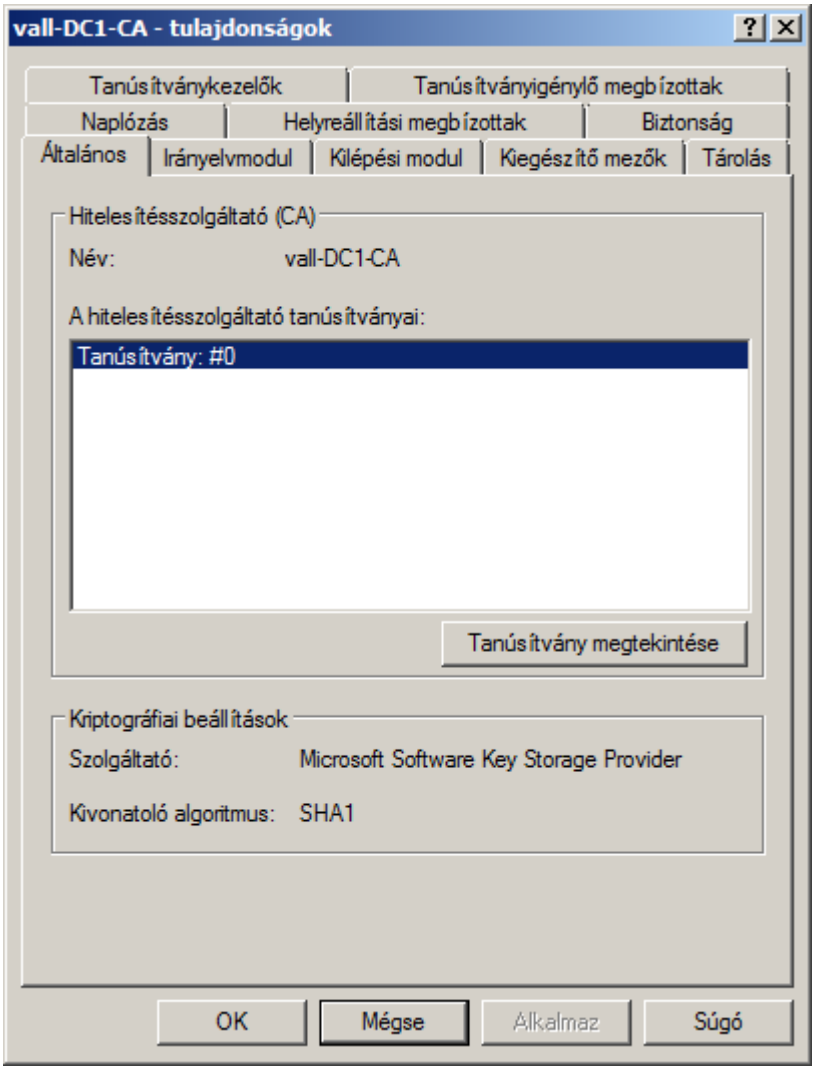
A tanúsítványkezelés elvégezhető a **kiszolgálókezelőből** az **Active Directory tanúsítványszolgáltatások** szerepkör konzol részfa alatt, de akár a **felügyeleti eszközök** (Administrative Tools) alól is indítható a **hitelesítésszolgáltató** (Certificate Authority) menüpont segítségével.

Ez utóbbit választva egy jobban áttekinthető, kevésbé zsúfolt konzolon keresztül adminisztrálható a hitelesítésszolgáltató, vagy tanúsítványkiszolgáló. A baloldalon található konzolfa alatt látható a helyi tanúsítványkiszolgáló, amely tanúsítványokat, kérelmeket és sablonokat tartalmazó mappákat tartalmaz. A tanúsítványkiszolgálóra jobb gombbal kattintva majd a megjelenő helyi menüből a **tulajdonságokra** (Properties) kattintva megjelenik a kiszolgáló beállításait tartalmazó adatlap, ahonnan a beállítások értékeiről lehet tájékozódni, illetve ahonnan meg lehet változtatni őket.



85. ábra: CA a kiszolgálókezelőben

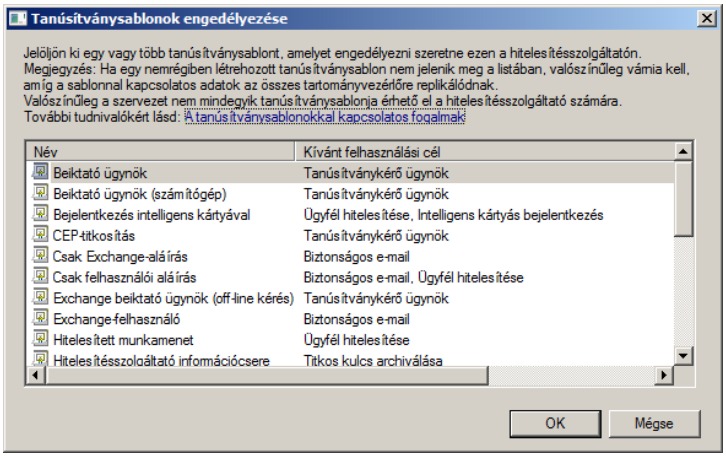
A tanúsítványkiszolgáló alatt található mappák a következők: **visszavont tanúsítványok** (Revoked Certificates), **kiállított tanúsítványok** (Issued Certificates), **várakozó kérelmek** (Pending Requests), **sikertelen kérelmek** (Failed Requests) és a **tanúsítványsablonok** (Certificate Templates).



86. ábra: Új kiállítandó tanúsítványsablon

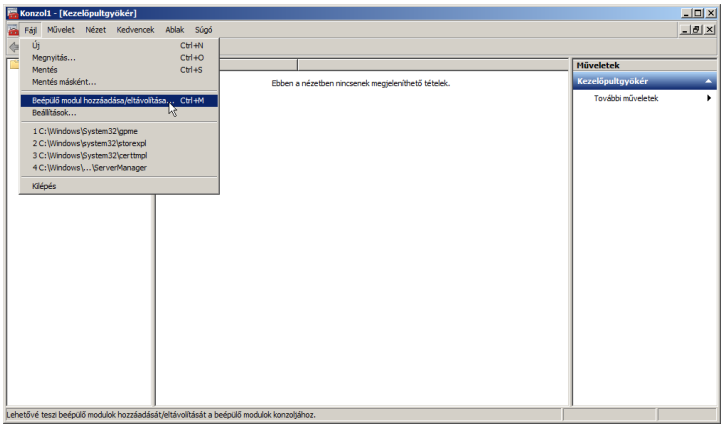
A **tanúsítványsablonok** mappában található sablonok segítségével lehet különböző típusú tanúsítványokat kiállítani. A listában felsorolt tanúsítvány típusoknál többet is támogat a kiszolgáló. Ha a kívánt sablon nincs a listában, érdemes lehet a lista egy üres területére a jobb gombbal kattintva egy új kiállí-

tandó tanúsítványsablont a listához illeszteni. A megjelenő listából további speciális tanúsítványtípusok sablonjai jelennek meg. A megfelelőt kiválasztva, majd az **OK** gombra kattintva a kívánt sablon megjelenik a sablonok mappában.



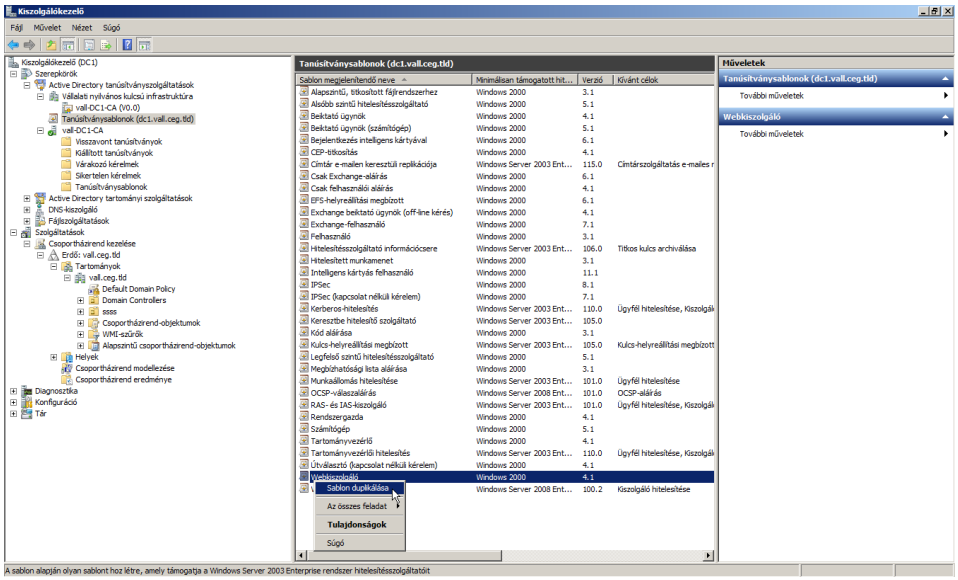
87. ábra: Tanúsítványsablonok engedélyezése

A különböző jogosultságok megbolygatásának elkerülése végett érdemes lehet a tanúsítványsablonokat másolni, valamilyen szempontból egyedivé tenni, majd a megfelelő kör számára megadni rájuk az igénylés engedélyét. Ehhez szükség lesz a **tanúsítványsablonok beépülő modult** (Certirficate Snap-in) betölteni az **felügyeleti konzolba** (Microsoft Management Console – MMC), de elérhető a modul a **kiszolgálókezelőből** (Server Manager) is.



88. ábra: Beépülő modul hozzáadása a felügyeleti konzolhoz

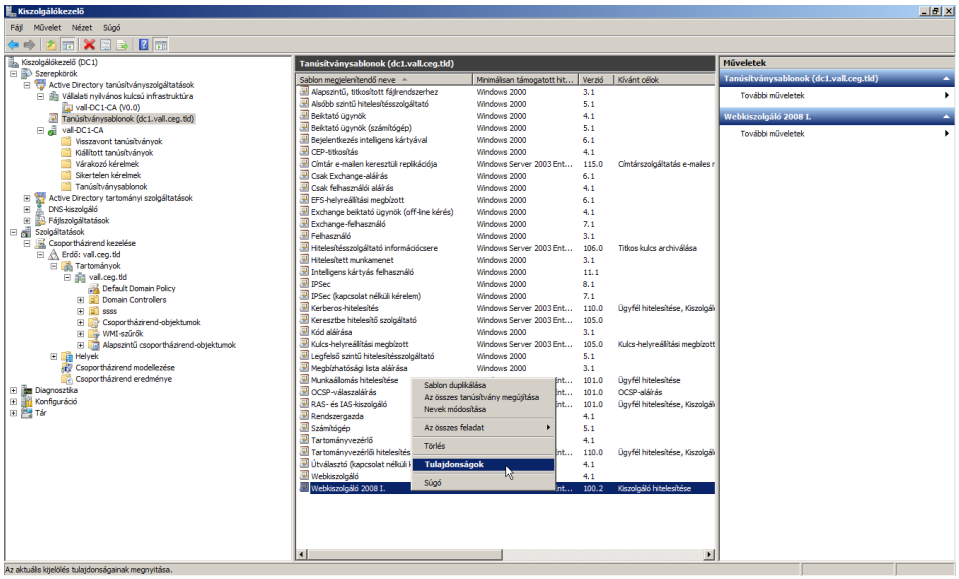
Előbbihez el kell indítani a **felügyeleti konzolt**, amelynek parancsát (mmc) a legegyszerűbben a **start menü** legalsó, kereső mezőjébe kell beírni, majd Enter-t ütni. Ezek után az elinduló konzol, **fájl** (File) menüjében a **beépülő modul hozzáadása/eltávolítása** (Add/Remove Snap-in) menüpontot kell választani. A bal oldali listában a megjelenő modulok közül ki kell választani a **tanúsítványsablonok** (Certificate Templates) modult, majd a **hozzáadás** (Add) gombra kell kattintani, mire a modul a jobb oldali kijelölt modulok listába kerül. A művelet végén az **OK** gombra kell kattintani.



89. ábra: Tanúsítványsablon duplikálása a kiszolgálókezelőből

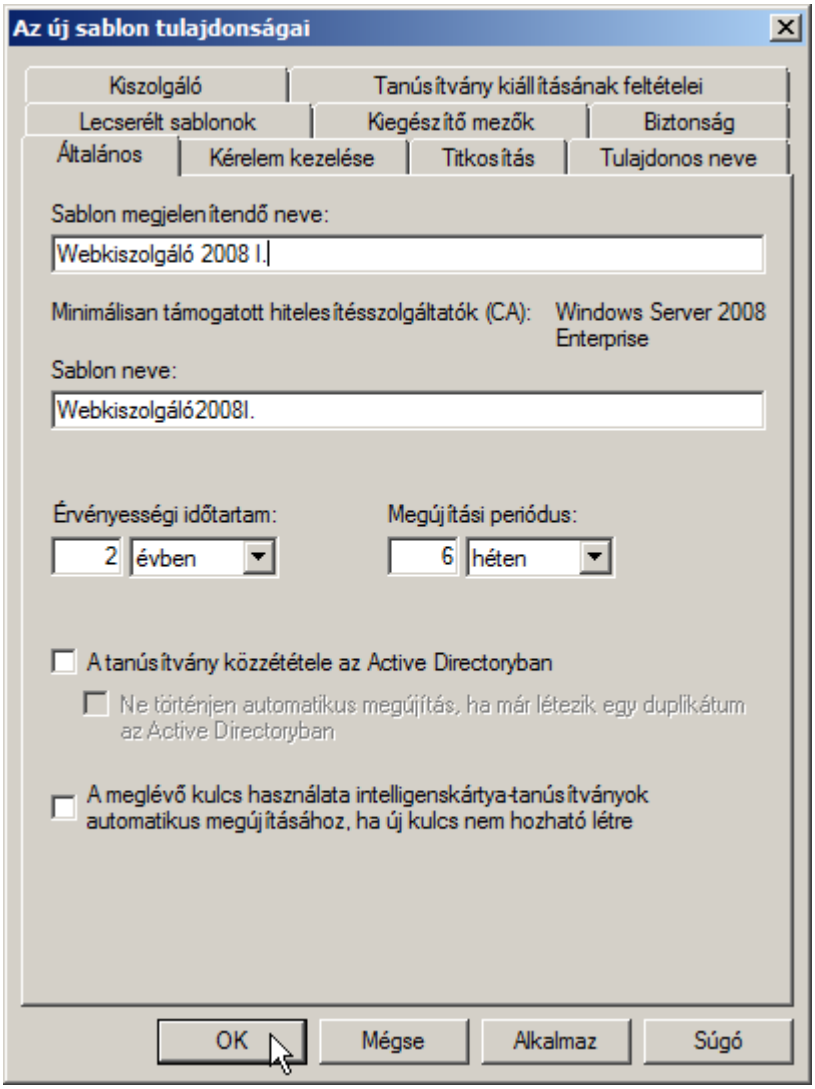
Számos saját igénynek megfelelő, testre szabott felügyeleti konzol készíthető ezzel a módszerrel. A konzol vagy konzolok el is menthetők, parancsikonjuk a start menübe helyezhetők a könnyebb elérés végett.

A kiszolgáló kezelőben ugyanez a modul az **Active Directory tanúsítványszolgáltatások** konzol részfa alatt található **tanúsítványsablonok (kiszolgálónév)** (Certificate Template (Server Name)) alatt található meg.



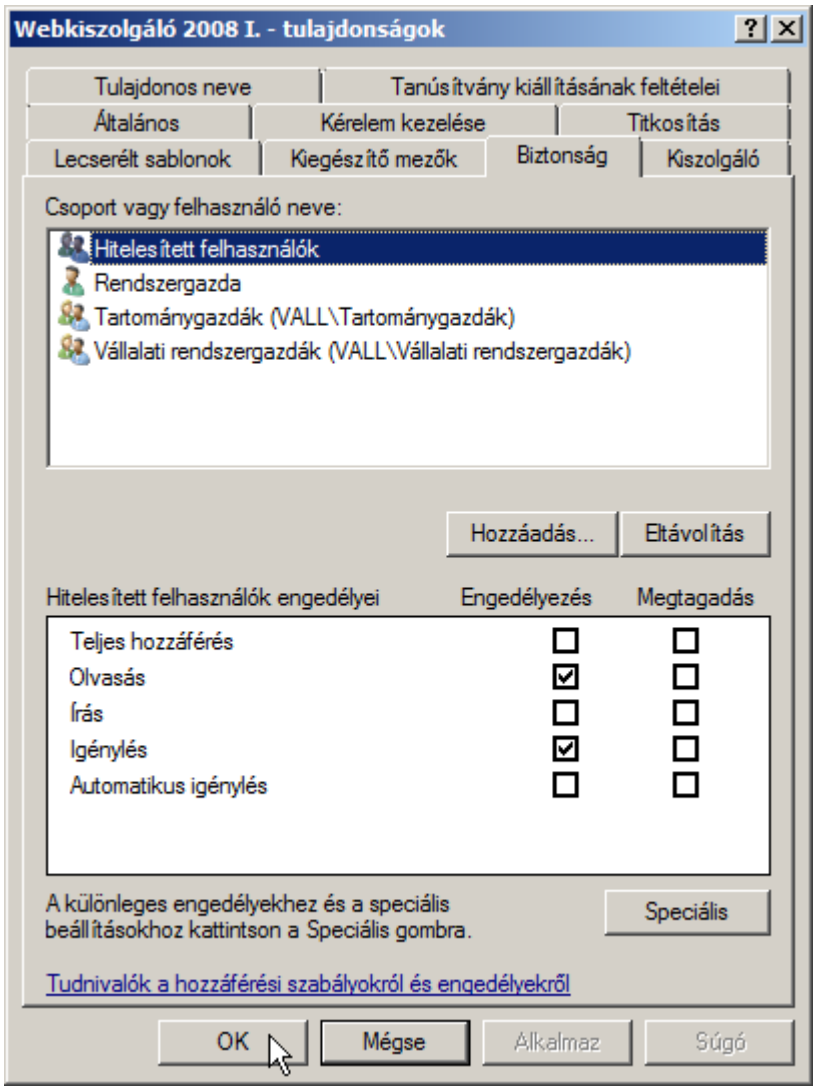
90. ábra: Az új tanúsítványsablon

A tanúsítványsablonok közül a megfelelőt kiválasztva, majd jobb gombbal kattintva, a helyi menüből a **sablon duplikálást** (Duplicate Template) kell választani. Ebben az esetben a **Webkiszolgáló** (Web Server) sablon kerül kiválasztásra. A **duplikálás** (Duplicate) menüpont kiválasztása után megjelenik a **sablon duplikálása** (Duplicate Template) ablak, ahol ki kell jelölni annak a Windows Servernek a verzióját, amelyik ezt a tanúsítványt használni fogja. Ebben az esetben ez a **Windows Server 2008** lesz.



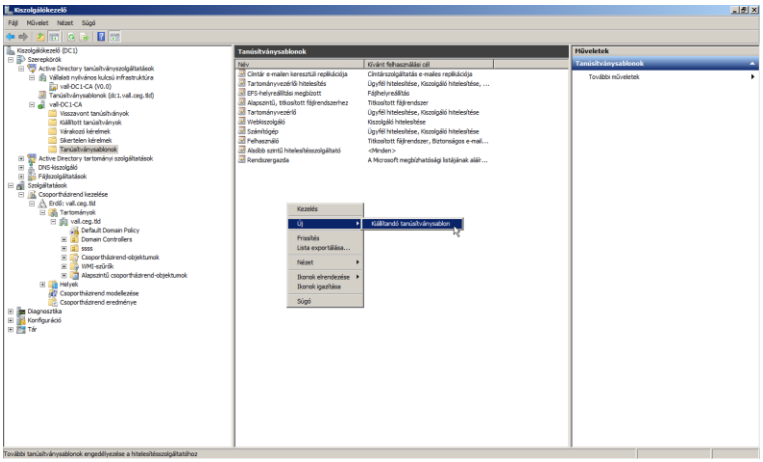
91. ábra: Az új sablon tulajdonságai

Kiválasztása után az **OK** gombra kell kattintani. Ezután a megjelenő **új sablon tulajdonságai** (Properties of New Template) adatlapon, az általános fülön a **sablon megjelenítendő nevéhez** (Template display name) a meg kell adni a másolt sablon nevét, amelynek nyilván különböznie kell az eredetitől. Legyen ez most **Webkiszolgáló 2008 I**, amely név alapján a sablon neve automatikusan létrejön. A többi beállítással az esetek nagy részében nem kell foglalkozni, hiszen pont azért van a sablon lehetőség, hogy ne legyen a művelet túlbonyolítva.



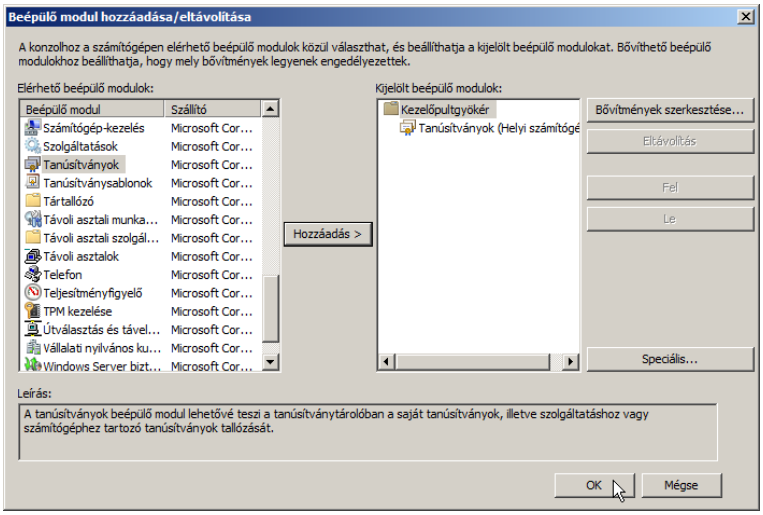
92. ábra: Engedélyek beállítása

A tulajdonságok beállításánál van még egy beállítási opció, amely szükséges a későbbi tanúsítványkérelmezéshez. A **biztonság** (Security) fülön a tanúsítványsablonhoz rendelt **engedélyek** (Permissions) látszódnak. Itt a hitelesített felhasználóknak meg kell adni az igénylés engedélyét.



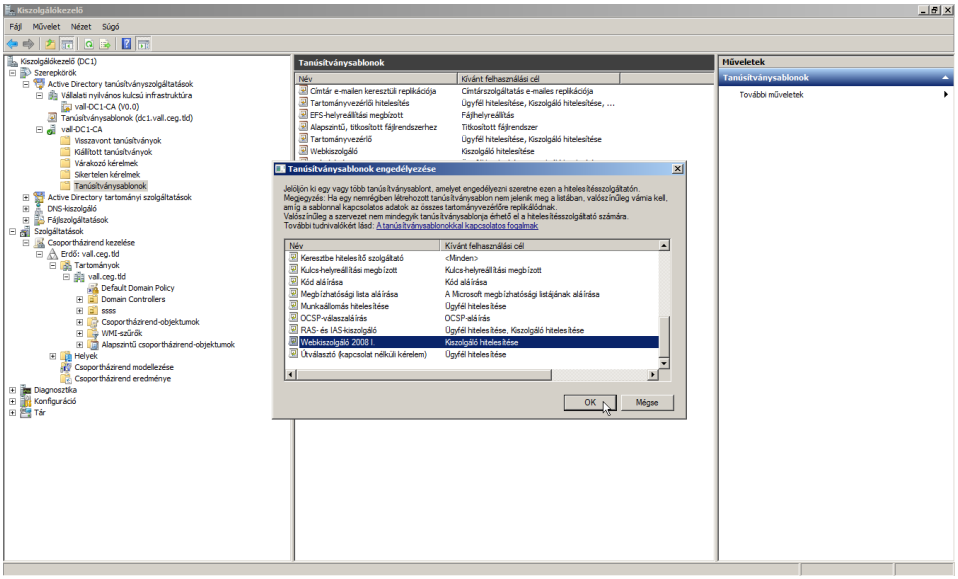
93. ábra: Új kiállítandó tanúsítványsablon

Ha ez készen van, akkor a hitelesítésszolgáltató **tanúsítványsablonok** (Certificate Template) mappájának egy üres területén jobb gombbal kattintva, majd a helyi menüből az **új kiállítandó tanúsítványsablon** (New Certificate Template to Issue) menüpontra kattintva a már ismertetett módszer szerint az új tanúsítványsablont hozzá kell illeszteni a jelenlegi listához.



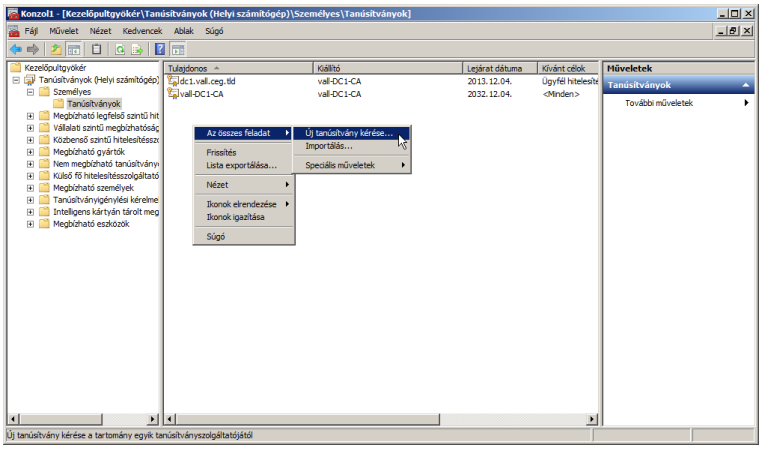
94. ábra: Az új, webkiszolgáló 2008 I. sablon engedélyezése

A tanúsítvány igénylése többféleképen történhet a népszerű webes felületen keresztüli igényléstől, a tanúsítvány beépülő modulon keresztüli, valamint a parancssoros **certreq** eszközön keresztüli igénylésig. Itt most a beépülő modulon keresztüli igénylés kerül ismertetésre.



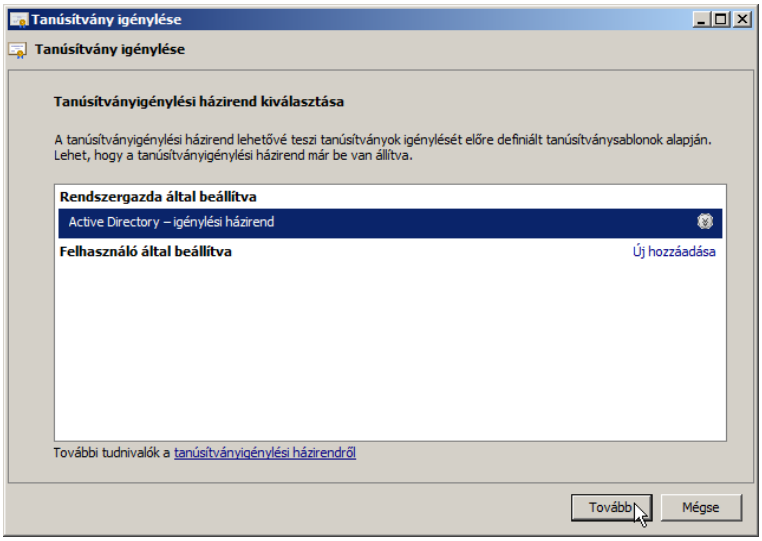
95. ábra: Tanúsítványok modul hozzáadása a felügyeleti konzolhoz

A **felügyeleti konzol** (mmc) elindítása után be kell tölteni a konzolba a **tanúsítványok** (Certificates) modult. A megjelenő párbeszédablakban ki kell választani a **számítógép fiókot** (Computer Account), mivel a tanúsítvány egy webkiszolgáló számítógéphez lesz hozzárendelve. A megjelenő konzolon a **tanúsítványok** (Certificates) alatt ki kell választani a **személyes** (Personal) mappában található **tanúsítványok** mappát. A konzol jobb oldalán megjelenő listában már kell lennie legalább egy vagy két tanúsítványnak, amelyek közül az egyik maga a legfelsőszintű tanúsítvány, a másik pedig a tartományvezérlő nevéhez rendelt tanúsítvány. Az üres területre jobb gombbal kattintva a megjelenő helyi menüben ki kell választani az **összes feladat** (All tasks) közül az **új tanúsítvány kérését** (Request New Certificate).



96. ábra: Új tanúsítvány igénylése

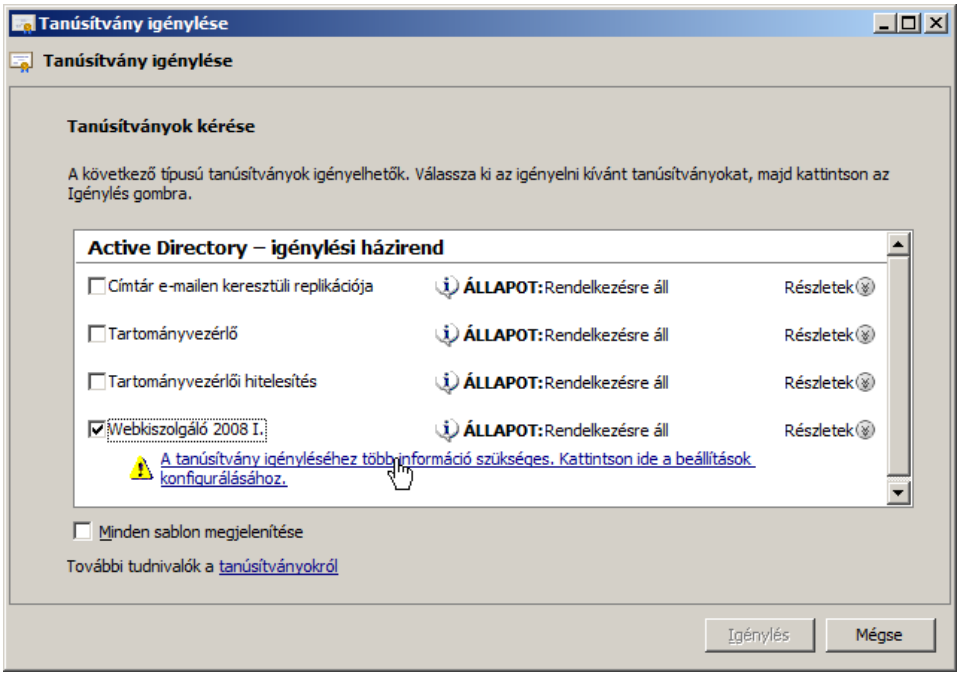
A menüpont kiválasztásának hatására elindul a **tanúsítvány igénylése** (Certificate Enrollment) eszköz, ahol az alapismeretek elolvasása után a **tovább** (Next) gombra kell kattintani. A következő ablakban a tanúsítványházirend kiválasztása történik meg, itt az alapértelmezett, **rendszergazda által beállított** (Configured by your administrator) lehetőséget kell választani.



97. ábra: Tanúsítványházirend kiválasztása

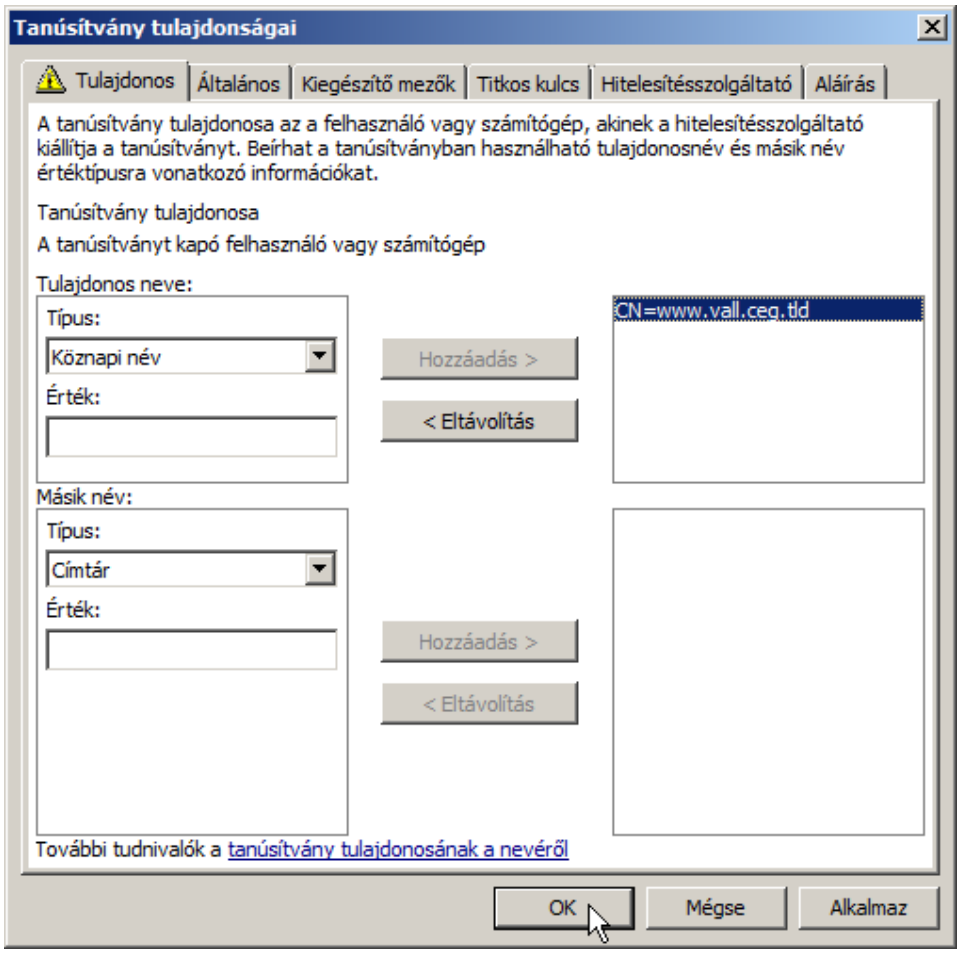
A **tovább** gombra kattintva egy kis várakozás után megjelenik az **Active Directory igénylési házirend** (Active Directory Enrollment Policy) és a jogosult-

ságok alapján használható tanúsítványsablonok. Itt ki kell választani a listából a **Webkiszolgáló 2008 I.** tanúsítványsablont, azonban az igénylés addig nem folytatható, amíg további információk nem lesznek megadva a készülő tanúsítvánnyal kapcsolatban.



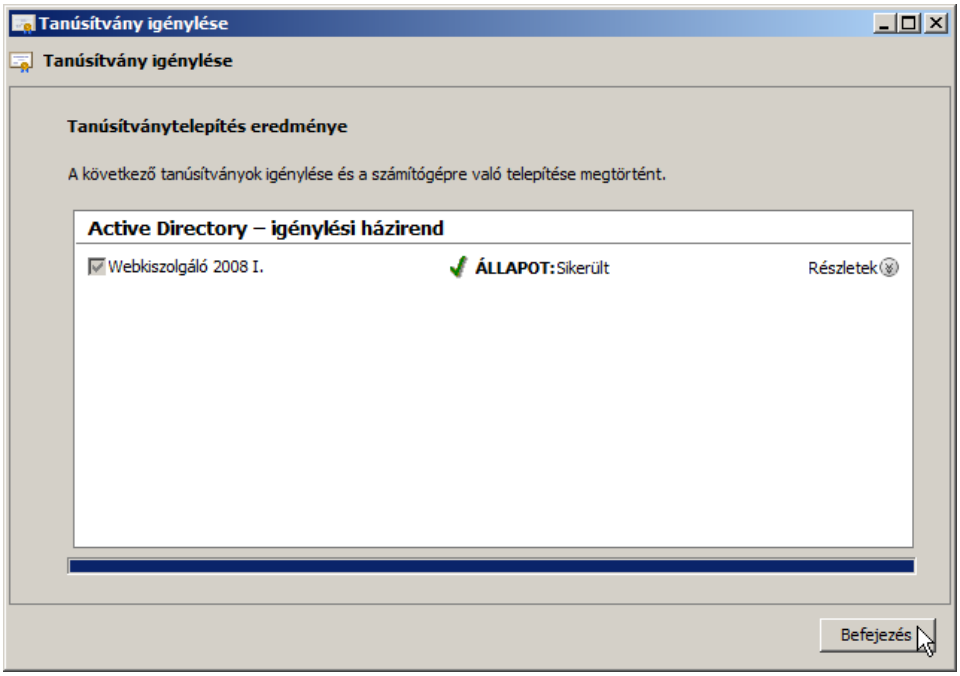
98. ábra: A tanúsítványsablon kiválasztása

A hiányzó adatok megadásához a **kattintson a beállítások konfigurálásához** (Clicke here to configure settings) szövegre kell kattintani. Ekkor megjelenik a **tanúsítvány tulajdonságai** (Certificate Properties) adatlap, amelynek hiányos adatot tartalmazó fülén megjelenik egy kis sárga felkijáltójel. Ebben az esetben ez a **tulajdonos** (Subject) lap, itt is a tulajdonos neve mezőben kell adatot megadni. Ehhez a **típus** (Type) listából a **köznapi nevet** (Common Name) kell kiválasztani, értékének pedig a tanúsítványt igénylő webkiszolgáló **teljes DNS-beli nevét** (FQDN) kell megadni, amely itt **www.vall.ceg.tld**, majd a **hozzáadás** (Add) gombra, végül az **OK** gombra kell kattintani.



99. ábra: A tanúsítvány köznapi nevének megadása

Ekkor már kiválasztható lesz az **igénylés** (Enroll) gomb, rákattintva elindul a tanúsítványigénylés folyamat, melynek végén a **befejezés** (Finish) gombra kattintva, megjelenik a tanúsítványok listájában az új tanúsítvány. Ha ezen a kiszolgáló számítógépen IIS webkiszolgáló lenne telepítve, akkor ez a tanúsítvány pár kattintás segítségével máris használható lenne HTTPS, SSL alapú titkosított HTTP kommunikációra. Persze azt is fontos megjegyezni, hogy az adott névnek léteznie kell a DNS kiszolgálón.



100. ábra: Az igénylés befejezése

7.2.7 A csoportházirend

Az AD címtárszolgáltatások kifejezetten megkönnyítik a hálózatban végzett munkát. Sokszorosan igaz ez a **csoportházirend** (Group Policy – GP) szolgáltatásra, amely számos lehetőséget biztosít a felhasználók munkakörnyezetének központi szabályozására. Segítségével többek között nem kell a különböző beállításokat külön-külön számítógépenként és felhasználónként megadni. Központi távvezérlést ugyan nem tartalmazz a csoportházirend szolgáltatás, ahhoz más eszközök kellenek (pl. a Microsoft System Center Configuration Manager – MSSCCM), azonban a munkakörnyezet szinte minden beállítása szabályozható segítségével. Ilyen beállítások a következők:

- Az elindítható (futtatható) programok és az **asztal** (Desktop) megjelenésének szabályozása.
- Segítségével olyan szinten testreszabható az **Intéző** (Explorer), hogy pl. korlátozhatók az intéző megjelenő menüpontjai, vagy akár az intézőn keresztül elérhető erőforrások is. Ezenkívül segítségével a webböngésző beállításai is szabályozhatók.

- A csoportházirenden keresztül szabályozhatók azok a rendszerszintű jogosultságok, melyek meghatározzák, hogy egy adott felhasználók mit tehetnek meg az egyes számítógépeken és a tartományban.
- A felhasználói mappák alapértelmezett helye a felhasználói profil mappájában található. A csoportházirend segítségével ezek a mappák akár egy kiszolgálóra is áthelyezhetők lesznek annélkül, hogy a munkaállomáson bármilyen beállítást is alkalmazni kellett volna.
- A különböző rendszereseményekhez rendelhető **parancsállományok** (scripts) központilag is szabályozhatók a csoportházirend segítségével. Ilyen parancsállományok lehetnek az **indítási** (startup script), a **leállítási** (shutdown script), a **bejelentkezési** (logon script) és a **kijelentkezési** (logoff script) **parancsállományok**. Mivel ezek a parancsállományok a felhasználók nagy részénél ugyanazok, így csoportházirenden keresztüli megadás jóval egyszerűbb és kezelhetőbb, mint minden felhasználó beállításainál egyenként megadni azokat.
- Mivel egy AD környezetben, ahol előfordulhat, hogy egy felhasználó más tartománybeli számítógépről is bejelentkezhet, nagyon hasznos csoportházirend-szolgáltatás, hogy előírható, hogy egy adott számítógépre milyen programok legyenek telepítve. A telepítés egyébként akkor történik meg valójában, amikor azt a bejelentkezett felhasználó először akarja használni. Ennek analógiájára meghatározhatók a frissítések, újratelepítések és eltávolítások is.[47]

A csoportházirend a Windows 2000 Server óta érhető el, és természetesen a Windows 2000 Workstation volt az első kliens verzió, amellyel lehetett használni a szolgáltatást. A beállítások a tartományvezérlőkön az AD-ban tárolódnak, a munkaállomások onnan töltik le és érvényesítik a szabályozások. Érdemes azt figyelembe venni, hogy a csoportházirend akkor használható hatékonyan, ha az több számítógép beállításait szabályozza. Az AD-ban a legkisebb olyan logikai egység, amelyre különböző csoportházirend beállítások húzhatóak, a szervezeti egység. Általában elmondható, hogy a szervezet (intézmény, cég) szervezeti egységeiben hasonló funkciókat használnak a számítógépeken, hasonló környezetben, ezért célszerű a szervezeti egységek AD-beli ábrázolása és az ezekben tárolt számítógépek csoportházirenddel történő szabályozása.

- A csoportházirendre épül a gyártó **IntelliMirror** nevű technológiája, melynek segítségével pl. meghibásodó, kieső kliens számítógép helyére

[47] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

állított számítógép telepítését a rendszer automatikusan elvégzi. (Indítólemezre is csak akkor van szükség, ha a számítógép nem támogatja a hálózatról történő indítást. A technológia az **AD**-re, a **távtelepítő szolgáltatásra** (Windows Deployment Services – WDS), és a **csoportházirendre** (Group Policy – GP) épül. Az AD a központosított felügyeletet, a WDS az operációs rendszerek távtelepítéstét, a GP pedig a programok telepítését és a számítógép biztonsági és környezeti beállításai biztosítja.[48]

7.2.8 A csoportházirend-objektumok

Az előbbiekben már említésre került, hogy a csoportházirend az AD-ban tárolódik. A tárolás alapja az ún. **csoportházirend-objektum** (Group Policy Object – GPO), azonban ezen keresztül csak az azonosító adatok kerülnek tárolásra. Maguk a beállítások a tartományvezérlők **Sysvol** mappájában tárolódnak egy **Policies** nevű mappa alatt elhelyezkedő mappastruktúrában. Az egyes csoportházirend-objektumok mappáinak nevei az objektumok kapcsos zárójelek közé fogott globális azonosítói (GUID). A kliens számítógépek ezen **Sysvol** mappán keresztül érik el és töltik le a rájuk vonatkozó csoportházirend beállításokat.

Több tartományvezérlő esetén az AD gondoskodik az adatbázis replikációjáról, azonban a **Sysvol** mappában elhelyezkedő csoportházirend beállítások replikációjáról külön kell a rendszernek gondoskodnia. A **Sysvol** mappa több olyan mappát és fájlt tartalmaz, melyek replikációja elkerülhetetlen. Ezt a replikációt Windows 2008 natív működési szinten az ún. **elosztott fájlrendszer replikáció** (Distributed File System Replication – DFSR) szolgáltatás, ezen működési szint alatt pedig a **fájlrendszer replikációs szolgáltatás** (File Replication Service) végzi.

A csoportházirend-objektumok két részből állnak. Az egyik rész a **számítógép beállításait** (Computer Configuration), a másik a **felhasználó munkakörnyezetének beállításait** (User Configuration) tartalmazza. Amikor egy tartományi számítógép elindul, az operációs rendszer betöltése után bejelentkezik a tartományba, majd letölti a tartományvezérlőről, és végrehajtja a rá vonatkozó házirendet. A számítógépre bejelentkező felhasználó munkakörnyezetének beállításai a felhasználó bejelentkezése közben töltődnek le a tartományvezérlőről és jutnak érvényre.[49]

A kétféle házirendobjektum független egymástól, hiszen gyakran előfordulhat például, hogy a felhasználó és a számítógép nem azonos szervezeti egy-

[48] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

[49] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

ségben található meg, ezért más csoportházirend-objektumok vonatkoznak rájuk. Az effektív felhasználói környezetet a két házirendobjektum kombinációja határozza meg.

A számítógépekre és felhasználókra valójában külön-külön is több csoportházirend-objektum lehet érvényes. Ebben az esetben is a különböző csoportházirend-objektumok összessége lesz hatással a felhasználói környezetre. A különböző szintű csoportházirend-objektumokban általában nincs minden beállítás szabályozva. Minden szinten meg van határozva, hogy mely beállításokat célszerű szabályozni, így a végén a különböző szinten szabályozott beállítások együttesen jelennek meg.

A csoportházirendeket szervezeti egységeken kívül a tartományokhoz és a telephelyekhez, rövidebben **helyekhez** (Site) lehet rendelni. Ezek a címtári egységek egy bizonyos hierarchiát alkotnak, amelyek segítségével kialakíthatók az említett szintek. Például ha egy tartományhoz hozzá van rendelve egy csoportházirend-objektum, akkor az szervezeti egységtől és telephelytől függetlenül a tartomány összes számítógépére és felhasználójára vonatkozik. Ha azonban ennek a tartománynak egy szervezeti egységéhez egy másik csoportházirend-objektum van hozzárendelve, akkor a szervezeti egységben található számítógépekre és felhasználókra már két csoportházirend is vonatkozni fog. Ilyen esetekben a két csoportházirend-objektum beállításai együtt lesznek érvényesek. Ha ugyanazt a beállítást mindkét csoportházirend-objektum szabályozza, és a beállítások különböznek, akkor mindig az alacsonyabb szinten (ebben az esetben a szervezeti egységben) található szabályozás lesz a mérvadó.[50]

Ha egy tartományi szintű csoportházirend-objektumban a felhasználók vezérlőpult használata engedélyezve van, a szervezeti egységben viszont tiltva, akkor az alacsonyabb szinten lévő szervezeti egység szabályozása lép érvénybe. Azaz a szervezeti egység felhasználói nem használhatják a vezérlőpultot.

A számítógépek az egyes csoportházirend beállításokat mindig egy megadott sorrend szerint érvényesítik. Először a számítógép helyi házirendjét veszi alapul, majd a telephelyi házirendek következnek. Ezután a tartományi házirend a következő a sorban, amely mindig a tartomány gyökerében található. A sort fentről lefelé haladva a címtár hierarchián, a szervezeti egységhez kapcsolódó csoportházirend zárja. Ha egy beállítás több házirendben is szerepel, akkor mindig a hierarchiában a legalsó beállítás lesz az érvényes.

[50] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

Alapértelmezés szerint egy tartományban két csoportházirend-objektum található. Az egyik magához a tartományhoz, a másik a **tartományvezérlők** (Domain Controllers) szervezeti egységhez tartozó csoportházirend. A tartományhoz tartozó az **alapértelmezett tartományi házirend** (Default Domain Policy), míg a Domain Controllers szervezeti egységhez tartozó az **alapértelmezett tartományvezérlők házirend** (Default Domain Controllers Policy) nevet viseli. Ezekkel az alapértelmezett csoportházirendekkel érhető el, hogy a tartományban egységes biztonsági beállítások tartozzanak a számítógépekhez és felhasználókhoz, azonban a tartományvezérlők biztonsági beállításai jóval szigorúbbak lehessenek.[51]

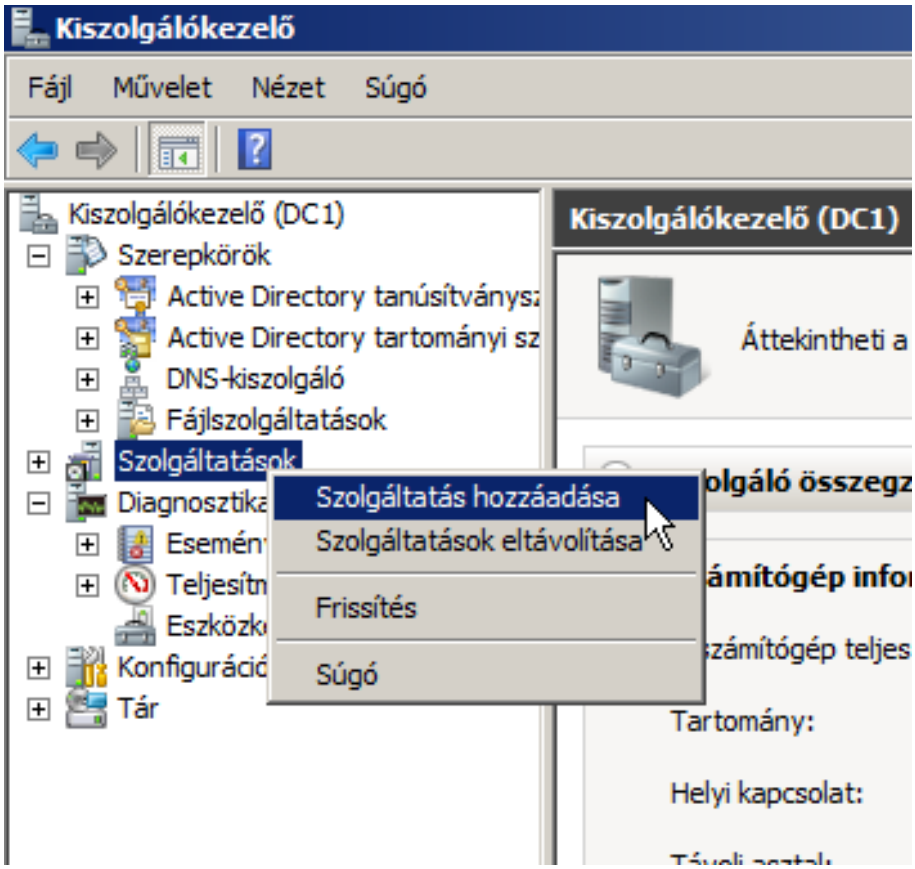
Egy tartományvezérlőn például csak olyan felhasználók jelentkezhetnek be helyben, amelyek rendelkeznek felügyeleti joggal, míg a tartomány többi számítógépére nincsen ilyen megkötés. Ezzel technikával érhető el, hogy a Domain Controllers szervezeti egység csoportházirendjében felülbírálja a tartományi házirend biztonsági beállításait.

- Ezért szükséges, hogy a Domain Controllers tároló egyben szervezeti egység is legyen, az egyéb tárolókhoz (pl.: Computers, Builtin, Users stb.) ugyanis nem lehet csoportházirend-objektumot rendelni.

7.2.9 A csoportházirend-objektumok kezelése

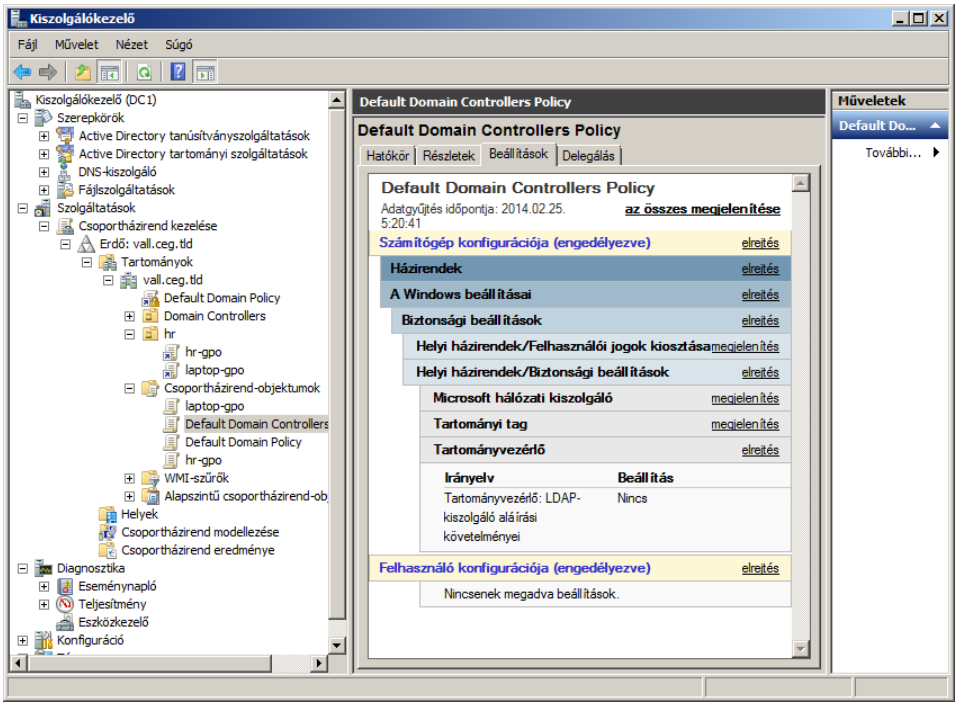
A csoportházirend szolgáltatás és a csoportházirend-objektumok elérése a **csoportházirend kezelése felügyeleti konzolon** (Group Policy Managment Console – GPMC) keresztül történik. A GPMC telepítéséhez a kiszolgálókezelőben (Server Manager), a szolgáltatások hozzáadása szövegre kell kattintani, majd a megjelenő listából a csoportházirend kezelése elemet kiválasztva a **tovább** (Next), majd a **telepít** (Install) gombra kell kattintani. Ezek után a csoportházirend-objektumok kezelése a kiszolgálókezelő **szolgáltatások** (Services) ágán keresztül lesz elérhető.

[51] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008



101. ábra: Szolgáltatás hozzáadása

A **csoportházirend kezelés** alatti struktúrában legfölül az erdő, az alatt pedig a tartományok, illetve helyek látszódnak. A csoportházirend-ojektumok a tartományok neve alatt található **csoportházirend-objektumok** (Group Policy Objects) mappában helyezkednek el. Azt, hogy melyik csoportházirend-objektum melyik AD-beli tároló objektumhoz (tartományhoz, szervezeti egységhez vagy telephelyhez) van hozzárendelve, a kérdéses tárolókban elhelyezett csoportházirend-objektumhoz kapcsolódó hivatkozások mutatják meg. Egy új csoportházirend-objektum létrehozásánál tehát erre is oda kell figyelni.

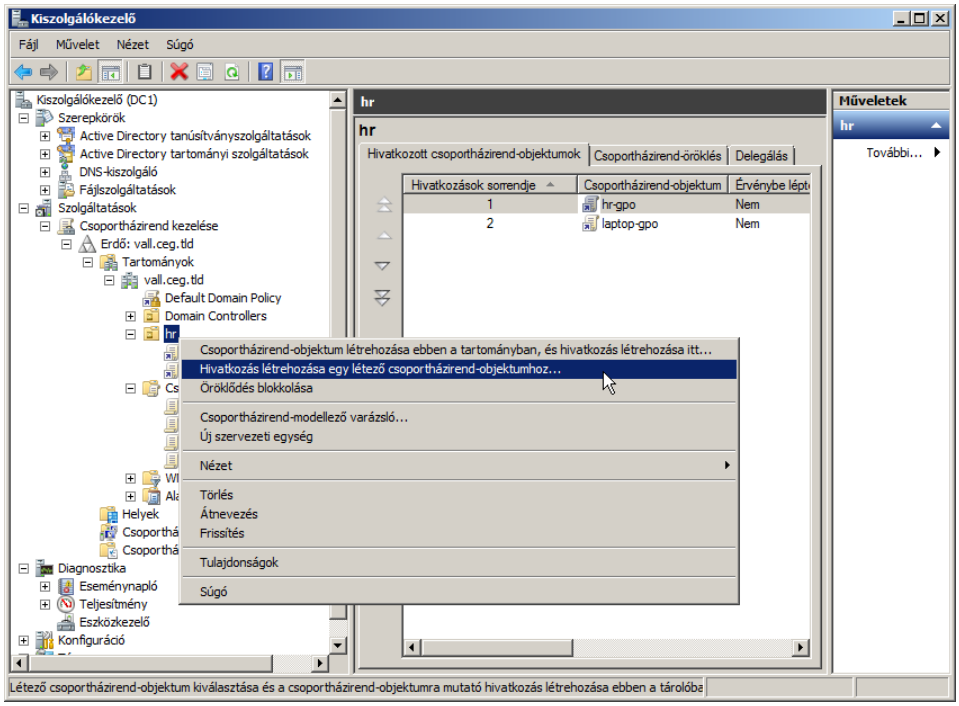


102. ábra: Csoportházirend kezelés a kiszolgálókezelőben

Csoportházirend-objektum és hivatkozásának létrehozása és törlése

Új csoportházirend-objektumot a **hely** (Site – telephely), tartomány (Domain) vagy **szervezeti egység** (Organizational Unit - OU) nevére jobb gombbal kattintva és a helyi menüben megjelenő **csoportházirend-objektum létrehozása ebben a tartományban, és hivatkozás létrehozása itt** (Create a GPO in this domain, and Link it here) menüpontra kattintva lehet létrehozni. Az **új csoportházirend-objektum** (New GPO) ablakban az új házirendobjektum **nevét** (Name) megadva és az **OK** gombra kattintva az új csoportházirend-objektum létrejön a **csoportházirend-objektumok** mappában. Ilyen esetben a csoportházirend-objektum létrehozásakor a kérdéses tárolóban (ebben az esetben szervezeti egységben) automatikusan létrejön az új csoportházirend-objektumra mutató hivatkozás is.

A beállítások szabályozásának módosításához az objektum nevére jobb gombbal kattintva, és a helyi menüből a **szerkesztés** (Edit) menüpontot kell választani. A menüpont kiválasztását követően a megjelenő **csoportházirend-objektum szerkesztő** (GPO Editor) felügyeleti konzol segítségével kell a beállításokat szerkeszteni.



103. ábra: Hivatkozás létrehozása egy létező csoportházirendhez a HR szervezeti egységen

Előfordulhat, hogy létező csoportházirend-objektumot kéne egy pl. szervezeti egységhez rendelni. Ilyen esetben a szervezeti egység (vagy más speciális tároló) nevére jobb gombbal kattintva a megjelenő helyi menü **hivatkozás létrehozása egy létező csoportházirend-objektumhoz** (Link an Existing GPO) menüpontot kell választani, majd a megnyíló ablakban meg kell adni, hogy melyik házirendobjektumot kell a szervezeti egységhez rendelni.

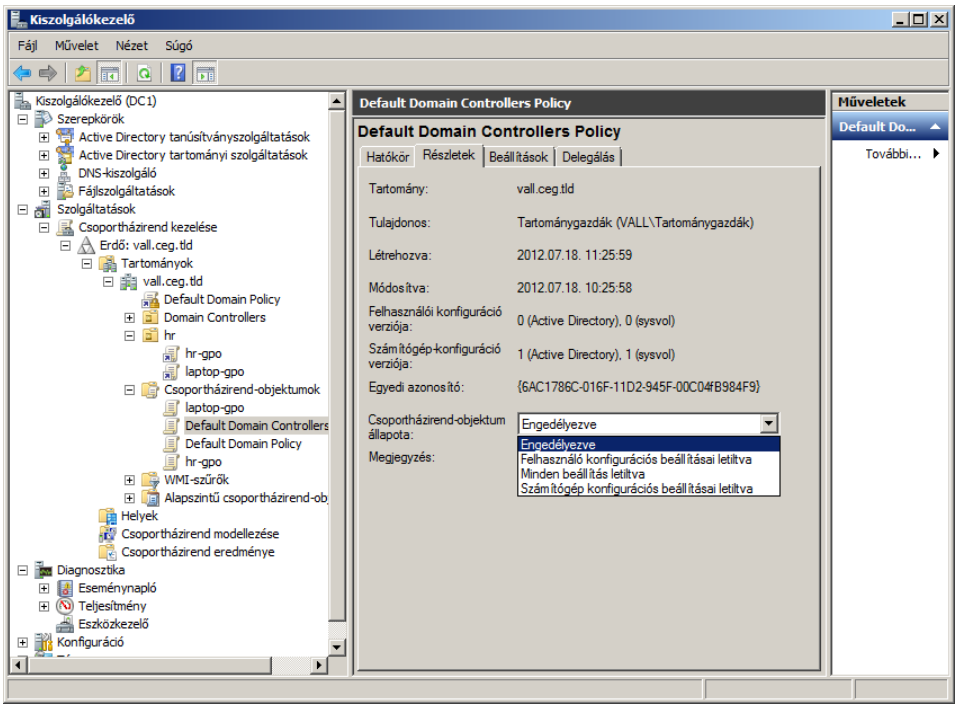
Ha már nincs igény egy csoportházirendre egy adott szervezeti egységben, akkor el kell dönteni, hogy magát a csoportházirend-objektumot, vagy csak a rámutató hivatkozást kell törölni, hiszen pl. az adott csoportházirend esetleg több szervezet egységhez is tartozhat, és így törlése esetén a többi szervezeti egységben alkalmazott szabályozás is elveszhet. Ezért célszerű mindig először a hivatkozást törölni, majd ha az objektum már semmihez sincs hozzárendelve, akkor abban az esetben, ha már biztosan nem lesz többet szükség rá, törölhető.

A hivatkozás törléséhez a hivatkozásra jobb gombbal kattintva, a megjelenő helyi menüből a **törlés** (Delete) menüpontot kell kiválasztani. A hivatkozás törléséhez hasonlóan alakul az objektum törlése is, de ilyenkor a csoportházirend-objektumok mappában kell a kérdéses objektumra jobb gombbal kattin-

tani, majd a megjelenő helyi menüből a **törlés** (Delete) menüpontot választani. Ha az objektumhoz léteztek a tartományban hivatkozások, akkor más tartományok hivatkozásaival ellentétben azok is törlődni fognak.

Több csoportházirend-objektum együttes alkalmazása

Több csoportházirend-objektum együttes alkalmazása esetén gyakran előfordul, hogy a hierarchiában különböző szinteken található csoportházirend-objektumok egyik, vagy másik részét nem szükséges alkalmazni, mert az egy másik szinten lesz majd szabályozva. Ilyenkor gyakori, hogy olyan csoportházirend-objektumok jönnek létre, amelyeknek vagy a számítógépre, vagy a felhasználóra vonatkozó része nem szabályozott. Ebben az esetben célszerű a nem szabályozott részeket letiltani. Olyan is előfordulhat, hogy ideiglenesen ki kell kapcsolni egy adott tárolóra vonatkozó csoportházirendet a hivatkozás, vagy az objektum eltávolítása nélkül. Ilyen esetben akár az egész csoportházirend-objektum is letiltható.



104. ábra: Az együttes alkalmazás esetén ilyen szabályozások érhetők el

A csoportházirend szóban forgó részének letiltásához ki kell jelölni a kérdéses csoportházirend-objektumot, vagy annak bármelyik hivatkozását, majd a jobb oldalon a **részletek** (Details) fülre kattintva a **csoportházirend-objektum**

állapota (GPO Status) legördülő listából ki kell választani a megfelelő elemet. A lista elemei a következők:

- **Engedélyezve** (Enabled): ilyenkor az egész csoportházirend érvényben van.
- **Felhasználó konfigurációs beállításai letiltva** (User configuration settings disabled): ebben az esetben csak a felhasználóra vonatkozó beállítások szabályozása kerül letiltásra.
- **Számítógép konfigurációs beállításai letiltva** (Computer configuration settings disabled): ezzel a beállítással csak a számítógépre vonatkozó beállítások szabályozása lesz tiltva.
- **Minden beállítás letiltva** (All settings disabled): ha ez egész csoportházirendet tiltani kell, akkor ezt az elemet kell kiválasztani.

Korábban már említésre került, hogy egy adott számítógépre vagy felhasználóra egyidejűleg akár több csoportházirend-objektum beállításai is hatással lehetnek, hiszen minden attól függ, hogy a tartományi hierarchiában hol helyezkedik el, illetve van-e csoportházirend-objektum rendelve a hierarchiát alkotó tárolókhoz. Arról is szó volt, hogy több csoportházirend-objektum együttes alkalmazása esetén addig nem lehet igazából semmilyen probléma, amíg a különböző házirendek beállításai nem „ütköznek” egymással, azaz ugyanazok a beállítások nem ellentétes hatásúak. Ha ez nem így van, akkor a csoportházirend-objektumok beállításainak együttes hatásai, azaz a házirendek eredője a következő szabályok mentén alakulnak:

Csoportházirend-objektumok öröklődése: a csoportházirend-objektumok hatása a hierarchiában felülről lefelé terjed, azaz a magasabb szintű tárolóhoz rendelt csoportházirend-objektum hatása érvényes lesz az alatta lévő tárolókra is.

A hierarchiában közelebb eső házirend az erősebb: a hierarchiában az adott számítógép vagy felhasználó objektum szintjéhez közelebb eső tárolóhoz rendelt csoportházirend-objektum beállításai felülbírálják a magasabb szinteken található tárolókhoz rendelt házirendekét.

Rendszergazda által beállított prioritás: adott tárolóhoz több csoportházirend-objektum is rendelhető. Hogy ilyen esetben melyik házirendnek lesz nagyobb prioritása a többi felülbírálásához, csak a rendszergazda beállításain múlik.

Öröklés blokkolása: a hierachiában egy adott tárolótól lefelé letiltható az öröklött csoportházirend-objektumok hatásai. Fontos, hogy az adott tárolóra (és annak tartalmára) vonatkozó összes öröklött házirendre történik a blokkolás.

Öröklődés kikényszerítése: egy adott tárolón történő öröklés blokkolás minden öröklött házirendre vonatkozik, ezért ilyen esetekben a központi menedzsment által megadott házirend beállítások megkerülhetőek lennének. Az öröklődés kikényszerítése segítségével ez a helyzet megoldható, hiszen hiába lesz tiltva az adott tárolóra az összes csoportházirend között pl. egy központi csoportházirend is, ha ez utóbbinál be van állítva az öröklődés kikényszerítése, akkor az mindenféleképpen érvényre fog jutni.[52]

A csoportházirend érvényre jutásámak folyamata

A számítógép elindulása után a hozzá legközelebbi tartományvezérlőről letölti a rá vonatkozó (helyi, tartományi ill. szervezeti egységhez tartozó) csoportházirend-objektumokat.

A csoportházirend-objektumok letöltése után, az esetleges felülbírálati szabályok alkalmazásával kiszámításra kerül a számítógépre vonatkozó egyesített csoportházirend. A számítógépen érvényre jutnak a számítógépszintű beállítások. Ezt követően a felhasználó beléphet a számítógépre.

A felhasználó bejelentkezésekor a tartományvezérlőről a felhasználóra vonatkozó (helyi, tartományi ill. szervezeti egységhez tartozó) csoportházirend-objektumokat. Ezek az objektumok akár teljesen más objektumok is lehetnek, mint a számítógép indulásakor érvényre jutottak.

Kiszámításra kerül a felhasználóra vonatkozó egyesített csoportházirend, melyet a számítógép érvényre juttat, majd megjeleníti a felhasználó munkakörnyezetét (Asztal – Desktop).

A számítógép működése során a Windows másfél óránként megvizsgálja, hogy történt-e változás a csoportházirendben (mind a számítógép, mind a felhasználói rész esetén). Ha igen, akkor érvényesíti az új beállításokat.[53]

- Az automatikus frissítés alól kivételt képeznek a felhasználói mappák áthelyezésére és a programtelepítésre vonatkozó beállítások. Ezek változásai csak a számítógép indulásakor, illetve a felhasználó bejelentkezésekor jutnak érvényre.

A csoportházirend beállítások nagyrészt a Windows beállításjegyzékében (Registry) helyezkednek el. Abban az esetben, amikor egy számítógépen egy csoportházirend érvényre jut, a beállításjegyzék megfelelő bejegyzései ideiglenesen (pl. a felhasználó bejelentkezésének idejére) megváltoznak. (A felhasználó kijelentkezése után a beállítások visszaállnak az eredeti értékekre.)

[52] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

[53] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

A csoportházirendek automatikus érvényre juttatását kézzel is el lehet végezni a **gpupdate.exe** program futtatásával, pl. a Start menü **futtatás** (Run) menüpontjából indítva.

- Az új csoportházirend beállításokat érdemes az éles alakalmazás előtt kipróbálni. Ehhez érdemes teszt szervezeti egységeket létrehozni és szintén teszt felhasználókkal és teszt számítógép fiókokkal, majd ezeket a teszt számítógépeket indítva és rajtuk a tesztfelhasználókkal bejelentkezve kipróbálni a beállított csoportházirend szabályozásokat.

A csoportházirend-objektumok együttes hatásainak módosítása

A csoportházirend-objektumok együttes hatásának, eredőjének alapértelmezett módon történő kiszámítását több helyen lehet módosítani. A módszerek a már említett öröklés blokkolás, öröklés kikényszerítés, illetve prioritás konfiguráció, amelyeknek beállítása természetesen a **csoportházirend kezelése** (Group Policy Management) felügyeleti konzolon keresztül valósítható meg.

Egy adott tárolóra és tartalmára vonatkozó csoportházirend öröklődés blokkolása a tárolóra való jobb gombbal történő kattintás után a helyi menüből az **öröklődés blokkolása** (Block Inheritance) menüpontot kiválasztva történik.

Az öröklés kikényszerítésnél arra kell figyelni, hogy az nem az előző példában leírt módon a tárolóra, hanem a csoportházirend-objektumnak az adott tartományon vagy szervezeti egységen belüli érvényességére vonatkozik. Ezért beállításhoz a csoportházirend-objektumra mutató hivatkozáson kell jobb gombbal kattintani, majd a megjelenő helyi menüből az **érvénybe léptetve** (Enforced) lehetőséget kell választani.

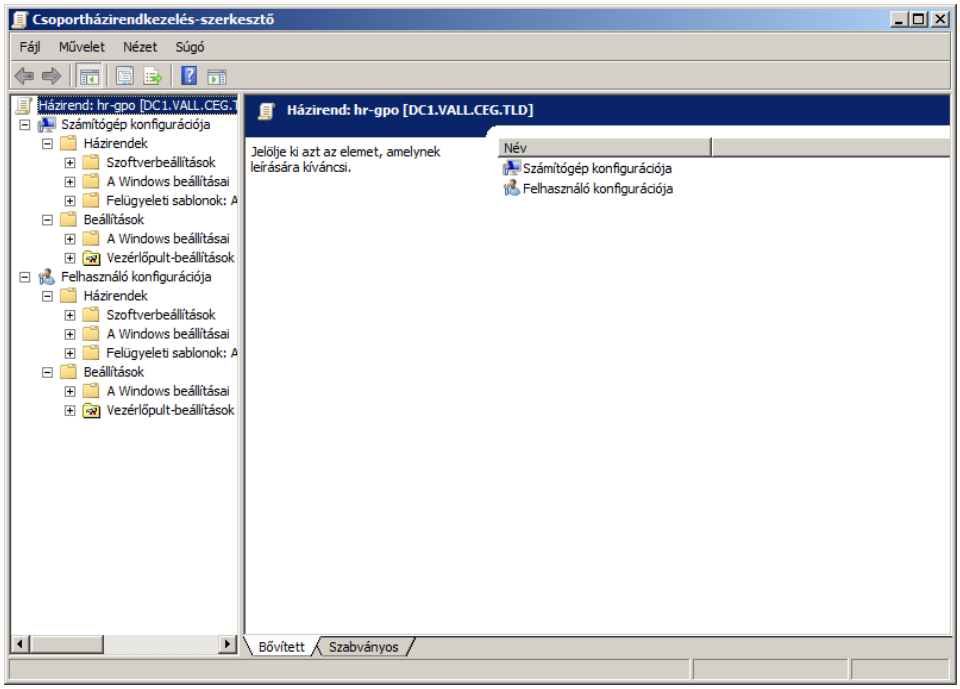
Abban az esetben pedig, amikor egy tárolóra több csoportházirend-objektum is vonatkozik, akkor a rendszergazda által beállítandó prioritást az adott tároló kijelölése után, a jobb oldalon, a **hivatkozott csoportházirend-objektumok** (Linked Group Policy Objects) lap bal szélén található nyilakkal lehet beállítani. A listából kijelölt csoportházirend-objektumot a felfelé mutató nyilakkal felfelé, a lefele mutatókkal lefelé lehet mozgatni. A prioritást a **hivatkozások sorrendje** (Link Order) mutatja meg. Minél előrébb szerepel a listában a kérdéses csoportházirend-objektum, annál nagyobb lesz a kiértékelésben a prioritása. A listában legelső csoportházirend-objektum minden beállítása felülbírálja a listában utána következő csoportházirend-objektum azonos, ám különböző értékű beállításait.

*Legyen a **vall.ceg.tld** tartományban egy **hr** és egy **finance** szervezeti egység, a **finance** szervezeti egységen belül pedig legyen egy **accounting** szervezeti egység. Legyen továbbá a **vall.ceg.tld** tartományban*

négy csoportházirend-objektum, melyek rendre hr_gpo, finance_gpo, accounting_gpo és laptop_gpo. A nevesített csoportházirend-objektumokat a megfelelő szervezeti egységhez rendelve szabályozzák a szervezeti egységekben található számítógép és felhasználó objhektumokat. A laptop_gpo házirendet az accounting szervezeti egységhez rendelve az accountig szervezeti egységre már négy csoportházirend-objektum lesz hatással. A négy házirend közül kettő öröklött (alapértelmezett tartományi csoportházirend és finance_gpo), kettő pedig közvetlenül a szervezeti egységhez rendelt házirend (accounting_gpo és laptop_gpo). Ha a négy házirendben azonos beállításokra vonatkoznak a szabályozások, de a beállítások eltérő értékekkel szerepelnek, akkor az egyesített csoportházirend szerint a hierarchiában a legközelebb szervezeti egységhez rendelt csoportházirend-objektum fogja felülbírálni a többit. Ebben az esetben azonban két házirend is létezik ezen a szinten a hierarchiában, azaz közöttük a rendszergazda által beállított prioritás fog dönteni. Ez alapértelmezetten a csoportházirend-objektum hivatkozások létrehozásának sorrendje. Azaz az előbb létrehozott csoportházirend-objektum (ebben az esetben accounting_gpo) szerepel feljebb a listában, annak nagyobb a prioritása. Ha a finance_gpo olyan beállításokat is tartalmaz, amely nem lenne jó ha az accounting szervezeti egységben lévőkre is hatással lenne, akkor célszerű lehet az accounting szervezeti egységen blokkolni az öröklődést. Mivel a központi menedzsment valószínűleg ragaszkodni fog az alapértelmezett tartományi csoportházirend beállításaihoz, ezért ennek a házirendnek a tartományra vonatkozó hivatkozásán be fogják állítani az öröklődés kikényszerítését.

7.2.10 A csoportházirend-objektumok szerkesztése

A csoportházirend-objektumok rengetegféle beállítást tartalmazhatnak, amelyeknek részletes ismertetése meghaladná a tankönyv kereteit, így itt csak a főbb beállításcsoportok kerülnek bemutatásra, és azok is az **alapértelmezett tartományi házirenden** (Default Domain Policy) keresztül. A csoportházirend-objektumok beállításainak szerkesztése a már korábban említett módon a **csoportházirend kezelése** (Group Policy Management) felügyeleti konzolon keresztül történik. A csoportházirend-objektum beállításainak szerkesztéséhez a csoportházirend-objektumra vagy annak hivatkozására kell jobb gombbal kattintani, majd a megjelenő menüből a **szerkesztés** (Edit) lehetőséget kell kiválasztani. Az elinduló csoportházirendkezelés-szerkesztő (Group Policy Object Editor) konzolban megjelenik a csoportházirend-objektum tartalma.



105. ábra: A csoportházirendkezelés-szerkesztő

A csoportházirend-objektumok részei

Minden csoportházirend-objektum alapvetően két részre osztható. Az egyik a számítógépre vonatkozó, ún. számítógép szintű, másik a felhasználóra vonatkozó, ún. felhasználói szintű rész. Ezek az alapvető részek további alrészekre bomlanak, amelyek a következők:

Beállítások (Preferences): olyan felhasználói felülettel kapcsolatos, de nem feltétlenül a beállításjegyzéket módosító opció, mint a hardvereszközök, nyomtatók telepítése, mappák és beállításjegyzékbeli beállítások létrehozása, vagy a fájlok másolása és helyi felhasználók és csoportok létrehozása.

Házirendek (Policies): hagyományos csoportházirend beállítások, melyek további három részre oszthatók:

Szoftverbeállítások (Software Settings): mind a számítógép szintű, mind a felhasználó szintű rész esetében a programtelepítés előírására használatos. A beállítási lehetőségek eltérhetnek attól függően, hogy a programtelepítés a számítógéphez vagy a felhasználóhoz van kapcsolva.

Windows beállításai (Windows Settings): a számítógép szintű és a felhasználói szintű beállítási lehetőségek eltérése itt már jóval jelentősebb. Előbbinél

előírhatók az indítási és leállítási parancsfájlok valamint a számítógépre vonatkozó biztonsági beállítások, utóbbinál beállíthatók többek között a felhasználói mappák áthelyezése, az Internet Explorer böngésző működése, illetve néhány felhasználói szintű biztonsági beállítás, mint pl. a felhasználói tanúsítványok.

Felügyeleti sablonok (Administrative Templates): a beállításjegyzékben érvényre jutó beállítások, melyek közül a számítógép szintűek a HKEY_LOCAL_MACHINE, a felhasználói szintűek a HKEY_CURRENT_USER részben jelennek meg.

- A Windows számítógépeken alapból van helyi biztonsági házirend, amelynek egészen addig nincs köze a csoportházirendhez, míg a számítógép nem csatlakozik egy tartományhoz. Amikor a csoportházirend tartományi környezetben érvényre jut, beállításai valójában az egyes számítógépek helyi házirendjébe íródnak be.

7.2.11 A csoportházirend kezelése felügyeleti konzol

Több tartományos, telephelyes, komolyabb rendszer konfigurálása is történhet a felügyeleti konzolon keresztül. Ehhez csak a megfelelő tárolókban kell a csoportházirend-objektumokat szerkeszteni, kezelni. Ezek a tárolók a következők:

Tartományok (Domains): a tartományokhoz és a szervezeti egységekhez rendelt csoportházirend-objektum hivatkozások jelennek meg a struktúrában. Kezdetben itt (minden tartomány gyökerében) található az alapértelmezett tartományi házirendre (Default Domain Policy) mutató hivatkozás is.

Csoportházirend-objektumok (Group Policy Objects): ez a tároló minden tartomány alatt megtalálható és benne az adott tartományban érvényes csoportházirend-objektum helyezkedik el.

WMI-szűrők (WMI Filters): az előző tárolóhoz hasonlóan ez is megtalálható minden tartomány alatt. Itt a számítógépek jellemzőire vonatkozó szűrők és lekérdezési parancsfájlok találhatók, melyek segítségével a számítógépek különböző paraméterei kérhetők le a Windows WMI felületén keresztül.

Helyek (Sites): a létrehozott telephelyek és a hozzájuk rendelt csoportházirendek találhatók meg ebben a tárolóban.

Csoportházirend modellezése (Group Policy Modeling): az eredő házirend modell megjelenítése különböző számítógépekre és felhasználókra húzva szimulálja az esetleges beállítások hatásait.

Csoportházirend eredménye (Group Policy Results): az együttes vagy eredő házirend kiszámítása adott számítógépre illetve felhasználóra, szervezeti egységre vagy biztonsági csoportra.[54]

7.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

7.3.1 Összefoglalás

A tanúsítványok használata manapság megkerülhetetlen. Egy modern rendszerben használatuk nélkülözhetetlen. A zökkenőmentes használat előirányozza egy publikus kulcsokon alapuló infrastruktúra (PKI Infrastruktúra) felállítását a helyi hálózatban. A tananyagban tárgyalásra kerültek a PKI elemei, illetve a hozzá kapcsolódó olyan fogalmak, mint a tanúsítvány, a hitelesítésszolgáltató, a digitális aláírás vagy a tanúsítvány visszavonási lista.

A hitelesítésszolgáltató telepítésénél, ha a hálózatban van AD, akkor mindig a vállalat típusú kiszolgálót kell telepíteni, méghozzá legfelsőszintű, vagy gyökér hitelesítésszolgáltatóként, legalábbis akkor, ha ez az első vagy egyetlen hitelesítésszolgáltató a hálózatban.

A tanúsítványsablonok szerkesztésével és duplikációjával nagyon meg lehet könnyíteni a későbbi tanúsítványigényléseket, melyek ezek után nagyon egyszerűen, pár lépésben elérhetővé válnak.

A csoportházirend szolgáltatás az egyik legnagyobb címtárszolgáltatás, amióta az AD létezik. A csoportházirend segítségével szabályozható a felhasználói környezet, felhasználói jogokat és korlátozásokat lehet a felhasználóknak adni. Ugyanígy lehet a tartomány számítógépeinek beállításait központosítottan vezérelni.

A csoportházirendek az ún. csoportházirend objektumokban tárolódnak, melyek egy része az AD-ban, másik része a Sysvol mappában tárolódik. A replikációról az elosztott fájlrendszer replikáció (DFSR) szolgáltatás gondoskodik.

A csoportházirend-objektumokat telephelyhez, tartományhoz vagy szervezeti egységhez lehet hozzárendelni. Alapértelmezetten a felhasználókra az alapértelmezett tartományi házirend lesz érvényes, hacsak nem egy új szervezeti egységben lesznek létrehozva, amelyhez hozzá van rendelve egy másik házirend. Ilyenkor a házirendek eredője lesz a végeredmény. A házirendek eredőjének kiszámításánál a rendszer a következő jellemzőket veszi figyelembe: csoportházirend-objektumok öröklődése, a hierarchiában közelebb eső házi-

[54] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

rend az erősebb, rendszergazda által beállított prioritás, öröklés blokkolása, öröklődés kikényszerítése.

A csoportházirend érvényrejutásának folyamata során a csoportházirend számítógép és felhasználó része külön-külön jut érvényre. A számítógép rész az operációs rendszer betöltődése után, míg a felhasználói rész a felhasználó bejelentkezése után.

A csoportházirendek szerkesztésénél szintén két különböző ágban lehet szerkeszteni a beállításokat, a főbb csoportok azonban ugyanazok mind a felhasználói rész, mind a számítógép rész esetén. Ezek pedig rendre: beállítások, házirendek, szoftverbeállítások, Windows beállításai, felügyeleti sablonok.

7.3.2 Önellenőrző kérdések

1. Mi a tanúsítvány és mire jó? Hozzon rá 3-4 példát!
2. Mit jelent a PKI?
3. Mire kell odafigyelni a tanúsítványsablonok szerkesztésénél?
4. Hogyan lehet kiszolgálótanúsítványt igényelni?
5. Mire jó a csoportházirend szolgáltatás?
6. Hol tárolódnak a csoportházirend objektumok?
7. Mi a szerepe a szervezeti egységeknek a csoportházirendek esetén?
8. Milyen szabályok vonatkoznak a csoportházirend-objektumok együttes alkalmazásánál, az egyesített házirend kiszámolására?
9. Ismertesse a csoportházirend érvényrejutási folyamatát!
10. Milyen műveletek végezhetőek el egy csoportházirend-objektummal?
11. Sorolja fel a csoportházirend-objektumok beállításainak főbb kategóriáit!

8 HOZZÁFÉRÉS-VEZÉRLÉS ÉS BIZTONSÁG

8.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A leckében a hozzáférés-vezérlés alapismereteinek ismertetése után a rendszer által történő hitelesítés formái kerülnek felsorolásra. Tárgyalásra kerülnek azok az erőforrások, melyekhez hozzáférési engedélyeket lehet rendelni Windows tartományi környezetben.

Az ACL és ACE fogalmak magyarázata után az NTFS fájl és mappaengedélyeinek ismertetése következik. Itt mind a szokásos, mind a speciális engedélyek ismertetésre kerülnek. Tárgyalásra kerül erőforrások tulajdonosa és tulajdonjoga, valamint az utóbbi átvételének engedélye. Ismertetésre kerül az engedélyek öröklésének szabályai, valamint az engedélyek hozzárendelése kapcsán a csoportok szerepe.

A továbbiakban kiderül, hogy a többféle forrásból származó engedélyek együttes hatása eredményezi a hatályos, vagy érvényes engedélyeket, amelyek bizonyos szabályok mentén számítódnak ki. Ismertetésre kerülnek továbbá a mappa és nyomtató megosztások engedélyei és működésük.

A tananyag elsajátítása után a hallgató képes lesz a megfelelő objektum engedélyek beállítására, a hozzáférés megtagadásból származó hibák felderítésére és javítására. Képes lesz hálózaton keresztül nyomatót és mappát megosztani.

8.2 TANANYAG

8.2.1 Az erőforrásokhoz való hozzáférés

A tananyagban többször is említésre került már az erőforrásokhoz való hozzáférés és annak valamilyen szabályozása. A legfontosabb erőforrásokat a lemezeken tárolt fájlok jelentik, amelyekhez az operációs rendszernek kell biztosítani a hozzáférést valamilyen módon. Az erőforrásokhoz való hozzáférés szabályozása a több felhasználós rendszerekkel együtt jelent meg, így jelentős múltra tekint vissza. A Microsoft operációs rendszereiben többek között ez a szolgáltatás is a Windows NT operációs rendszerrel és NTFS fájlrendszerrel együtt jelent meg.

Manapság egy többfelhasználós, hálózati környezetben működő számítógép egyik legfontosabb feladata, hogy a felhasználók szabályozott módon férhessenek hozzá a különböző számítógépes erőforrásokhoz. Ilyen erőforrások a már említett fájlok, mappák, de ilyenek pl. a nyomtatók illetve az AD különböző objektumai.

A hozzáférés megfelelő szabályozásához az operációs rendszernek az erőforrásokról valamilyen nyilvántartást kell vezetnie. A nyilvántartásnak tartalmaznia kell a felhasználókat és csoportokat, az erőforrásokat, illetve a hozzáférési engedélyeket. Ennek a nyilvántartásnak a megfelelő vezetése és karbantartása a hozzáférés vezérlés alapja.

8.2.2 A hozzáférés szabályozás alapjai

Ahhoz hogy a felhasználók az általuk igényelt erőforrást elérjék első lépésben valamilyen úton-módon jogot kell szerezniük a rendszer a használathoz. Ha ez meglenne, akkor következő lépésként a felhasználónak a kért erőforráshoz való viszonya a kérdéses. Ha van engedélye elérni az erőforrást, akkor hozzáférhet, ha nincs akkor nem.

Az első lépés tulajdonképpen a felhasználónak a rendszerbe történő belépését, a hitelesítést (idegen szóval autentikáció) jelenti. Ez egy Windows által kezelt erőforráshoz való hozzáférés esetében a következő háromféle lehet:

Bejelentkezés helyben: az erőforrást tartalmazó számítógépen interaktívan történik a bejelentkezés. A felhasználói azonosító adatok a számítógép saját felhasználói adtabázisában találhatók.

Bejelentkezés hálózaton keresztül: a felhasználó nem a helyi, hanem egy távolihoz számítógép erőforrásaihoz akar hozzáférni. Ehhez a hálózaton keresztül kell hitelesítenie magát a távoli számítógépen az ottani felhasználói adatbázisban szereplő felhasználói adatok alapján. Ilyenkor gyakran előfordul, hogy a felhasználó nem ugyanazzal a felhasználói név-jelszó párossal azonosítja magát a távoli számítógépen, mint a helyin. A fő probléma viszont az, hogy a távoli számítógép nem fogadja el hitelesnek a helyi bejelentkezést, ezért kéri a hálózaton keresztüli hitelesítést.

Tartományi bejelentkezés: a Windows Serverek által támogatott és preferált tartományi modellben a hálózat számítógépei és felhasználói nem helyi adatbázisokban vannak nyilvántartva, hanem a központi címtáradatbázisban és hitelesítésük is innen történik. A tartományba szervezett számítógépek és felhasználók a tartományvezérlő kiszolgálón keresztül azonosítják magukat, amelyet a tartomány többi szereplője (számítógép és felhasználó egyaránt) hitelesnek fogad el. Így a tartományba bejelentkezett felhasználó elviekben a tarto-

mányban található összes erőforrást elérheti anélkül, hogy szükséges lenne az erőforrásokat tartalmazó számítógépeken, azonosítania magát.[55]

A különböző erőforrásokhoz való hozzáféréshez a fent említett hitelesítések szükségesek, ámde közel sem elegendőek. Mivel többfelhasználós rendszerekről van szó, az erőforrásokat is több felhasználó között kell megosztani. A megosztott erőforrásokhoz való hozzáférés viszont valamilyen szabályozást kíván, hiszen ha minden felhasználó azt csinálhat az erőforrásokkal, amit csak akar, az előbb utóbb adatvesztéshez vezet, és végső soron felbecsülhetetlen károkat tud okozni. A szabályozás a hozzáférési jogosultságok, Microsoft terminológiával engedélyek (Permissions) segítségével történik. Ezt úgy kell elképzelni, hogy minden erőforráshoz hozzá van rendelve, hogy melyik felhasználó (csoport), milyen műveletet végezhet az adott erőforrással, azaz milyen műveletre van engedélye.

Nem minden erőforráshoz lehet hozzáférési engedélyeket rendelni. Nagyban függ az operációs rendszertől és attól, hogy melyik erőforrást miként kezeli. Ha az operációs rendszer egy adott erőforráshoz nem tud engedélyeket rendelni, mert pl. az engedélyek már nem férnek el az erőforrás tárolásának adatstruktúrájába, akkor az erőforráshoz nem rendelhetők engedélyek. A Windows operációs rendszer esetén pl. ilyen erőforrások a régi FAT (FAT32) fájlrendszerben tárolt fájlok és mappák.

A fájlrendszer történelmi okok miatt (a DOS operációs rendszer, amelyhez kifejlesztették, még csak egyfelhasználós rendszer volt) a fájl tárolásának megoldásánál nem „hagyott helyet” további adatok, pl. hozzáférési engedélyek tárolására. Így a FAT fájlrendszer már nem tudott érdemben megújulni, és bizonyos funkciókkal kapcsolatban leváltásra került (pl. rendszerlemez nem lehet FAT). Azóta a FAT fájlrendszert inkább csak cserélhető adathordozókon használjak (pendrive, memória kártya stb.). Ilyen erőforrások esetén a hozzáférés vezérlés két lépése közül csupán az első létezik, így az a felhasználó, aki tudja magát azonosítani a rendszerben, azaz be tud lépni, az korlátlanul hozzáférhet az ilyen típusú erőforráshoz.[56]

A Windows Server 2008 által kezelt, hozzáférési engedélyekkel ellátható erőforrások a következők:

- a NTFS fájlrendszerben tárolt fájlok és mappák
- a hálózati mappa és fájlmegosztások
- a beállításjegyzék (Registry) bejegyzései

[55] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

[56] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

- a címtáradatbázis objektumai
- a rendszerszolgáltatások

8.2.3 A hozzáférési engedélyek

Az erőforrásokat és felhasználókat összekötő hozzáférési engedélyek az erőforrás tárolásának adatstruktúrájában egy ún. hozzáférés vezérlési listában (Access Control List – ACL) vannak felsorolva. A lista több elemből áll, mely elemeket **hozzáférés vezérlő bejegyzéseknek** (Access Control Entry – ACE) neveznek, és három részből tevődnek össze. Ezek rendre:

- a felhasználó, vagy csoport biztonsági azonosítója (Security Identifier – SID)
- a hozzáférési engedélyek (Permissons), azaz hogy milyen műveleteket szabályoz az elem az azonosítóval rendelkező felhasználó vagy csoport számára az adott erőforráson (ez erőforrás típusonként eltérhet).
- maga a szabályozás, azaz hogy a fentebb említett műveleteket engedélyezi-e vagy tiltja a listaelem.

A hozzáférési engedélyek, azaz a szabályozható műveletek erőforrás típusonként változhatnak. Elsőként a fájl és mappa engedélyek, majd ezeken keresztül bemutatva a hozzáférési engedélyek tulajdonságai kerülnek ismertetésre.[57]

8.2.4 Fájl és mappa engedélyek

A fájl és mappa engedélyek szorosan kötődnek a Windows fájlrendszeréhez, az NTFS fájlrendszerhez. Az engedélyek ACL-ek segítségével vannak az egyes fájlokhoz és mappákhoz kapcsolva. A Windows a következő szokásos engedélyeket, vagy engedélyszinteket különbözteti meg fájlok és mappák esetén.

Olvasás (Read): ezen a szinten a felhasználók megtekinthetik az adott mappa tartalmát és megnyithatják a fájlokat és a mappákat.

Olvasás és végrehajtás (Read & Execute): itt a felhasználók megtekinthetik a meglévő fájlok és mappák tartalmát, és futtathatják a mappában található programokat.

[57] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

Mappa tartalmának listázása (List Folder Contents): ez a szint gyakorlatilag ugyanaz, mint az előző szint mappákra vonatkozó része. (Ez csak mappák esetén öröklődik.)

Módosítás (Modify): a módosítás engedélyszinten a felhasználók módosíthatják a meglévő fájlokat és mappákat, de újakat nem hozhatnak létre.

Írás (Write): ezen a szinten a felhasználók létrehozhatnak új fájlokat és mappákat hozhatnak létre, és módosíthatják a meglévő fájlokat és mappákat.

Teljes hozzáférés (Full Control): A felhasználók megtekinthetik az adott fájl vagy mappa tartalmát, módosíthatják a meglévő fájlokat vagy mappákat, új fájlokat vagy mappákat hozhatnak létre, és programokat futtathatnak a mappából.[58]

- Parancsfájlok, szkriptek (Script) futtatásához nem szükséges végrehajtási engedély, elég az olvasási.
  Parancsikonok és a parancsikonok céljának eléréséhez mind kettőhöz olvasási engedély szükséges.
  Ha egy felhasználónak van írási, de nincs törlési engedélye, attól még a a felhasználó az adott fájl tartalmát képes törölni.
  Ha egy felhasználónak teljes hozzáférés engedélye van egy mappához, akkor a fájlok engedélyeire való tekintet nélkül bármikor képes törölni a mappából azokat.[59]

Ezek az engedélyek több speciális, alapvető engedélyből állnak össze. Erre az egyszerűbb kezelhetőség miatt van szükség, hiszen a szokásos műveletek jogosultság szempontjából összetettek, de előfordulhat olyan speciális eset, amikor szükséges lehet az alapvető, speciális engedélyek egyenkénti finom szabályozása. A speciális engedélyek a következők:

Mappa bejárása, fájl végrehajtása (Traverse Folder, Execute File): mappák esetén a **mappa bejárása** engedély segítségével engedélyezhető vagy letiltható a mappák bejárása más fájlok vagy mappák elérése érdekében, még akkor is, ha a felhasználónak nincs engedélye a bejárt mappákhoz. Az engedélyt csak akkor alkalmazza a rendszer, ha a csoportházirend beépülő programban a csoport vagy a felhasználó nem rendelkezik **bejárás ellenőrzésének mellőzése** (Bypass traverse checking) felhasználói engedéllyel. (Alaphelyzetben a **mindenki** (Everyone) csoport **bejárás ellenőrzésének mellőzése** felhasználói engedéllyel rendelkezik.) Fájlok esetén a **fájl végrehajtása** engedély segítségével engedé-

[58] Windows Súgó

[59] William R. Stanek:File and Folder Permissions. Online cikk, Microsoft Corporation,1999 <http://technet.microsoft.com/en-us/library/bb727008.aspx>, 2012.09.25

lyezheti vagy megtagadhatja a programfájlok futtatását. A **mappa bejárása** engedélyt egy mappára beállítva, a rendszer nem állítja be automatikusan a **fájl végrehajtása** engedélyt a mappában levő összes fájlra.

Mappa listázása, adatok olvasása (List Folder, Read Data): mappák esetén a felhasználó engedélyezheti vagy megtagadhatja az adott mappában található almappák és fájlok nevének megtekintését. Az engedély csak az adott mappa tartalmára vonatkozik, magára a mappára már nem. Fájlok esetén az **adatok olvasása** engedély segítségével engedélyezhető vagy megtagadható a fájlok adatainak megtekintése.

Attribútumok olvasása (Read Attributes): lehetővé teszi vagy letiltja a fájlok vagy mappák attribútumainak, például az írásvédett vagy a rejtett attribútumnak a megjelenítését. Az attribútumokat az NTFS fájlrendszer határozza meg.

Kiterjesztett attribútumok olvasása (Read Extended Attributes): lehetővé teszi vagy letiltja egy fájl vagy mappa kiterjesztett attribútumainak megjelenítését. A kiterjesztett attribútumokat a programok definiálják és programonként különbözhetnek.

Fájlok létrehozása, adatok írása (Create Files, Write Data): mappák esetén a **fájlok létrehozása** engedély segítségével engedélyezhető vagy megtagadható fájlok létrehozása egy mappában. Fájlok esetében az **adatok írása** engedély segítségével engedélyezhető vagy megtagadható a fájlok módosítása és jelenlegi tartalmának felülírása.

Mappák létrehozása, adatok hozzáfűzése (Create Folders, Append Data): ez az engedély mappák esetében a mappák egy mappán belüli létrehozhatóságát, míg fájlok esetében a fájl végéhez való hozzáírás lehetőségét szabályozza. Utóbbi esetben ugyanakkor nem vonatkozik a fájlban levő adatok módosítására, törlésére vagy felülírására.

Attribútumok írása (Write Attributes): lehetővé teszi vagy letiltja a fájlok vagy mappák attribútumainak, például az írásvédett vagy a rejtett attribútumnak a módosítását. Fontos, hogy ezzel az engedéllyel nem hozhatók létre és nem is törölhetők fájlok és mappák, csupán azok attribútumai módosíthatók.

Kiterjesztett attribútumok írása (Write Extended Attributes): lehetővé teszi vagy letiltja egy fájl vagy mappa kiterjesztett attribútumainak a módosítását.

Almappák és fájlok törlése (Delete Subfolders and Files): ez az engedély csak mappákra vonatkozik és az almappák és a fájlok törlését szabályozza tekintet nélkül az almappák vagy fájlok törlési engedélyének megengedő vagy tiltó beállítására.

Törlés (Delete): lehetővé teszi vagy letiltja a fájl vagy a mappa törlését. Ha egy felhasználó nem rendelkezik törlés engedéllyel egy fájlhoz vagy mappához, de a szülőmappán van **almappák és fájlok törlése** engedélye, akkor törölheti a fájlt vagy a mappát.

Engedélyek olvasása (Read Permissions): lehetővé teszi vagy letiltja a fájlok vagy mappák engedélyeinek (például Teljes hozzáférés, Olvasás és Írás) olvasását.

Engedélyek módosítása (Change Permissions): segítségével engedélyezhető vagy letiltható a fájlok vagy mappák engedélyeinek módosítása.

Saját tulajdonba vétel (Take Ownership): lehetővé teszi vagy letiltja a fájl vagy a mappa saját tulajdonba vételét. A fájl vagy mappa tulajdonosa a fájlt vagy mappát védő meglévő engedélyektől függetlenül mindig módosíthatja annak engedélyeit.[60]

A következő táblázat az mutatja, hogy a szokásos engedélyek, vagy engedélyszintek, speciális engedélyek milyen kombinációjából állnak elő.

Speciális engedélyek	Teljes hozzáférés	Módosítás	Olvasás és végrehajtás	Mappa tartalmának listázása (csak mappák)	Olvasás	Írás
Mappa bejárása, fájl végrehajtása	x	x	x	x		
Mappa listázása, adatok olvasása	x	x	x	x	x	
Attribútumok olvasása	x	x	x	x	x	
Kiterjesztett attribútumok olvasása	x	x	x	x	x	
Fájlok létrehozása, adatok írása	x	x				x
Mappák létrehozása, adatok hozzáfűzése	x	x				x
Attribútumok írása	x	x				x

[60] Microsoft Corporation: Fájlok és mappák engedélyei. Online cikk, Microsoft Corporation, <http://technet.microsoft.com/hu-hu/library/cc787794(v=ws.10).aspx>, 2012.09.26

Speciális engedélyek	Teljes hozzáférés	Módosítás	Olvasás és végrehajtás	Mappa tartalmának listázása (csak mappák)	Olvasás	Írás
Kiterjesztett attribútumok írása	x	x				x
Almappák és fájlok törlése	x					
Törlés	x	x				
Engedélyek olvasása	x	x	x	x	x	x
Engedélyek módosítása	x					
Saját tulajdonba vétel	x					
Szinkronizálás	x	x	x	x	x	x

7.*NTFS jogosultságok és engedélyezett műveletek (forrás: Windows Súgó)*

A táblázatból jól látszik, hogy a **teljes hozzáférés** (Full Control) engedély nem más, mint az összes speciális engedély együtt alkalmazása. Ennek ellentéte az, amikor **nincs a hozzáférés szabályozva** (No Access), ilyenkor egyik speciális engedély sincs szabályozva. (Ezt implicit tiltásnak is nevezik.)

Az ACL elemei, az ACE-k a hozzáférési engedélyeken kívül magát a szabályozást is tárolják, amely szerint a hozzáférési engedély **engedélyezéséről** (Allow) vagy **tiltásáról** (Deny) van szó. Fontos szabály, hogy a közvetlenül meghatározott (explicit) engedélyezés és tiltás, mindig erősebb, mint az implicit tiltás, az explicit tiltás pedig mindig erősebb, mind az engedélyezés. Ez összefoglalva annyit jelenti, hogy ha egy felhasználóhoz és egy erőforráshoz nincs hozzáférési engedély rendelve, akkor a felhasználó nem tehet semmit az erőforrással. Amennyiben van hozzáférési engedély, és az engedélyező típusú, akkor a felhasználó a hozzáférési engedélyben meghatározott műveleteket elvégezheti az erőforrással. Ha azonban egy másik ACE-ben ugyanezen műveletek közvetlenül tiltva vannak, akkor a felhasználó a kérdéses műveleteket nem végezheti el az erőforráson.

A Windows telepítésekor alapértelmezetten több engedély is beállításra kerül. Ezek nélkül az engedélyek nélkül maga az operációs rendszer, és egyetlen program sem lenne feltelepíthető, és a különböző beállításokat sem lehetne eltárolni. Ezeket az engedélyeket bármikor felül lehet bírálni, ám ez nem minden esetben célszerű.

8.2.5 Az erőforrások tulajdonosa

A többfelhasználós rendszerekben az erőforrások többségének – így a fájloknak és mappáknak is – van egy fontos tulajdonságuk, miszerint létezik tulajdonosuk. Ez a Windows esetében is így van (kivételek ez alól a mappamegosztások), a különbség a többi rendszerhez képest inkább ennek a tulajdonjognak a kezelése.

A tulajdonos alapértelmezetten az erőforrást létrehozó felhasználó, amely a későbbiekben megváltoztatható. Fontos megjegyezni, hogy a tulajdonjoggal nem jár automatikusan a teljes hozzáférés az erőforráshoz, azonban az erőforráshoz való hozzáférés szabályozható, így a tulajdonos könnyedén adhat magának, de akár másnak is teljes hozzáférést. Miután a tulajdonos teljes hozzáférést adott egy felhasználónak az erőforráshoz, a teljes hozzáféréssel együtt a hozzáférés szabályozás „összetett" engedélye is a felhasználó birtokába kerül.

A tulajdonos a tulajdonjogot másnak nem adhatja át, ám az a felhasználó, aki pl. teljes hozzáféréssel rendelkezik egy erőforráson, az a **saját tulajdonba vétel** (Take Ownership) speciális engedélyen keresztül átveheti az erőforrás tulajdonjogát. A saját tulajdonba vétel jog alkalmazásának egy speciális esete azt a hatáskori problémát írja át, amely abból adódna, hogy egy teljes hozzáféréssel rendelkező felhasználó eltilthatja a rendszergazda felhasználót fájloktól, mappáktól, akár teljes lemezektől is. A Windows rendszer ezért engedélyezi, hogy a rendszergazda a saját tulajdonba vétel engedély birtoklása nélkül is saját tulajdonba vehessen erőforrásokat, megkerülve a rendszergazda kizárásának lehetőségét. Az, hogy a rendszergazdák minden erőforrást saját tulajdonba vehetnek, csak alapértelmezés. Ezt valójában egy csoportházirendben szabályozott jogosultság.

Itt kell még megjegyezni, hogy a fájlok és mappák tulajdonosát használja a rendszer a lemezkvóták esetében a felhasznált tárterület kiszámítására. Azaz, azoknak a fájloknak a méretét adja össze a rendszer, ahol a tulajdonos a kérdéses felhasználó. A lemezkvóták tipikus felhasználási területe a fájlkiszolgálókon a felhasználók által használt tárterület korlátozása. A kvóta alkalmazása esetén a felhasználók nem tudják elfoglalni az összes szabad lemezterületet, amely elég nagy gondot okozhat egy éles rendszer működésében.[61]

8.2.6 Az engedélyek öröklése

Amikor egy olyan erőforrás objektumhoz, amelynek léteznek gyermek objektumai, hozzárendelésre kerül egy hozzáférési engedély, akkor amennyiben

[61] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

az lehetséges, a gyermek objektumok öröklik a szülőnek adott engedélyeket. (Mappák és fájlok esetében a szülő mappa, gyermekei az almappák és a benne lévő fájlok.)

Az örökölt engedélyek azonos erősségűek a közvetlenül beállított, ún. explicit engedélyekkel. Ez azt jelenti, hogy ha egy felhasználó hozzáférését egy erőforráshoz explicit és a örökölt engedélyek is szabályozzák, akkor az mindig a bővebb szabályozást, a kiadott engedélyek összességét jelenti.

Az örökölt engedélyek módosítására mindig csak az öröklés forrásánál módosíthatók, az öröklés helyén soha. Egy objektum több helyről is örökölhet engedélyeket attól függően, hogy a felette álló objektumokra explicit módon be lettek-e állítva engedélyek, illetve hogy mennyire mélyen helyezkedik el az objektumhierarchiában (mappa struktúrában), mivel az örökölt engedélyek tovább öröklődnek.

Az örökölt engedélyek egy másik módosítási lehetősége az öröklés megszakítása. Ennek hátránya, hogy ilyenkor az összes öröklött hozzáférési engedély törlődik, bármelyik forrásból is származik az öröklés.

8.2.7 A csoportok szerepe

A hatodik fejezetben tárgyalt felhasználói csoportok előnyei leginkább az engedélyek kapcsán jönnek elő. Ezek az előnyök összefoglalva a következők:

Személycserék esetén óriási könnyebbség, hogy az új felhasználónak nem kell minden erőforráshoz a megfelelő engedélyeket beállítani, elég csak a megfelelő csoportokba kell felvenni és a csoporttagságokon keresztül megkapja az engedélyeket.

Az ACL-nek kevesebb eleme lesz, hiszen akár több száz felhasználói bejegyzés helyett csak egy-két csoport bejegyzése tárolódik el. Ez csökkenti az – amúgy fölöslegesen – elfoglalt lemezterületet. Az NTFS engedélyek közvetlenül a fájlrendszerben, a mappa és nyomtató megosztások, valamint beállításjegyzékbeli bejegyzések a beállításjegyzék fájlokban, a címtárobjektumok pedig a címtáradatbázis fájljaiban tárolódnak és foglalják a helyet a lemezen.

Ha az ACL kevesebb elemet tartalmaz, akkor gyorsabbá válik a hozzáférési engedélyek kiértékelése, amely gyorsabb működést eredményez.

8.2.8 A hatályos (érvényes) engedélyek

Az előzőekben már többször említésre került, hogy egy erőforráshoz egy felhasználó többféleképpen is kaphat hozzáférési engedélyeket. A hozzáférési engedélyek tulajdonságai alapján a rendszer kiszámolja a több forrásból szár-

mazó engedélyek eredőjét, az ún. hatályos, vagy érvényes engedélyeket. Egy felhasználó gyakorlatilag kétféleképpen kaphat hozzáférési engedélyeket egy erőforráshoz:

Explicit módon: valamilyen csoporttagság(ok)on keresztül, vagy közvetlenül a felhasználóhoz rendelve.

Örökölt módon: valamilyen csoporttagság(ok)on keresztül, vagy közvetlenül a felhasználóhoz rendelve.

A két legfontosabb szabály közül az egyik, hogy a tiltás erősebb, mint az engedélyezés, a másik pedig az, hogy az explicit engedély erősebb az örökölt engedélynél, még akkor is, ha az örökölt szabály tiltó.

Azaz, ha örökölt engedélyei vannak egy felhasználónak, melyet akár csoporton keresztül, akár közvetlenül kapott, az engedélyek összeadódnak. Kivétel ez alól, ha van tiltó szabály, mert olyankor hiába az összeadódó engedélyek, erősebb lévén a tiltás lesz érvényben az adott engedélyre. Ugyanakkor az explicit módon megadott engedélyek, még az örökölt tiltást is felülbírálják. A legerősebb mindent felülbíráló szabály az explicit módon megadott tiltás.[62]

8.2.9 Mappák megosztása

A Windows Server egyik kiemelkedő szolgáltatása a fájlkiszolgáló (File Server) szerepkör, amelynek segítségével fájl és mappa erőforrásokat lehet megosztani hálózaton keresztül. A mappák ilyen jellegű elérhetővé tételét hívják mappa megosztásnak (Folder Sharing). A mappa megosztás nem csak kimondottan dedikált kiszolgáló számítógépen működhet, hanem akár kliens számítógépeken is, ha azokon is Windows operációs rendszer fut (legalább Windows XP). Gyakran előfordulhat, hogy a hálózatban egy felhasználó a saját számítógépén lévő mappákat meg akar osztani más felhasználókkal. Ilyen esetben is működhet a megosztás. A kliens számítógépeken ezt a szolgáltatást Fájl és nyomtatómegosztásnak (File and Printer Sharing) nevezik.

Egy dedikált fájlkiszolgáló esetén a kiszolgáló számítógép kimondottan azért lett üzembe állítva, hogy tárhelyein olyan fájlokat tároljon, amelyeket a hálózat felhasználói részére elérhetővé tegyen. Ebben a felállásban a fájlkiszolgáló szolgáltatását használó számítógépeket kliensnek nevezik. A továbbiakban a dedikált fájlkiszolgálók mappa megosztása kerül tárgyalásra.

A fájlkiszolgálón csak a kiszolgálófelelősök (Server Operators), a tartománygazdák (Domain Admins) és a helyi rendszergazdák csoport tagjai oszthatnak meg mappákat. A mappák megosztásához is lehet ún. megosztási engedé-

[62] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

lyeket rendelni, de ezzel korántsem lehet egy megosztás elérhetőségét olyan finoman szabályozni, mint az NTFS fájl és mappa hozzáférési engedélyekkel. Célszerű tehát a mappa megosztásokat NTFS fájlrendszeren létrehozni, és a fájl és mappa engedélyeket is használni a megosztási engedélyeken kívül.

Alapvetően kétféle megosztási engedély létezik. Az egyik az olvasás (Read), másik a módosítás (Modify) vagy írás/olvasás (Read/Write). Ha a kettő együtt van alkalmazva, azt a rendszer teljes hozzáférésnek (Full Control) hívja. Alapértelmezés szerint minden megosztott mappához olvasási engedélye (Read) van a mindenki (Everyone) csoportnak. A mappához vagy fájlhoz a továbbiakban a hozzáférést a fájlrendszer szintű engedélyek szabályozzák.

8.2.10 Nyomtatók megosztása

Egy másik nagyon fontos helyi hálózatban használt szolgáltatást a nyomtatás kiszolgáló valósítja meg. A nyomtatás kiszolgáló segítségével a számítógéphez valamilyen módon csatlakoztatott nyomtatót lehet megosztani a hálózat felhasználói és számítógépei számára.

A Windows rendszerekben a nyomtatás szolgáltatás alapvetően két részre bontható. Az egyik rész a nyomtatást kezdeményező számítógépen van. Ez a rész állítja elő a nyomtató számára szükséges formátumot, ez a nyomtatási szolgáltatás kliens része.

A másik rész azon a kiszolgáló számítógépen fut, amelyhez a nyomtató is csatlakozik. Ez a rész fogadja a kliensektől a nyomtatandó dokumentumokat, sorba állítja őket, és vezérli a nyomtatót. Ez a szolgáltatásban a kiszolgáló rész.

Ez a két rész elhelyezkedhet egy számítógépen is, de a nyomtatási folyamat ekkor is kettéválik. A nyomtatási feladatok sorbaállítása azért szükséges, mert előfordulhat, hogy egyszerre több nyomtatási feladat érkezik a kiszolgálóra, azonban a nyomtató egy alapvetően lassú hardvereszköz, amely egyszerre egy feladatot tud kiszolgálni, míg a többinek addig kell várnia, amíg rá nem kerül a sor. A kliens rész amint átadja a nyomtatási feladatot a kiszolgálónak számára a nyomtatás véget ért.

Egy egyszerű felhasználó nem csinálhat meg akármit egy nyomtatóval, ezért a nyomtatóhoz is szükség van hozzáférésvezérlésre. A nyomtatóhoz rendelhető hozzáférési engedélyek a következők:

Nyomtatás (Print): Alapértelmezésben minden felhasználó nyomtathatja, megszakíthatja, szüneteltetheti és folytathatja azon dokumentumok és fájlok nyomtatását, amit a nyomtatóra küldött.

Nyomtató kezelése (Manage printers): Ez az engedély lehetővé teszi a nyomtató átnevezését, törlését, megosztását és beállításainak módosítását. Lehetővé teszi továbbá a többi felhasználó nyomtatóengedélyeinek meghatározását és az összes nyomtatási feladat kezelését. A rendszergazdák csoportja alapértelmezés szerint rendelkezik engedéllyel a nyomtatók kezelésére.

Dokumentumok kezelése (Manage documents): Ha egy felhasználó rendelkezik ezzel az engedéllyel, a nyomtatási várólista minden feladatát kezelheti, beleértve a más felhasználók által nyomtatott fájlokat és dokumentumokat is.

Speciális engedélyek (Special permissions): Ezeknek az engedélyeknek a használatával szükség esetén módosítani lehet a nyomtató tulajdonosát. A nyomtatót létrehozó felhasználó minden nyomtatóengedéllyel rendelkezik, és általában ő telepíti a nyomtatót.[63]

8.2.11 A hozzáférési engedélyek beállitási elvei

A hozzáférés vezérlés szabályozása során a következő elveket célszerű betartani:

- Érdemes mindig megtervezni a hozzáférési engedélyek rendszerét. Itt az egyik legfontosabb alapelv az egyszerűségre és áttekinthetőségre való törekvés. Nem szabad túlbonyolítani.
- A hozzáférési engedélyeket felhasználók helyett csoportoknak érdemes beállítani. Ehhez a felhasználókat valamilyen elv (főként munkájuk vagy erőforrásigényük) szerint kell csoportosítani.
- A hozzáférési engedélyek jobban áttekinthetőek maradnak, ha a szabályozás megmarad az öröklés rendszerére támaszkodva a mappák szintjén. Minél kevesebb a nyilvántartásban az explicit engedély, annál egyszerűbb a rendszer kezelése.
- Az engedélyek mindig úgy legyenek beállítva, hogy a System csoportnak (amely gyakorlatilag az operációs rendszert jelenti) mindig legyen teljes hozzáférése a rendszer (%systemroot%, Windows) és felhasználói mappákhoz (Users). Célszerű az alapértelmezett engedélyeket békénhagyni.
- Mappa megosztás esetén érdemes a megosztott mappákat NTFS fájlrendszerű lemezen létrehozni, és a megosztási engedélyek használatán kívül az NTFS hozzáférési engedélyek szintjén is beállítani a hozzáférés szabályait.

[63] Microsoft Corporation: Néhány szó a nyomtatóengedélyekről. Online cikk, Microsoft Corporation, <http://windows.microsoft.com/hu-HU/windows-vista/What-are-printer-permissions>, 2012.09.27

- Explicit tiltást csak akkor szabad használni, ha az feltétlenül szükséges. Érdemes helyette implicit tiltást használni, azaz nem engedélyezni az adott felhasználónak vagy csoportnak az elérést.[64]

8.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

8.3.1 Összefoglalás

A többfelhasználós rendszereknél egyszerűen nélkülözhetetlen az erőforrások hozzáférésének szabályozása. Egy modern rendszer esetében két biztonsági lépcsőfokot kell eredményesen venni, hogy az erőforrást elérje a felhasználó. Az egyik a hitelesítés, melynek három fajtája került ismertetésre. A bejelentkezés helyben, bejelentkezés hálózaton keresztül és a tartományi bejelentkezés. A másik lépcsőfok a hozzáférési engedélyek által szabályozott hozzáférés.

Minden objektummal eltárolódik az ún. hozzáférés vezérlési lista (ACL), amelynek minden eleme (ACE) egy felhasználói vagy csoport fiókot és azoknak az erőforráshoz való hozzáférés szabályozását tartalmazza. A szabályozás lehet engedélyező és lehet tiltó.

Az objektumok közül az NTFS fájl és mappa engedélyeknek van a legtöbbféle beállítási lehetősége. A szokásos engedélyek száma azonban nem több, mint más objektumok esetében. Ezek rendre: olvasás, olvasás és végrehajtás, mappa tartalmának listázása, módosítás, írás, valamint az összeset egyszerre tartalmazó teljes hozzáférés. A speciális engedélyekből ennél jóval több van, de azokat speciális esetektől eltekintve nem szokták alkalmazni.

Egy felhasználó több forrásból is kaphat hozzáférési engedélyt egy erőforráshoz. Az engedélyek lehetnek örököltek, vagy közvetlenül ún. explicit módon megadottak, illetve a szabályozás lehet engedélyező és tiltó. Két alapszabály létezik, az egyik szerint az explicit megadás erősebb, mint az örökölt, illetve a tiltás erősebb, mint az engedélyezés. Összefoglalva, az explicit tiltás a legerősebb, majd az explicit engedélyezés következik, aztán az örökölt tiltás, majd a végén az örökölt engedélyezés. Abban az esetben, ha egy felhasználó több csoporton keresztül kap hozzáférési engedélyeket, akkor az örökölt engedélyek egymással, és az explicit engedélyek is egymással adódnak össze, tiltás esetén a tiltott engedély „kivonódik”.

A mappák nem csak az adott számítógépen, hanem a hálózaton keresztül is megoszthatók, hasonlóan a nyomtatók is. Ezekhez az objektumokhoz is szabá-

[64] Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

lyozni kell a hozzáférést, melyhez ezek is rendelkeznek engedélyekkel, melyek nem annyira finoman szabályozhatók, mint a fájl és mappa engedélyek.

8.3.2 Önellenőrző kérdések

1. Miért van szükség hozzáférés-vezérlésre?
2. Ismertesse az erőforrásokhoz való hozzáférés lépéseit!
3. Mi az ACL és az ACE? Mik az ACE részei?
4. Milyen típusú lehet egy hozzáférési engedély szabályozás?
5. Sorolja fel a szokásos NTFS fájl és mappa engedélyeket!
6. Melyek az engedély-öröklés szabályai?
7. Mi a csoportok szerepe a hozzáférés-vezélés esetében?
8. Mit jelent a hatályos engedély kifejezés? Mikor lehet vele találkozni?
9. Sorolja fel, a mire kell figyelni a mappa megosztás esetén!
10. Ismertesse a nyomtató megosztások hozzáférési engedélyeit!
11. Melyek a hozzáférési engedélyek beállításának elvei?

9 TÖMEGES TELEPÍTÉS

9.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Ebben a leckében olyan technológiákkal találkozhat a hallgató, amelyek a hálózatba kötött számítógépek központosított kezelésének a telepítéssel kapcsolatos területeit érintik. Ezek nagyobb, tipikusan vállalati környezetben, nagyrészt homogén gépparkból kialakított hálózatok esetén használhatók. Először a központi Windows-telepítési szolgáltatások (WDS), Windows kiszolgálói szerepkör jellemzői, majd a WDS telepítése, beállítása és működése kerül ismertetésre. Majd ezek után bemutatásra kerülnek a WDS használatával történő távtelepítés lépései.

A lecke második részében a tömeges telepítés technológiája kerül ismertetésre, melynek keretein belül tárgyalásra kerül a Windows automatikus telepítési csomag (WAIK) és a válaszfájlok szerepe is. A lecke végén a tömeges telepítés lépéseivel, valamint a telepítéssel kapcsolatos javaslatokkal ismerkedhet meg a hallgató.

A tananyag elsajátítása után a hallgató képes lesz Windows hálózati környezetben teljesen automatikus, vagy manuális, beavatkozás igénylő, egyedi és tömeges telepítések elvégzésére hálózaton keresztül, vagy akár hálózatról indítva a kliens számítógépeket.

9.2 TANANYAG

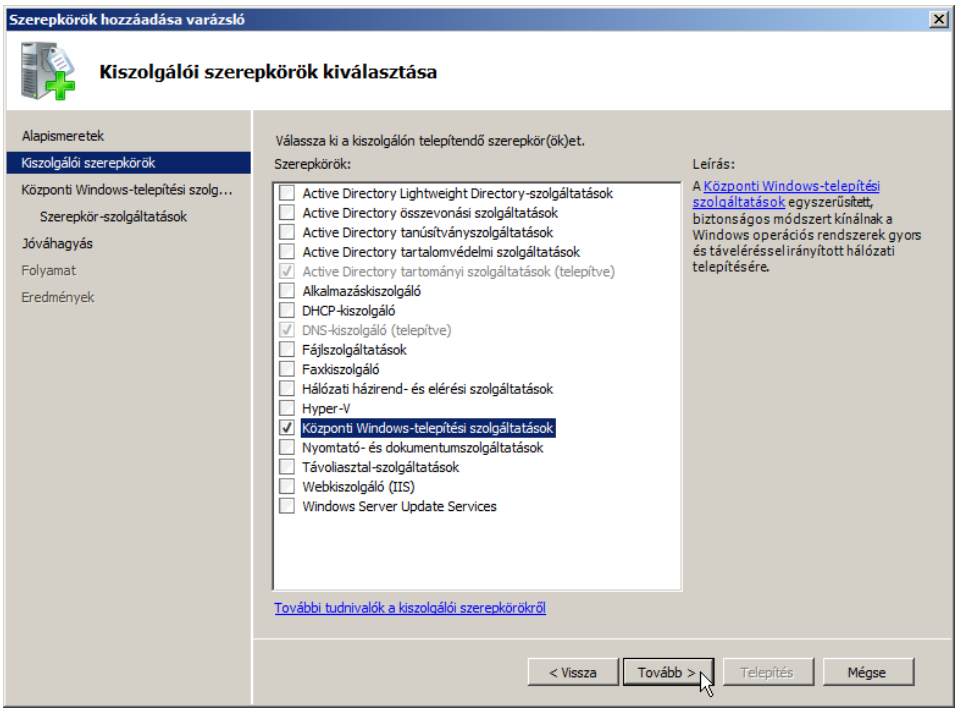
9.2.1 Telepítés vállalati környezetben

Egy kis vagy közepes vállalat esetében is legalább több tíz kliens számítógéppel kell a rendszergazdának számolnia, amikor a rendszerek telepítéséről vagy karbantartásáról van szó. Ilyen esetekben általában homogén környezettel lehet számolni a számítógépek hardver és szoftver ellátottságával kapcsolatban. Azaz általában ugyanolyan hardveren, ugyanolyan szoftvereknek kell futnia, beleértve ebbe az operációs rendszert is. Ezekre az esetekre találták ki a Microsoft különböző, tömeges telepítést és központi menedzsment is támogató szoftvereit. Ezek közül ebben a leckében a Windows telepítési szolgáltatások tömeges telepítéssel kapcsolatos funkciói kerülnek előtérbe.

9.2.2 A központi Windows-telepítési szolgáltatások

A Windows Server 2003-tól rendelkezésre áll a **központi Windows-telepítési szolgáltatások** szerepkör (Windows Deployment Services – WDS), amely segítséget nyújt a rendszergazdáknak, hogy hálózaton keresztül, akár több számítógépet is telepítsen egyszerre emberi közbeavatkozás nélkül. Ez utóbbi a tömeges telepítés.

A WDS segítségével természetesen nem csak tiszta telepítést lehet végrehajtani, hanem akár egy referencia számítógép is „sokszorosíthatóvá" válik. Ebben az esetben a referencia számítógép létrehozása után, amelyen minden használandó program telepítve megtalálható, létrehozható a gépről egy **telepítési kép** (Windows Image) fájl, amely a WDS segítségével lesz telepíthető. Ezekhez a műveletekhez szükség lesz még a **Windows automatikus telepítési csomagra** (Windows Automated Installation Kit – WAIK), amely ingyenesen elérhető a Microsoft weboldalán.[65]

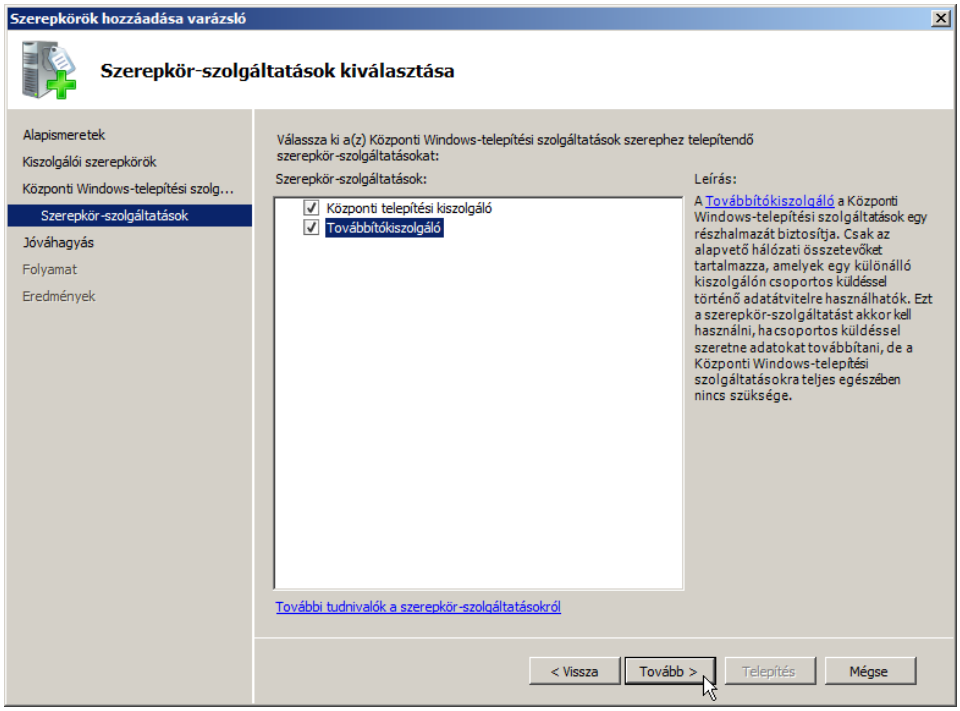


106. ábra: A központi Windows telepítési szolgáltatások szerepkör kijelölése telepítésre

[65] Trina Gorman: Windows Deployment Services Getting Started Guide. Elektronikus kiadvány, Redmond, Microsoft Corporation, 2009

A WDS telepítése

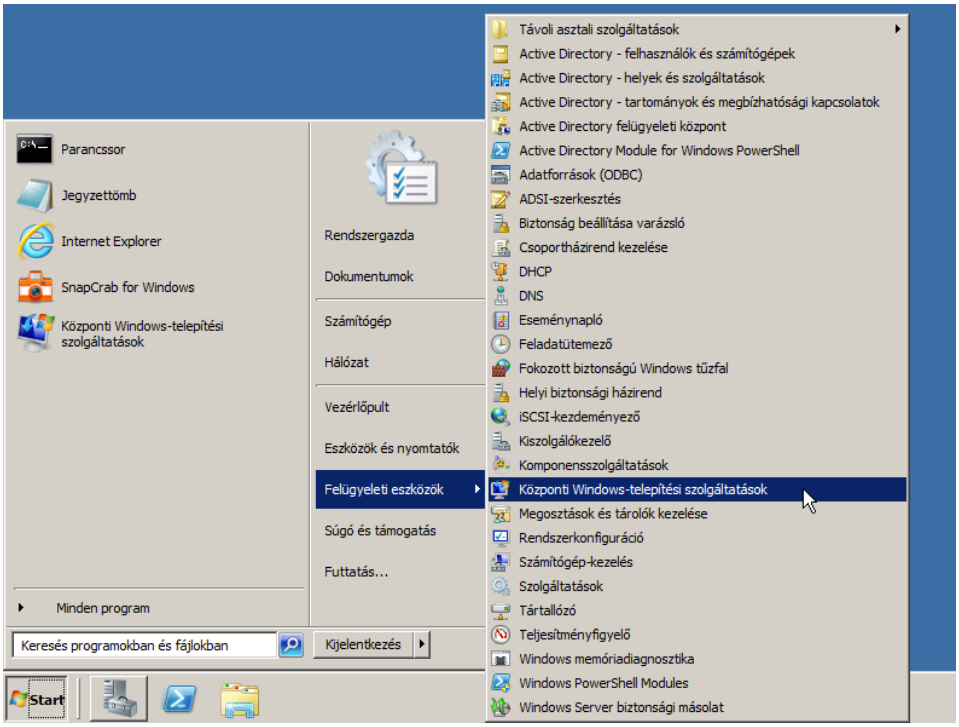
A WDS szerepkör telepítéséhez a **kiszolgáló kezelőben** (Server Manager) ki kell választani a **szerepkör hozzáadása** (Add Roles) lehetőséget, majd a megjelenő **szerepkör hozzáadása varázsló** (Add Roles Wizard) alapismeretek lapján a **következő** gombra kell kattintani. A megjelenő szerepkör listából a **központi Windows-telepítési szolgáltatások** választása után megint csak ki kell választani a **következő** gombot. A következő **áttekintő** ablak tartalmát figyelmesen elolvasva, majd a **következő** gombra kattintás után két szerepkör szolgáltatás válik láthatóvá.



107. ábra: Továbbítókiszolgáló a tömöges telepítéshez

A Windows Server 2008-as verziótól egy új funkció épült be a **csoportos küldéssel** (Multicasting) működő központi telepítés szolgáltatás megjelenésével, amelyet igény szerint itt lehet bekapcsolni a **továbbítókiszolgáló** (Transport Server) kiválasztásával. A **központi telepítési kiszolgáló** (Deployment Server) a tulajdonképpeni hagyományos értelemben vett csoportos küldés nélküli WDS, azaz ez a szerepkör szolgáltatás mindenképpen bekapcsolandó. A **következő** (Next) gomb megnyomása után a **jóváhagyás** (Confirmation) lépésnél a tájékoz-

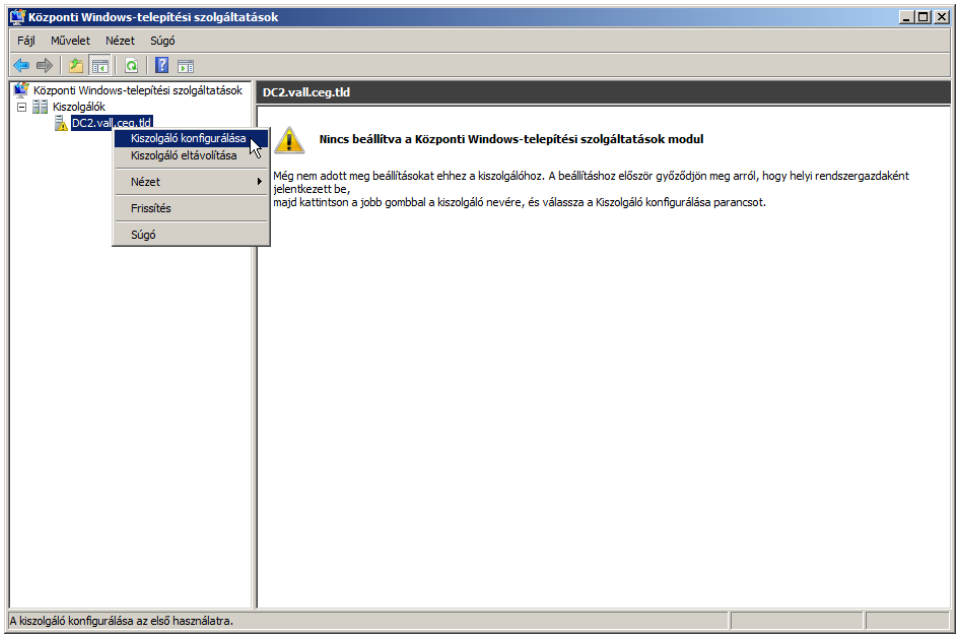
tató üzenet elolvasásával a **telepítés** (Install) gombra kattintva indul a szerepkör telepítése. A folyamat végén a **bezárás** (Close) gombra kell kattintani.



108. ábra: Indítás

A WDS konfigurálása

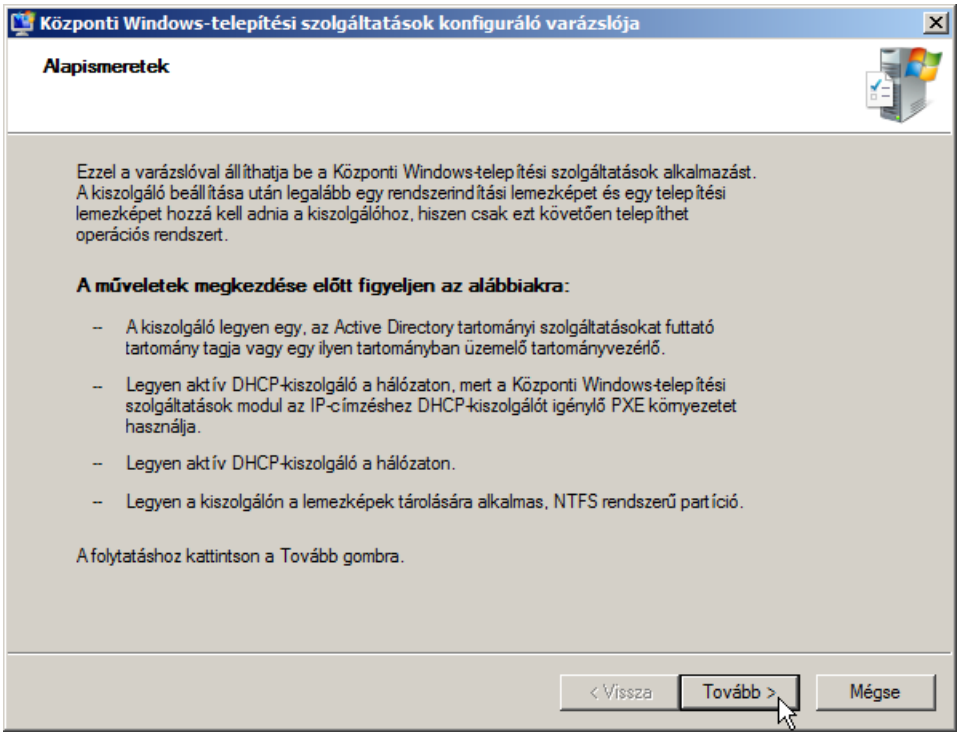
A WDS első indításakor szükséges a kiszolgáló megfelelő konfigurálása. A WDS kezelő konzolja elérhető a kiszolgáló kezelőben a szerepkörök között, de elindítható külön ablakban is a **start menü felügyeleti eszközök** (Administrative Tools) almenüjében található **központi Windows-telepítési szolgáltatások** (Windows Deployment Services) menüpontjának kiválasztásával.



109. ábra: A kiszolgáló konfigurálása

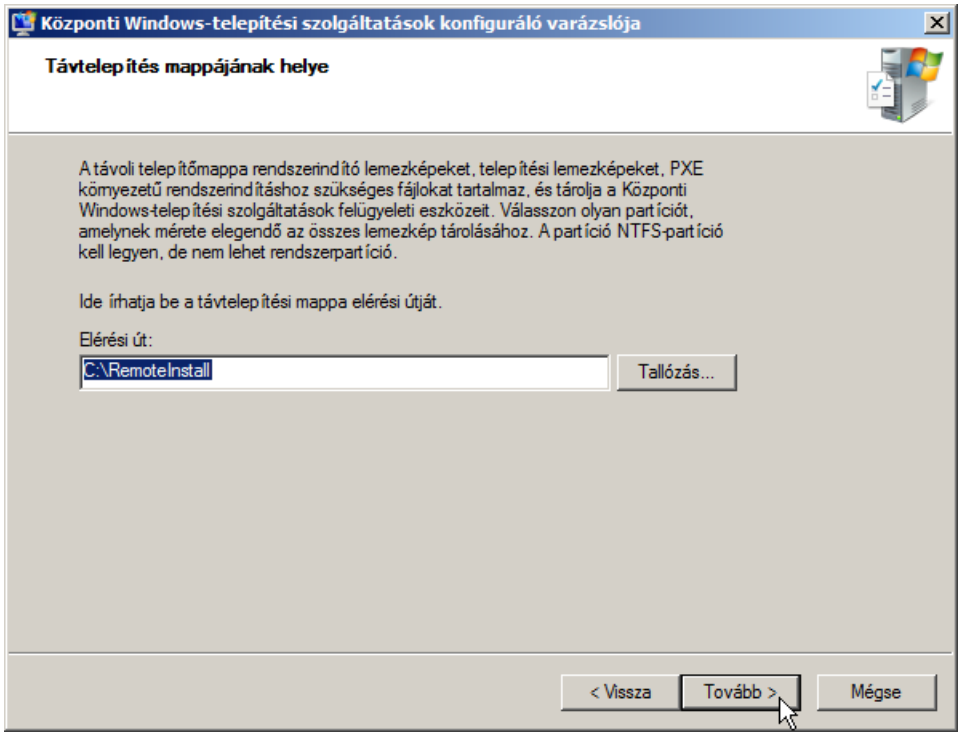
A kezelő konzol bal oldalán a **kiszolgálók** (Servers) előtti plusz jelre kattintva kibontható a kiszolgálók listája. Most egyelőre csak egy kiszolgáló látható a listában. A kiszolgáló megfelelő működéséhez jobb gombbal a kiszolgáló nevére kell kattintani és a megjelenő helyi menüből ki kell választani a **kiszolgáló konfigurálása** (Configure Server) menüpontot. Az alapismeretek ablakban megjelenő figyelmeztető szövegből kiderül, hogy a WDS megfelelő működésének a következők a feltételei:

- A kiszolgáló legyen egy, az AD tartományi szolgáltatásokat futtató tartomány tagja vagy egy ilyen tartományban üzemelő tartományvezérlő.
- Legyen aktív DHCP-kiszolgáló a hálózaton, mert a Központi Windows telepítési szolgáltatások modul az IP címzéshez DHCP-kiszolgálót igénylő PXE környezetet használja.
- Legyen aktív DNS kiszolgáló a hálózaton
- Legyen a kiszolgálón lemezképek tárolására alkalmas, NTFS rendszerű partíció.



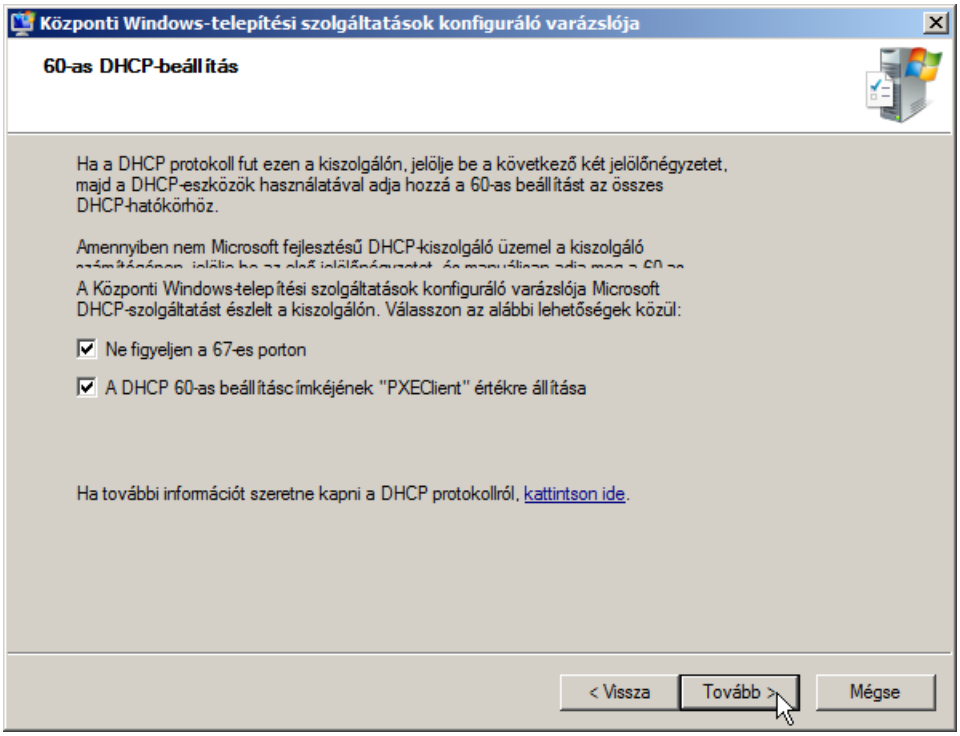
110. ábra: Feltételek a működéshez

Ha a feltételek adottak, akkor a **tovább** (Next) gombra kattintva meg kell adni a **távtelepítés mappájának a helyét** (Remote Installation Folder Location). Ugyan a megjelenő szöveg tájékoztat arról, hogy a mappa nem lehet a rendszerpartíción, valójában lehet, csak legfeljebb nem szerencsés. (Ebben az esetben a mappa a C: meghajtón lesz, de nem teszt környezetben a gyártó ajánlatait célszerű a betartani. Ezt a lehetőséget választva a konfiguráló varázsló is figyelmeztet. Itt a C:\RemoteInstall mappa lesz.)



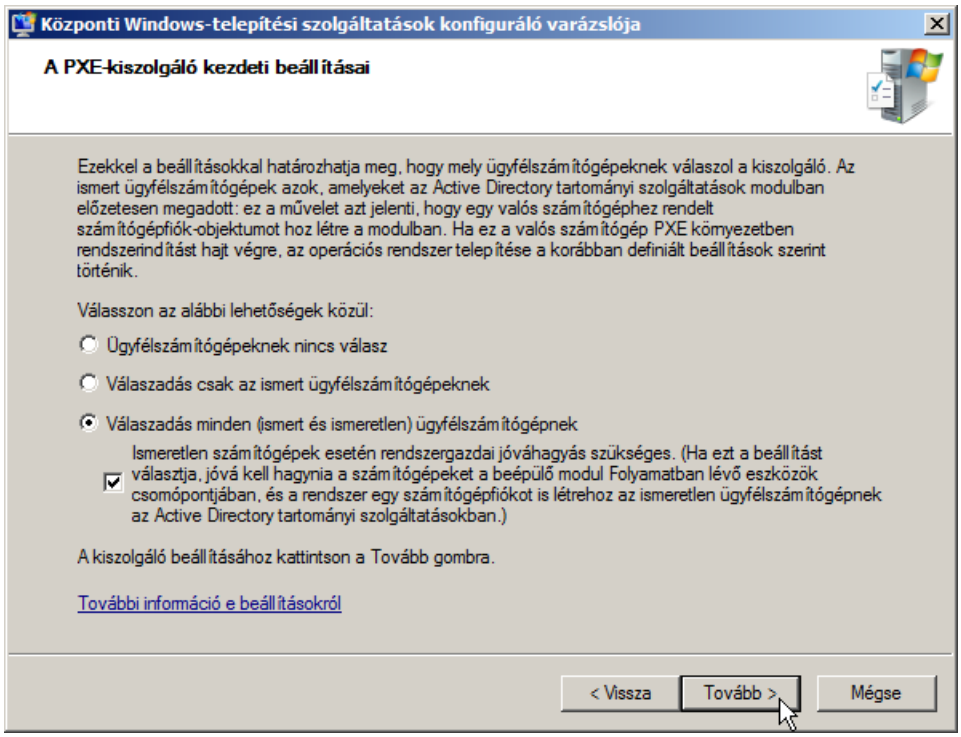
111. ábra: A távtelepítés mappája

A következő lépésben a hálózat DHCP kiszolgálójával kapcsolatos beállításokat lehet megadni. Abban az esetben, ha az adott WDS-t futtató kiszolgálón DHCP kiszolgáló is fut, a **ne figyeljen a 67-es porton** (Do not listen on port 67) kapcsolót be kell kapcsolni, ugyanis ezen a porton figyel a DHCP kiszolgáló is. Így viszont be kell állítani a DHCP kiszolgálón a 60-as opciót, úgy hogy értéke 'PXEClient' legyen. Ugyancsak be kell kapcsolni **a DHCP 60-as beállításcímkéjének 'PXEClient' értékre állítását** (Configure DHCP option to 'PXEClient'), de csak abban az esetben, ha a helyben működő DHCP kiszolgáló Microsoft, ugyanis a WDS konfiguráló varázsló csak ebben az esetben tudja a 60-as opciót konfigurálni. Minden más esetben a rendszergazdának kell azt kézzel megtennie a hálózat DHCP kiszolgálóján.



112. ábra: DHCP beállítás

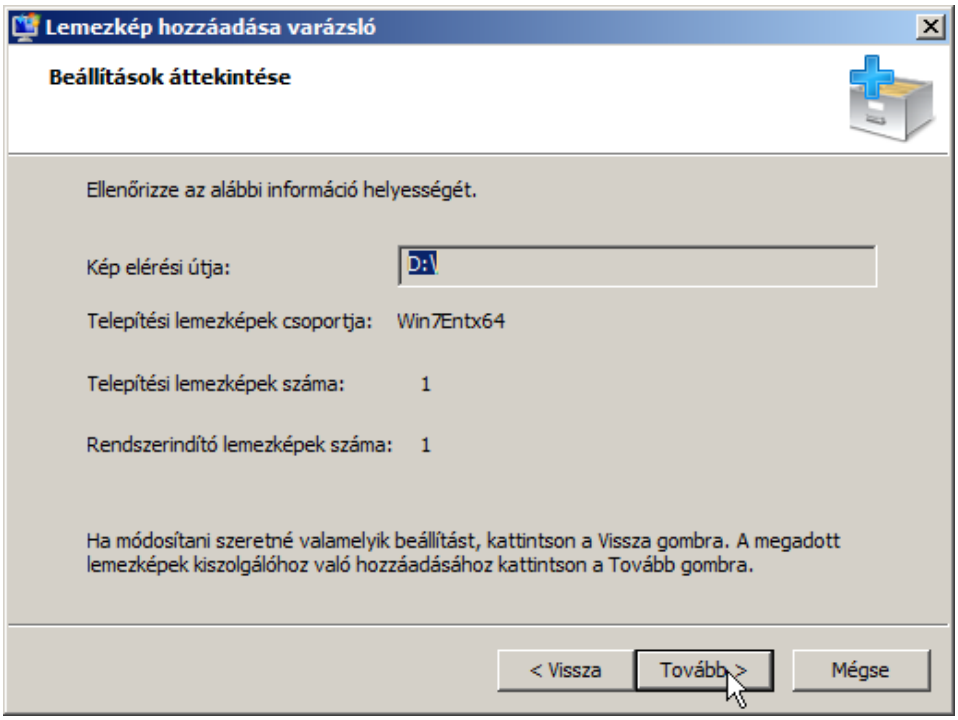
A **tovább** (Next) gombra kattintva következő párbeszédpanelen a PXE kiszolgáló kezdeti beállításait lehet megadni. A részletes leírás elolvasása után az egyszerűbb kezelhetőség miatt célszerű a **válaszadás minden (ismert és ismeretlen) ügyfélszámítógépnek** (Respond to all (known and unknown) client computers), illetve az **ismeretlen számítógépek esetén rendszergazdai jóváhagyás szükséges** (For unkown clients, notify administrator and respond after approval) lehetőségek választása.



113. ábra: A PXE kiszolgáló kezdeti beállításai

Ezután a **tovább** (Next) gombra kattintva befejeződik a WDS konfigurálása és a varázsló elindítja a szolgáltatást. A **befejezés** (Finish) gomb megnyomása előtt lehetőség van **a lemezképek azonnali hozzáadása a kiszolgálóhoz** (Add images to Windows Deployment Services now) kapcsoló bekapcsolásával telepítési és rendszerindító lemezképek megadásával folytatni a konfigurációt. Ha ez az opció bekapcsolásra került, akkor a **befejezés** (Finish) gomb megnyomása után elindul a **lemezkép hozzáadása varázsló** (Add Image Wizard). Lemezképeket természetesen utólag bármikor hozzá lehet adni a rendszerhez, arról nem is beszélve, hogy a gyártó a WDS getting started guide-ban is erre bíztatja a felhasználót.[66]

[66] Trina Gorman: Windows Deployment Services Getting Started Guide. Elektronikus kiadvány, Redmond, Microsoft Corporation, 2009



114. ábra: Lemezkép hozzáadása

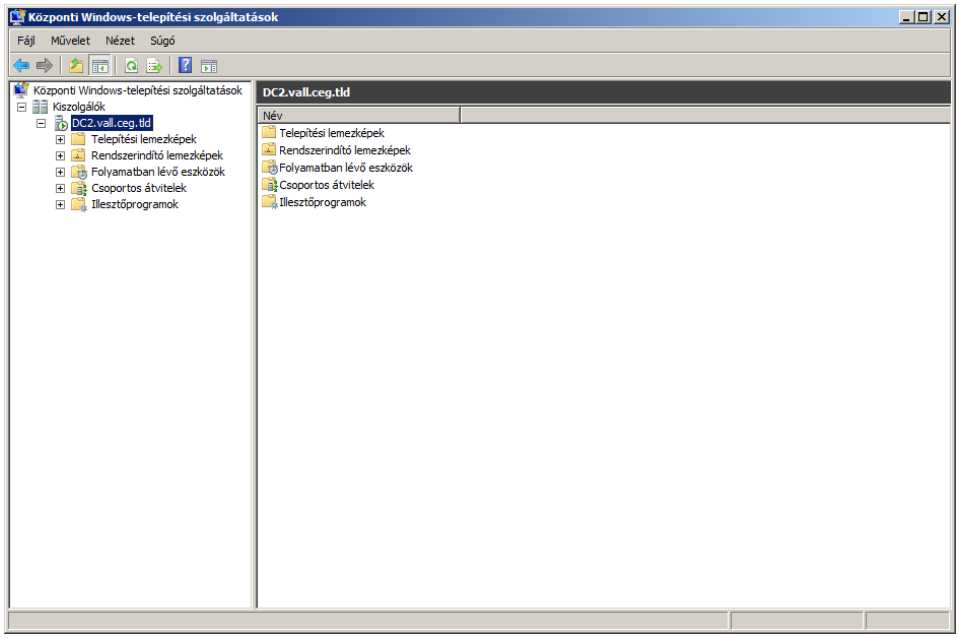
A telepítés előkészítése

A konfiguráció után a kezelő konzolban a kiszolgáló neve alatt létrejön egy 5 mappa, melyek a következők:

- **Telepítési lemezképek** (Install Images): Idesorolhatók azok az alapértelmezett operációs rendszer képfájlok, amelyek a telepítő DVD-n találhatók és install.wim a nevük, valamint az egyedileg készített telepítő képfájlok, amelyek akár egy előre feltelepített referencia gépről készültek el korábban. A lényeg, hogy az ide telepített képfájlok lesznek a WDS-hez csatlakozó kliensekre telepítve.
- **Rendszerindító lemezképek** (Boot Images): Ebbe a mappába olyan ún. **Windows előtelepítési környezet** (Windows Preinstallation Environment – Windows PE) képfájlokat kell telepíteni, amelyek a telepítendő számítógépek indításához szükségesek. Az alapértelmezett képfájlok a telepítő DVD-n található **boot.wim** fájlok (Sources mappa), ezek tartalmazzák az előtelepítési környezetet valamint a WDS klienst.
- **Folyamatban lévő eszközök** (Pending Devices): Ha a PXE kiszolgáló kezdeti beállításainál be van kapcsolva az **ismeretlen számítógépek esetén**

rendszergazdai jóváhagyás szükséges (For unkown clients, notify administrator and respond after approval) kapcsoló, akkor azok a számítógépek, amelyek eddig nem voltak tagjai a tartománynak megjelennek ebben a mappában és várják a rendszergazdai jóváhagyást.

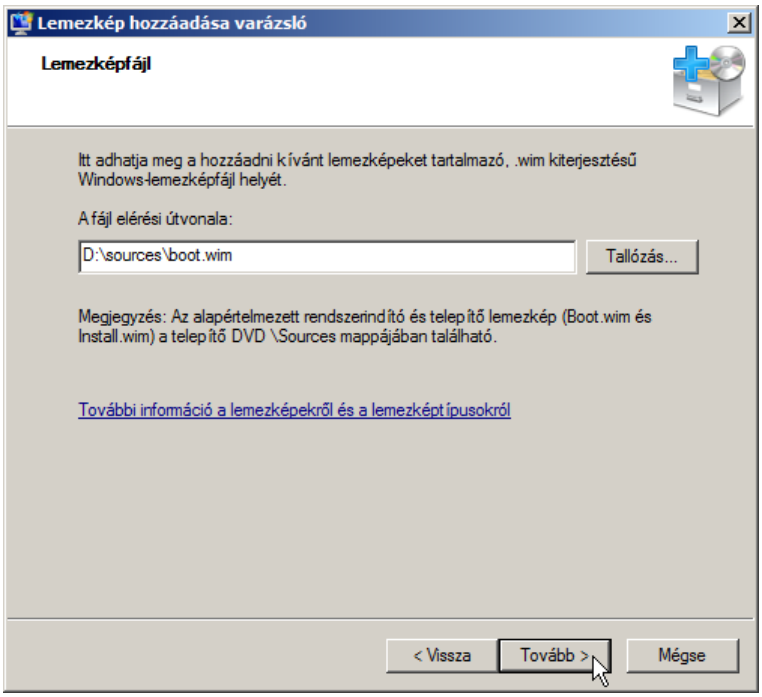
- **Csoportos átvitelek** (Multicast Transmissons): Ez az újdonság, amelynek segítségével különösebb hálózati terhelés nélkül tömegesen telepíthetők a számítógépek **csoportos küldés** (Multicast) segítségével. A telepítés folyamán a mappában megjelennek a telepítendő számítógépek, és láthatóvá válik a telepítési folyamat kijelzője is.
- **Illesztőprogramok** (Legacy Images): Abban az esetben, ha olyan hardver eszközt (pl. hálózati kártya vagy merevlemez vezérlő) tartalmaz a telepítendő számítógép, amelynek meghajtó programja nem található meg az adott operációs rendszer telepítő képfájljában (mert pl. nem volt rajta a telepítő lemezen), ide telepíthetők kérdéses a meghajtó programok.



115. ábra: A kezelő konzol

A rendszerindító lemezképek telepítéséhez az egér jobb gombjával a **rendszerindító lemezképek** (Boot Images) mappára kattintva ki kell választani a **rendszerindító lemezkép hozzáadása** (Add boot image) menüpontot. Az elinduló lemezkép hozzáadása varázsló párbeszéd ablakában a **tallózás** (Browse)

gombra kattintva ki kell jelölni a telepíteni kívánt operációs rendszer (ebben az esetben Windows 7) telepítő lemezén a **Sources** mappában található **boot.wim** fájlt. (Ehhez természetesen be kell helyezni a telepítő lemezt a megfelelő meghajtóba.)



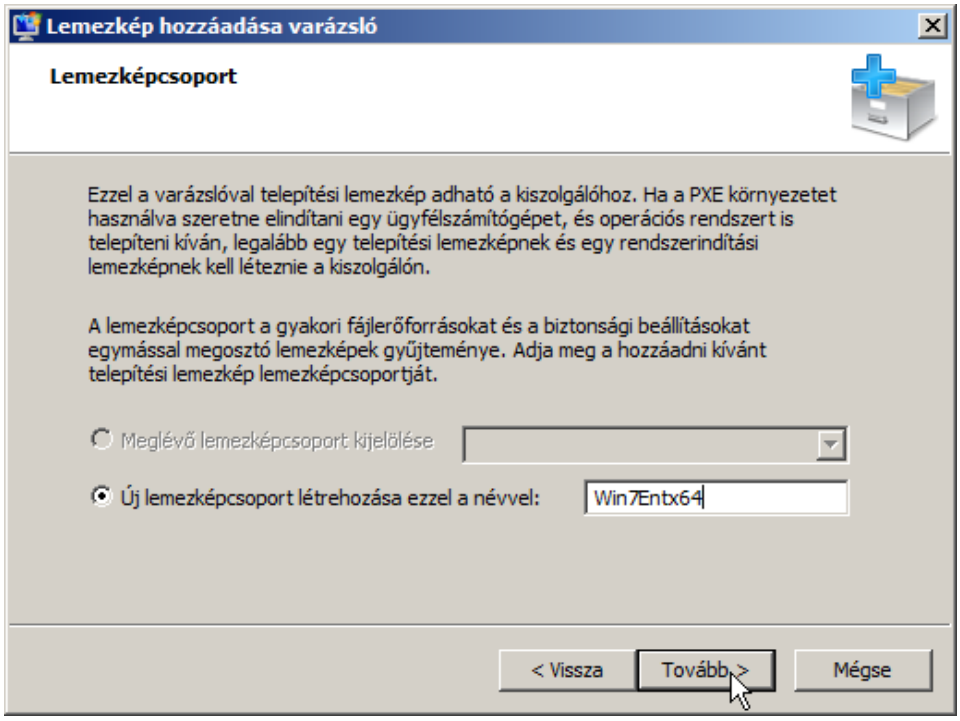
116. ábra:

A kiválasztás után megadható a lemezkép neve és egy részletesebb leírás a lemezképhez, valamint látható lesz a lemezkép architektúrája, amely x86, x64, IA64 lehet attól függően, hogy 32 bites vagy 64 bites Intel, vagy Intel Itanium 64 bites architektúrájú a telepítendő számítógép. (A 64 bites Intel rendszerek általában indíthatók 32 bitessel is, az irányadó mindig a telepítendő operációs rendszer architektúrája legyen.)

Az **összegzés** (Summary) párbeszédablakban leellenőrizhető, hogy valóban jó lemezkép fájl lett-e megadva, majd a **tovább** (Next) gombra kattintva megtörténik a lemezkép hozzáadása, mely műveletet a **befejezés** (Finish) gombra kattintva lehet lezárni. Több rendszerindító lemezkép is telepíthető, hiszen elképzelhető más architektúrájú telepítendő számítógép is. Az azonos architektúra esetén célszerű a WDS-t tartalmazó Windows Server 2008-as telepítő lemezen található rendszerindító képet vagy annál újabb verziójút megadni. Régebbi

lemezképpel indítva (pl. Windows Vista telepítő lemezről származó boot.wim) gyakran fordulhat elő probléma.

A következő fontos teendő a telepítések megkezdése előtt a telepítési lemezkép telepítése. A műveletet a telepítési lemezképek mappára jobb gombbal kattintva, majd a telepítési lemezkép hozzáadása menüpontot kiválasztva lehet megkezdeni. A megjelenő párbeszédablakban megadhatjuk annak a lemezkép csoportnak a nevét, amelyhez a telepítési lemezképet szeretnénk hozzáadni. Mivel még nincs telepítve egyetlen telepítési lemezkép sem, így az **új lemezképcsoport létrehozása ezzel a névvel** (Create a new image group) opciót kell választani és meg kell adni a létrehozandó csoport nevét (ebben az esetben pl. Win7x64). Ha a későbbiekben szükséges újabb lemezképek telepítése, akkor már választható lesz az új csoport létrehozása helyett a **meglévő lemezképcsoport kijelölése** (Select from exsisting image groups) opció is. Természetesen lemezkép csoport létrehozható lemezkép hozzáadása nélkül is a **lemezképcsoport hozzáadása** (Add image group) menüpont kiválasztásával.[67]

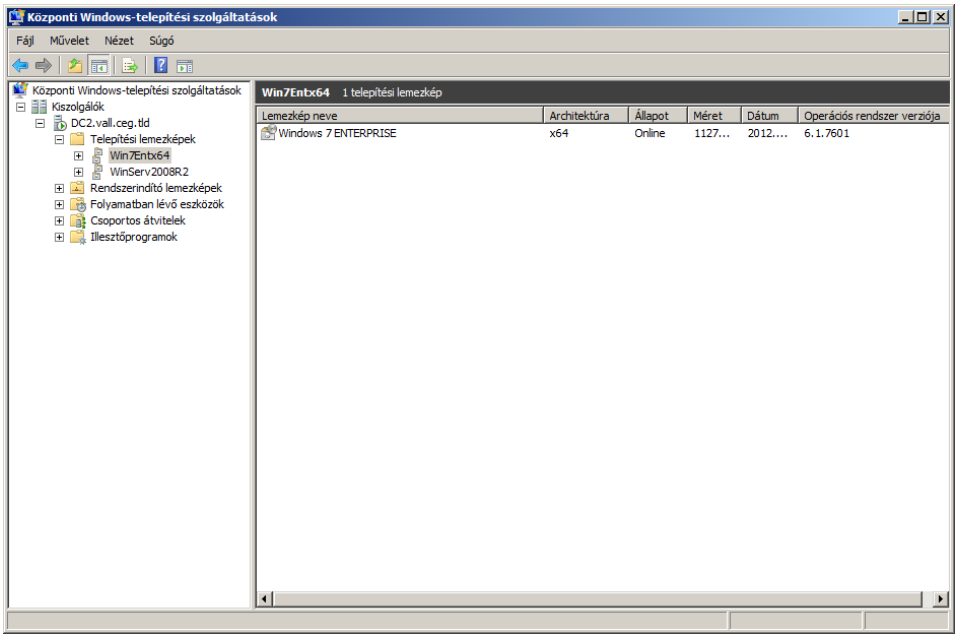


117. ábra: Lemezképcsoport létrehozása

[67] Trina Gorman: Windows Deployment Services Getting Started Guide. Elektronikus kiadvány, Redmond, Microsoft Corporation, 2009

A kiválasztott lemezkép csoport után a **tallózás** (Browse) gombra kattintva ki kell választani a telepítő lemez Source mappájából az **install.wim** képfájlt. A **tovább** (Next) gombra kattintva a rendelkezésre álló lemezképek listából ki kell választani a megfelelő lemezképet. (Ebben az esetben csak egy lemezkép látható, a Windows 7 ENTERPRISE, így azt kell választani.)

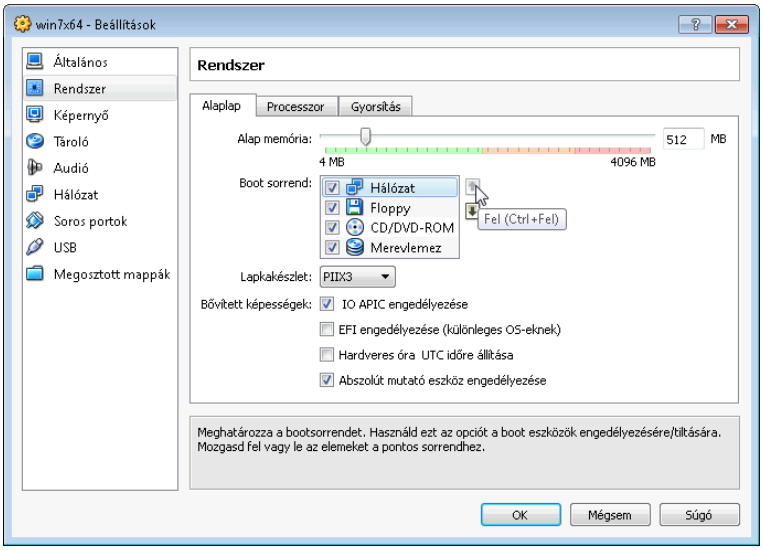
Az **összegzés** (Summary) párbeszédablakban leellenőrizhető, hogy minden megfelelően lett-e kiválasztva, majd a **tovább** (Next) gombra kattintva elindul a telepítési lemezképek hozzáadása. A művelet végén a **befejezés** (Finish) gombra kattintva a varázsló bezáródik.



118. ábra: A Windows 7 ENTERPRISE lemezkép a helyére került

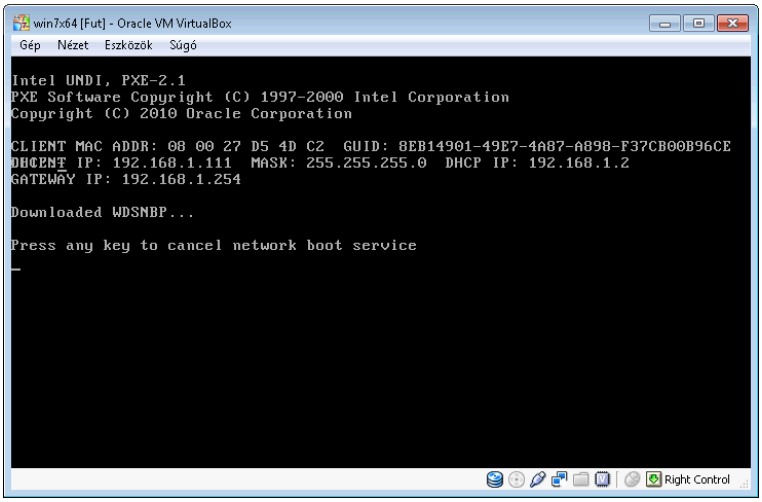
9.2.3 Távtelepítés WDS segítségével

Ezek után már hozzá is lehet kezdeni a hálózaton keresztül végzett, ún. távtelepítéshez, mindössze arra van szükség, hogy a telepítendő számítógépek hálózati kártyája rendelkezzen ún. **előindítási végrehajtási környezet** (Pre-Boot eXecution Environment – PXE) ROM-mal és az **indítási sorrendben** (Boot order) ez a lehetőség legyen az első elérhető.



119. ábra: Indítási sorrend beállítása VirtualBox-os VM esetén

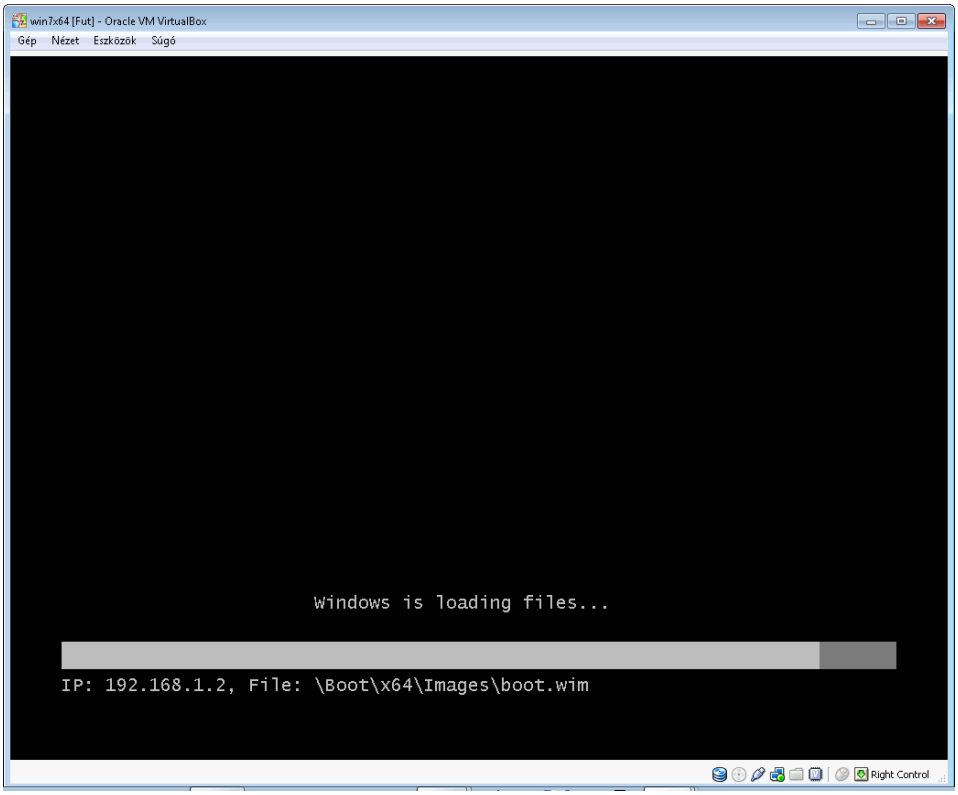
A telepítendő számítógép indítás után megpróbál hálózatról indulni. Ehhez először a DHCP kiszolgálótól kap IP címet a számítógép, illetve a többi IP beállításon kívül megkapja a 60-as opcióban a PXEClient értéket, és csatlakozik a PXE kiszolgálóhoz, majd alapértelmezetten az **F12** billentyű leütésére vár.



120. ábra: Elindult a letöltés

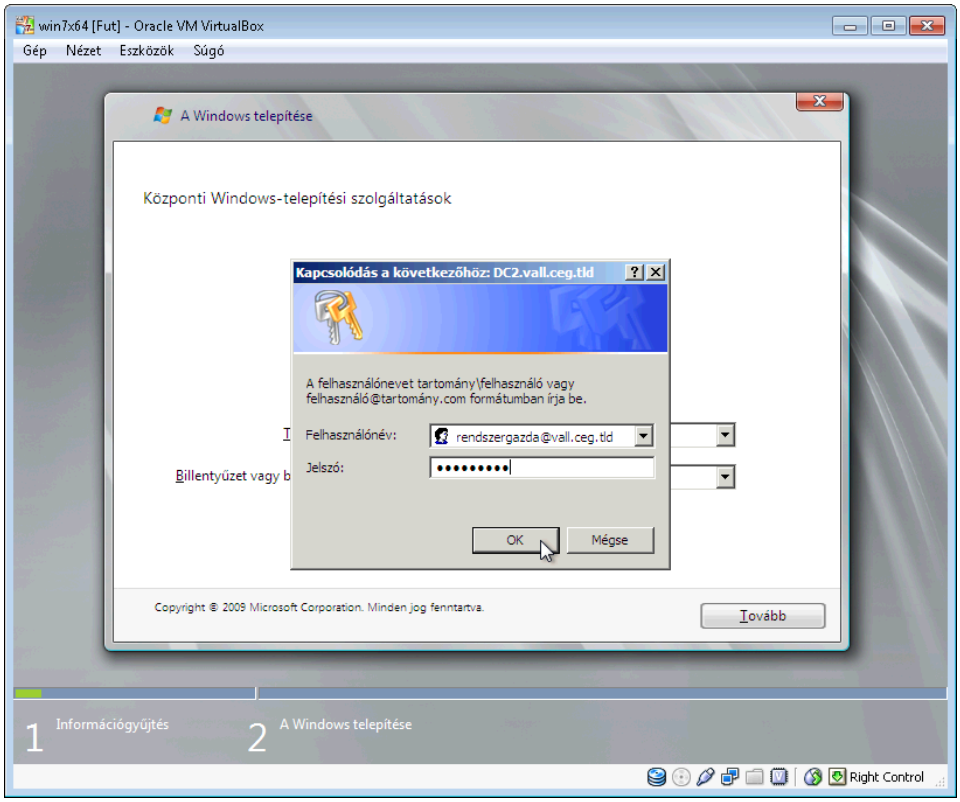
Ha ez elmarad, az indítás meghiúsul, ellenkező esetben pedig a számítógép a TFTP kiszolgálóról megpróbálja letölteni az indítási képfájlt. Mind a PXE, mind

a **triviális fájlátviteli protokoll** (Trivial File Transfer Protocol – TFTP) kiszolgáló a WDS része. Az alapértelmezett **F12** leütésre várást a kezelő konzolban a kiszolgáló nevére jobb gombbal kattintva és a megjelenő helyi menüből a tulajdonságokat választva meg lehet változtatni a **rendszerindítás** (Boot) tulajdonságlapon.



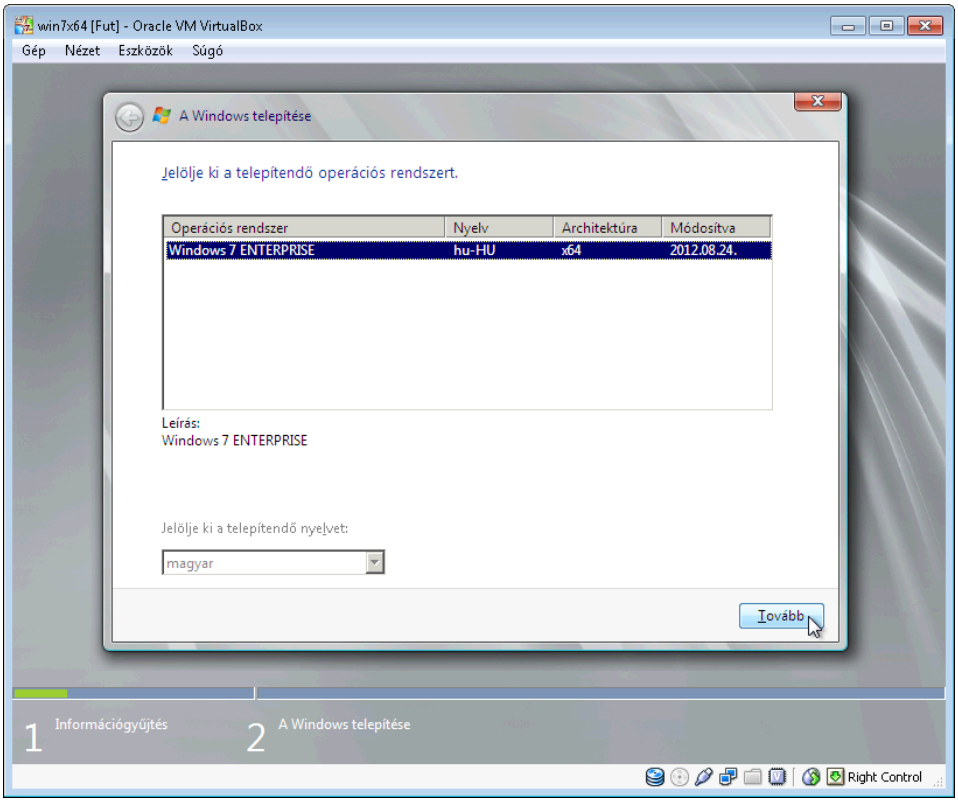
121. ábra: Töltődik a telepítő

Miután a Windows PE képfájl letöltődött a TFTP kiszolgálóról elindul a WDS kliens. Elsőként a **területi beállítást** (Locale) illetve a **billentyűzet vagy beviteli módszert** (Keyboard settings) kell megadni. Ebben az esetben mindkettő a magyar. A **tovább** (Next) gombra kattintva megjelenik egy bejelentkezési ablak, ahol a tartományi rendszergazda felhasználó nevét (rendszergazda@vall.ceg.tld vagy VALL\rendszergazda) és jelszavát megadva azonosítani kell a WDS-en a klienst.



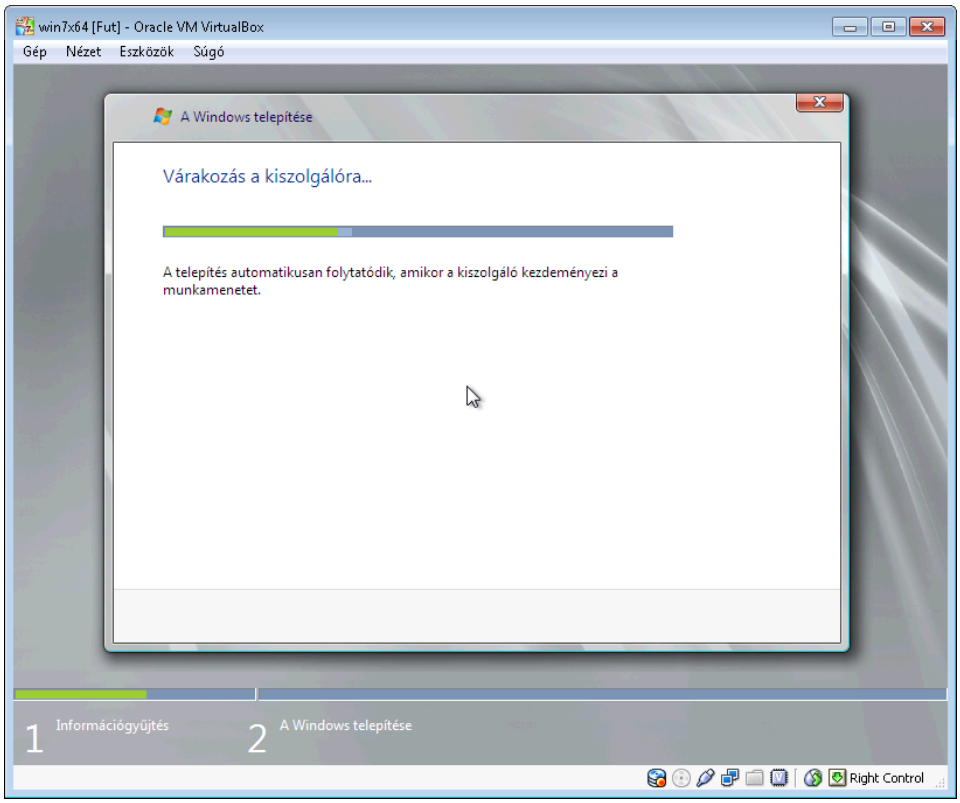
122. ábra: A telepítésre jogosult felhasználó azonosítása

A következő ablakban a WDS-re telepített telepítési képfájlok nevei, azaz a **telepítendő operációs rendszerek** (Select the operating system you want to install) jelennek meg. (Ebben az esetben csak egy választható a listából: Windows 7 Enterprise). Ha a telepítő csomag tartalmaz több nyelvet is tartalmaz, akkor a **telepítendő** rendszer **nyelvét** (Select language to install) is ki lehet választani. (Ebben az esetben ezt nem lehet.)



123. ábra: Windows 7 Enterprise a telepítendő rendszer

A **tovább** (Next) gombra kattintva a **hova kívánja telepíteni a Windows rendszert** (Where do you want to install Windows?) feliratú ablak jelenik meg, ahol ki lehet választani azt a lemezterületet, ahova az operációs rendszer telepítve lesz. Itt egyedi lemez-partícionálásra is van lehetőség a **meghajtó beállításai (haladó)** (Drive Options /advanced/) szövegre kattintva. Továbbá a telepítő által nem támogatott **illesztőprogram** (Load Driver) is megadható a Windows 7 és Windows Server 2008 R2 tiszta telepítéseinél bemutatott módon. A **tovább** (Next) gomb megnyomása után elkezdődik a rendszer telepítése.



124. ábra: Ilyen nincs a DVD-s telepítésnél

A telepítési folyamat ugyanazon lépésekből áll, mint a tiszta DVD-ről történő telepítés esetén, hiszen mindkettő esetben egy telepítő képfájlról történik a telepítés. (Ebben az esetben ráadásul gyakorlatilag ugyanarról a képfájlról.)

Az összetevők és frissítések telepítése végeztével a számítógép újraindul. Ha az indulás során az **F12** nem lesz lenyomva, akkor a hálózati indítás elmarad, és már a telepített Windows rendszer indul el.

9.2.4 Mi kell a tömeges távtelepítéshez?

A tömeges telepítéshez több tényezőt kell figyelembe venni. Nagyon fontos, hogy a telepítésnél ugyanolyan architektúrájú számítógépekkel kell dolgozni, hiszen egyszerre egyféle telepítési lemezképet lehet a hálózaton a klienseknek elküldeni. Természetesen ki kell használni a csoportos küldés adta lehetőséget is. Egy tömeges telepítés nehezen képzelhető el úgy, hogy a rendszergazdának minden egyes telepítési lépésnél közbe kell avatkoznia, mert pl. a **tovább** (Next) gombra kattintani. Ennek a problémának a kivédésére lehetőség

van automatikus, ún. **nem felügyelt** (Unattended) telepítésre. A nem felügyelt telepítéshez létre kell hozni egy ún. **válaszfájlt** (Unattend.xml), amelyben tulajdonképpen előre meg kell adni a válaszokat a telepítő kérdéseire. Ezenkívül további beállítások megadására is van lehetőség, amelynek eredményeképpen a telepítés után egy szinte teljesen felkonfigurált rendszer kapható.

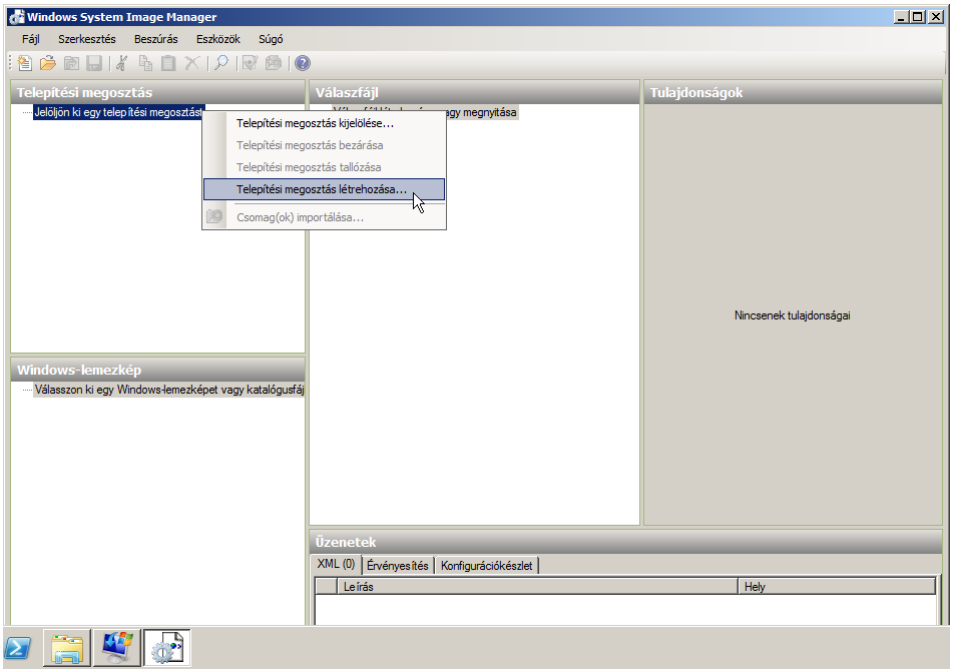
A nem felügyelt telepítés válaszfájljának létrehozásához szükség van egy **Windows rendszerképkezelő** (Windows System Image Manager) nevű programra, amely a **Windows automatikus telepítési csomag** (Windows Automated Installation Kit – WAIK) része, amelynek 3.0-ás verziója **CD kép** (ISO image) formátumban letölthető a
http://www.microsoft.com/hu-hu/download/details.aspx?id=5753 címről.

A WAIK telepítése

A telepítő CD lemezre írását követően a lemezt a meghajtóba helyezve (vagy egy alkalmas programmal virtuális meghajtóként a rendszerhez csatolva) a telepítő elindul.

125. ábra: Így indul a WAIK telepítése

A jobb oldali menüből a **Windows AIK telepítőt** (Windows AIK Setup) választva elindul a telepítő varázsló (Install Wizard). A **tovább** (Next) gombra kattintva licensz szerződés jelenik meg. Figyelmes elolvasását követően az **elfogadom** (Accept) opciót választva és a következő gombra kattintva a **telepítési mappa megadása** (Select Installation Folder) párbeszéd ablak jelenik meg. Itt el lehet fogadni a telepítő által felajánlott értékeket, majd ismét a **tovább** (Next) gombra kell kattintani. A telepítés megkezdéséhez ismét a **tovább** (Next) gombra kell kattintani **a telepítés megerősítése** (Confirm Installation) párbeszédablakon. A telepítési folyamat végén a **bezárás** (Close) gombbal be kell zárni a telepítő alkalmazást. Meg kell jegyezni, hogy a telepítő egy jó adag dokumentációt is feltelepített a kiszolgálóra, amely szinte nélkülözhetetlen lehet a válaszfájlok elkészítéséhez.[68]



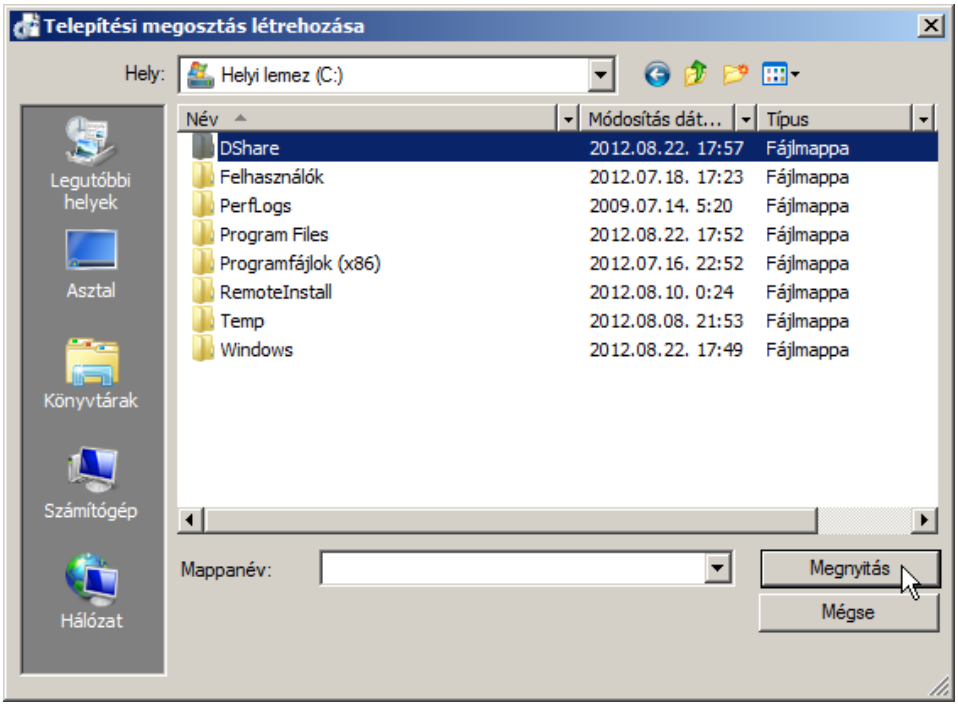
126. ábra: Telepítési megosztás létrehozása

A válaszfájl elkészítése

A Start menüből a Microsoft Windows AIK almenüben található **Windows rendszerképkezelő** (Windows System Image Manager) menüponttal indítható a válaszfájlt elkészítő program. Miután a program elindult a **telepítési megosztás**

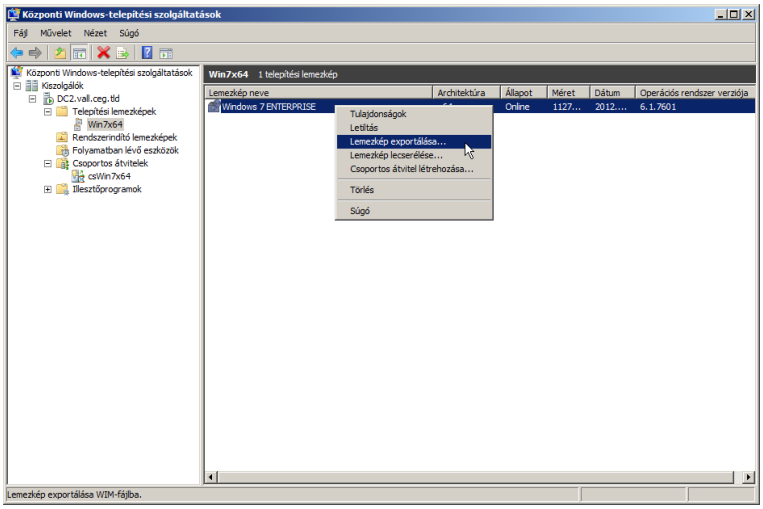
[68] Trina Gorman: Windows Deployment Services Getting Started Guide. Elektronikus kiadvány, Redmond, Microsoft Corporation, 2009

(Distribution Share) ablakban a **jelöljön ki egy telepítési megosztást** (Select a Distribution Share) szövegre jobb gombbal kattintva a megjelenő helyi menüből ki kell választani a **telepítési megosztás létrehozása** (Create New Distribution Share) menüpontot.



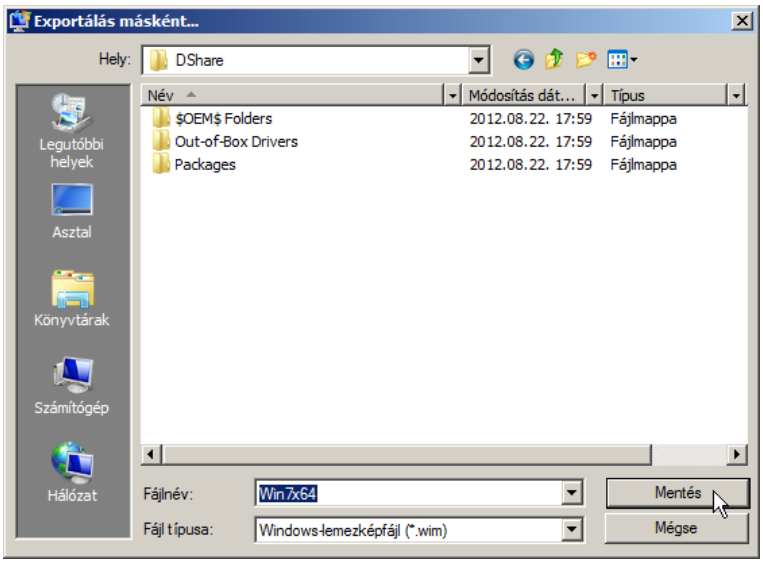
127. ábra: A megosztás megnyitása

A megjelenő párbeszédpanelen ki kell jelölni egy üres mappát (ha nincs alkalmas, akkor az **új mappa** (New Folder) ikonra kattintva létre kell egyet hozni), majd a **megnyitás** (Open) gombra kell kattintani. (Ebben az esetben ez a C:\DShare mappa.) A kijelölés hatására a kiválasztott mappán belül létrejön három további mappa (OEMFolders, Out-of-Box Drivers, Packages).



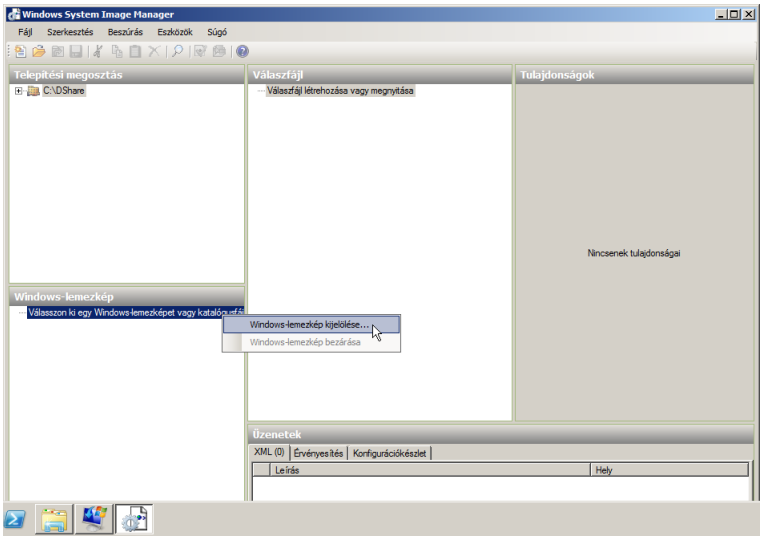
128. ábra: Lemezkép exportálása

A következő lépés az lesz, hogy a WDS-ben a telepítési lemezképek közül jobb gombbal ki kell választani a telepítendő telepítési lemezképet, azaz a telepítendő operációs rendszert (ebben az esetben a Windows 7 ENTERPRISE-t), majd a megjelenő helyi menüből ki kell választani a **lemezkép exportálása** (Export) menüpontot.



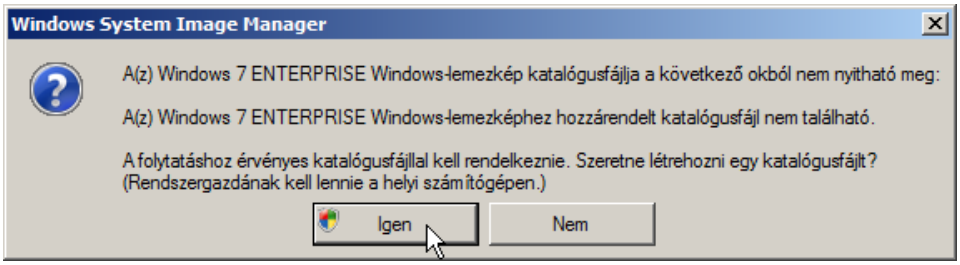
129. ábra: Exportálás másként

A megjelenő párbeszédablakban meg kell adni az exportálandó fájl helyét és nevét. A hely legyen a Windows rendszerképkezelőben megadott telepítési megosztás mappája, a név pedig pl. Win7x64. Ezek után a **mentés** (Save) gombra kattintva a lemezkép exportálása megkezdődik.



130. ábra: Windows-lemezkép kijelölése

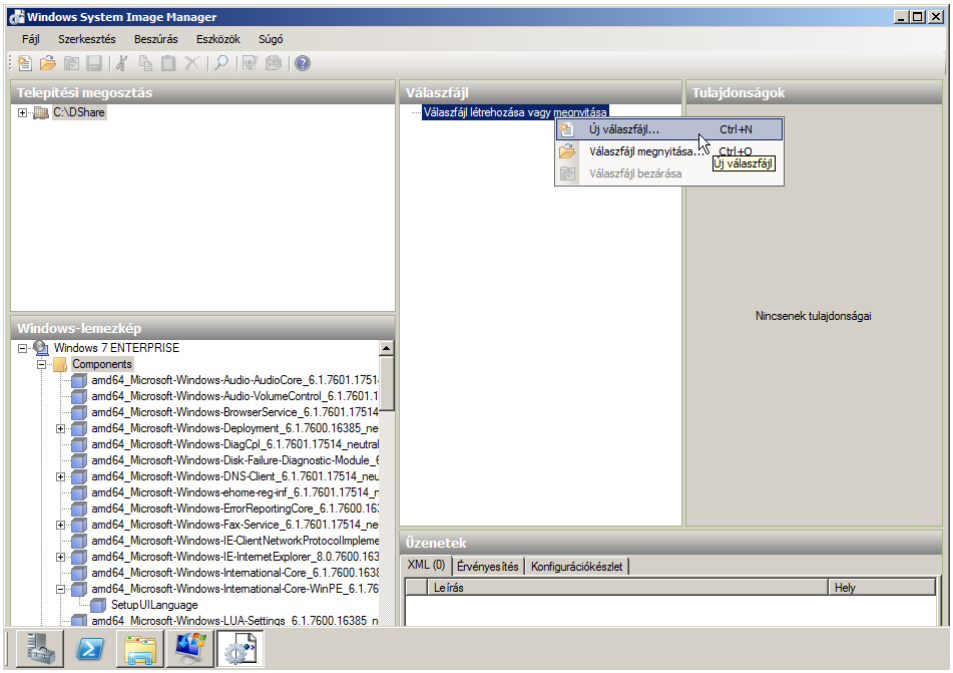
Exportálás befejeztével a **Windows-lemezkép** (Windows Image) ablakban a **válasszon ki egy Windows-lemezképet vagy katalógusfájlt** (Select a Windows image or catalog file) elemre jobb gombbal kattintva megjelenik egy helyi menü, melyből a **Windows-lemezkép kijelölése** (Select a Windows Image) menüpontot választva a megjelenő párbeszéd ablakban meg kell adni az előzőekben exportált lemezképet (C:\DShare\Win7x64.WIM).



131. ábra: Ez látható, ha nincs katalógusfájl

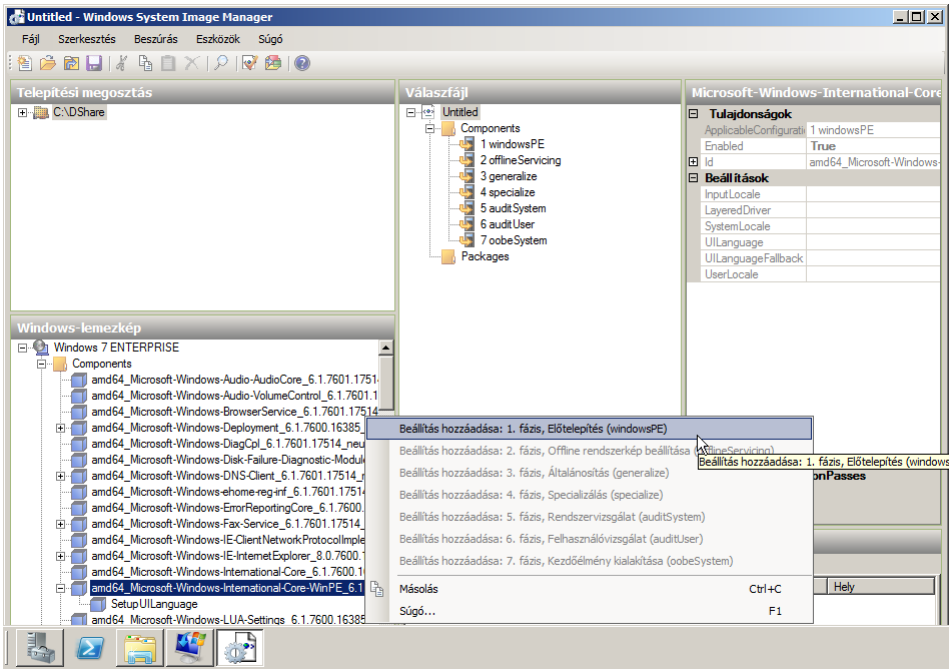
Egy dialógus ablak jelenik meg, amelyben a rendszerképkezelő figyelmezteti a felhasználót, hogy a lemezképhez nem tarozik katalógus fájl, de ha van rá

igény, akkor az **igen** (Yes) gombra kattintva a program létrehozza azt. Ezt célszerű elfogadni, mert érvényes katalógus fájl nélkül a procedúrát nem lehet folytatni. A katalógusfájl előállítása eltart egy pár percig, de amint elkészül a **windows-lemezkép** (Windows Image) ablakban megjelenik a megadott lemezkép. A „+” jelre kattintva kibontható fa struktúra két fő eleme a **komponensek** (Components), amely az alaprendszer különböző komponenseinek beállításait tartalmazza, illetve a **csomagok** (Packages), amely a **csomagfrissítésektől** (Update) kezdve a további extra funkciókig (FeaturePack) tartalmaz összetevőket.



132. ábra: Új válaszfájl létrehozása

Következő lépésként a **válaszfájl** (Answare file) ablakban a **válaszfájl létrehozása vagy megnyitása** (Create or Open Answare file) elemre jobb gombbal kattintva a megjelenő helyi menüből ki kell választani az **új válaszfájl** (New Answare file) menüpontot. Ezt követően a válaszfájl ablakban megjelenik egy a Windows-lemezkép ablakban találhatóhoz hasonló fa struktúra, amely az üres válaszfájlt reprezentálja.



133. ábra: Beállítás hozzáadása a válaszfájlhoz

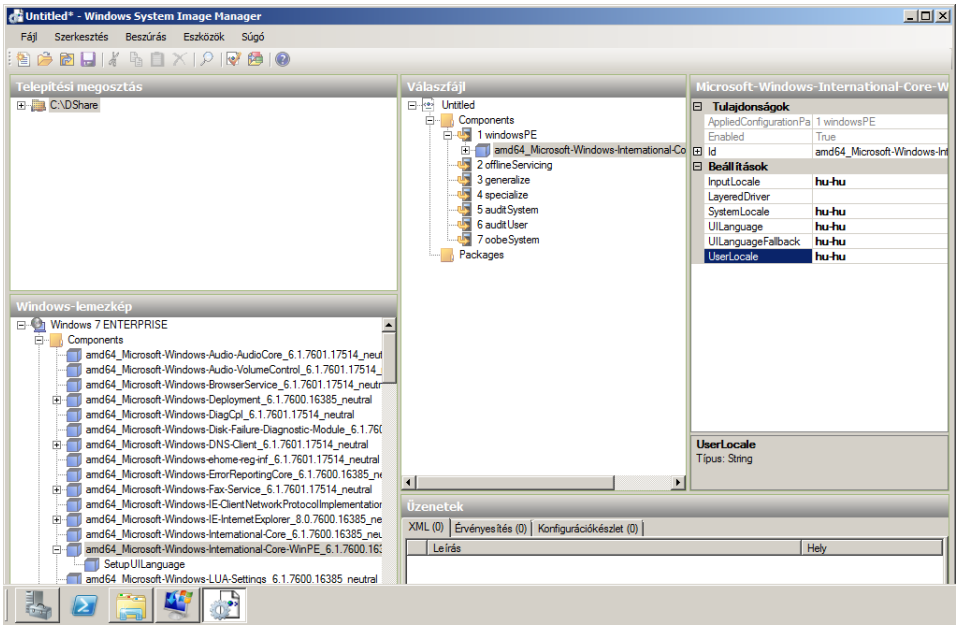
A telepítési folyamatban felmerülő beállításokat alapvetően két részre tudjuk osztani. Az első kimondottan a telepítő beállításaira, illetve a telepítési folyamat alatt beállítandó dolgokra vonatkozik, míg a második tulajdonképpen a telepítés utáni beállítások összességére.

Az első beállítások összefoglalva a WDS kliensre vonatkoznak, így az ezen beállításokat tartalmazó válaszfájl neve WDSClientUnattend.xml lesz. A WDS kliens válaszfájljába a következő beállításokat kell megadni az automatizált telepítéshez.

- A telepítő regionális és nyelvi beállításai
- Tartományi azonosítás
- Partíciók beállítása és módosítása

Elsőként a regionális és nyelvi beállítások megadása következik. Ehhez a Windows-lemezkép ablakban a **Components** tárolót kibontva ki kell jelölni jobb gombbal a **windows-international-core-winpe** elemet. (64 bites rendszer esetén az elem pontos neve: **amd64_Microsoft-Windows-International-Core-WinPE**, 32 bites esetén **x86_Microsoft-Windows-International-Core-WinPE** A többi beállítási elem névmegadása hasonlóan alakul.) A megjelenő helyi menü-

ből ki kell választani a **beállítás hozzáadása: 1. fázis, Előtelepítés (windowsPE)** (Add Setting to Pass 1 windowsPE) menüpontot.[69]

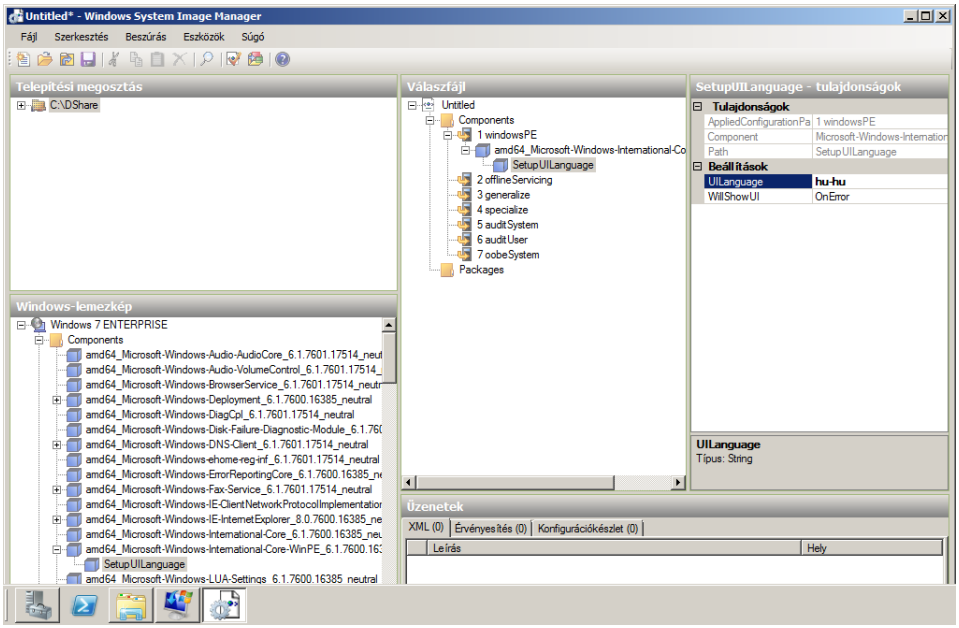


134. ábra: Magyar nyelvi beállítások

A művelet hatására a **válaszfájl** (Answare File) ablakban a **Components** alatt található **1 windowsPE** elem alatt megjelenik az előzőleg kijelölt elem. A mellette lévő **tulajdonságok** (Properties) ablak neve a kiválasztott elem nevét veszi fel és az ablakban megjelennek az adott elemhez tartozó beállítási lehetőségek.

A **beállítások** (Settings) szakaszban a **LayeredDriver** lehetőség kivételével mindenhova be kell állítani a nyelvet. (Magyar esetén a beállítás: **hu-hu**, angol esetén: **en-us**.)

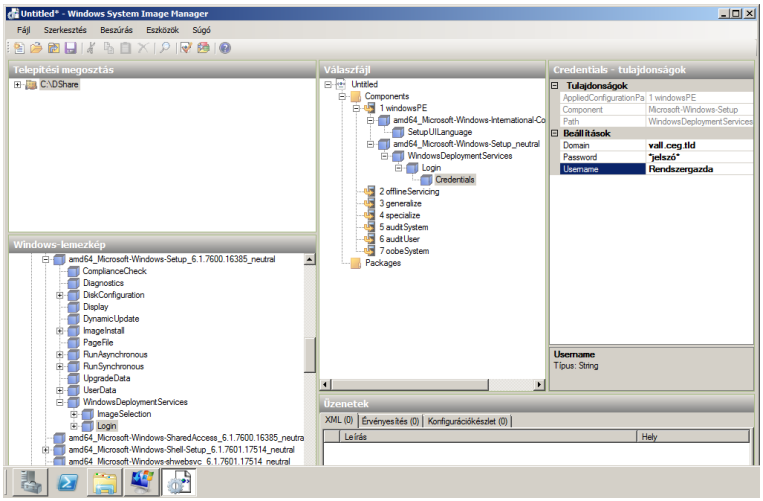
[69] Trina Gorman: Windows Deployment Services Getting Started Guide. Elektronikus kiadvány, Redmond, Microsoft Corporation, 2009



135. ábra: A telepítő nyelvi beállítása

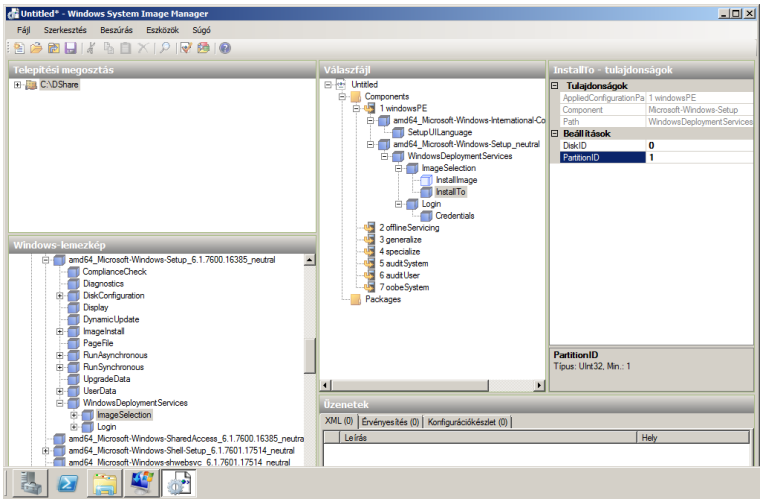
Az elemet kibontva egy újabb **SetupUILanguage** nevű elem jelenik meg, melynek **beállítások** (Settings) szekciójában az imént említett nyelvi beállítást kell az **UILanguage** lehetőségnél megadni. (Ebben az esetben hu_hu.)

A következő megadandó opció már a tartományi azonosítás beállításaihoz tartozik. A **windows-setup\WindowsDeploymentServices** elemet kibontva a **Login**-ra jobb gombbal kattintva, a megjelenő menüből ki kell választani a **beállítás hozzáadása: 1. fázis, Előtelepítés (windowsPE)** (Add Setting to Pass 1 windowsPE) menüpontot.



136. ábra: A rendszergazda felhasználó

A **válaszfájl** (Answare File) ablakban a **Login** elem alatt ki kell választani a **Credentials**-t. A megjelenő **beállításoknál** (Settings) ki kell tölteni a **tartomány** (Domain), a **jelszó** (Password) és a **felhasználónév** (Username) mezőket. (A tartomány ebben az esetben a vall.ceg.tld, a felhasználó a rendszergazda a jelszó pedig értelem szerűen a rendszergazda felhasználó jelszava.)

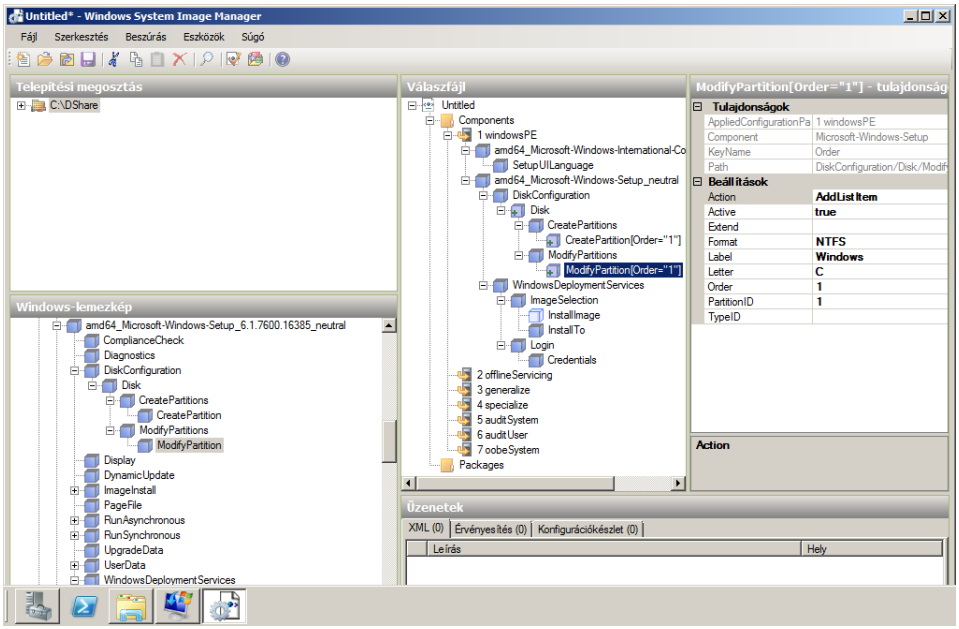


137. ábra: Diszk és partíció beállítások

A következő beállítandó opció az **ImageSelection** elem szintén a **windows-setup\WindowsDeploymentServices** alatt található. A beállításhoz a megszo-

kott módon ezt is hozzá kell adni a válaszfájlhoz. A **válaszfájl** (Answare File) ablakban az **ImageSelection** alatt az **InstallTo** elemet választva a **beállítások** (Settings) szakaszban meg kell adni a **lemez azonosító** (DiskID) és **partíció azonosító** (PartitionID) mezőket. Itt rendre 0 és 1.

A megadott lemez és partíció azonosítóknak akkor van értelme, ha ezek a valóságban is léteznek, egyébként létrehozásukat be kell állítani a válaszfájlban. A **Windows-Setup\DiskConfiguration\CreatePartitions** alatt a **CreatePartition** elemet jobb gombbal kiválasztva ezt is hozzá kell adni a válaszfájlhoz. A **CreatePartition beállításainál** (Settings) a **kiterjeszt** (Extend) mezőt **igazra** (true), a **sorrendet** (Order) **1**-re a **típust** (Type) **elsődlegesre** (Primary) kell állítani.

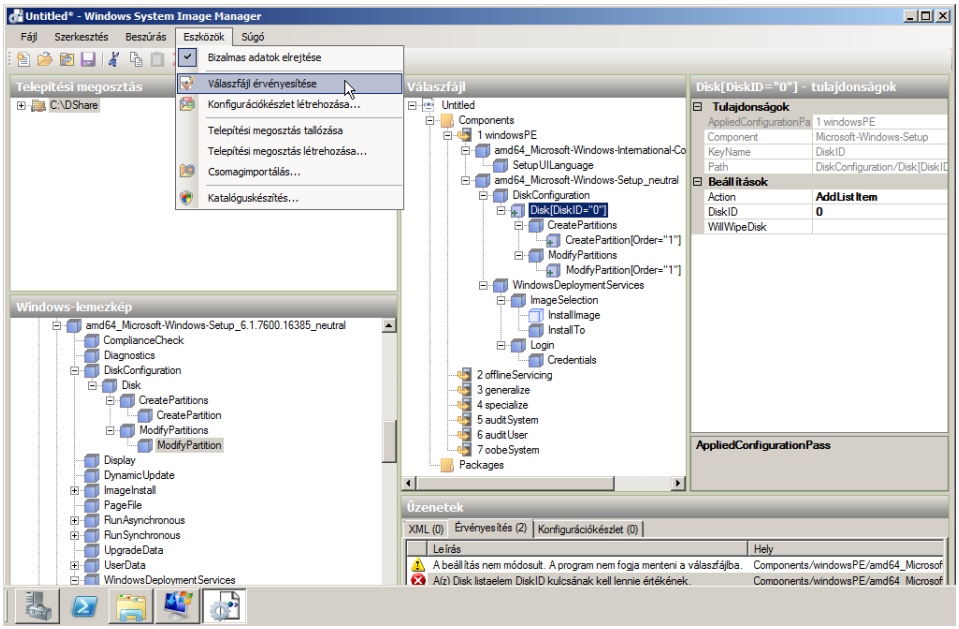


138. ábra: Partíció megadása

A **Windows-Setup\DiskConfiguration\ModifyPartitions** alatt található **ModifyPartition** a következő elem, amelyet a válaszfájlhoz kell adni a szokásos módon, és a következő beállításokat kell megadni. A partíció **aktív** státusza (Active) legyen **igaz** (true), a **formátum** (Format) **NTFS**, a **címke** (Label) például **Windows**, a **meghajtó betűjele** (Letter) **C**, a **sorrend** (Order) és a **partíció azonosító** (PartitionID) is legyen **1**.

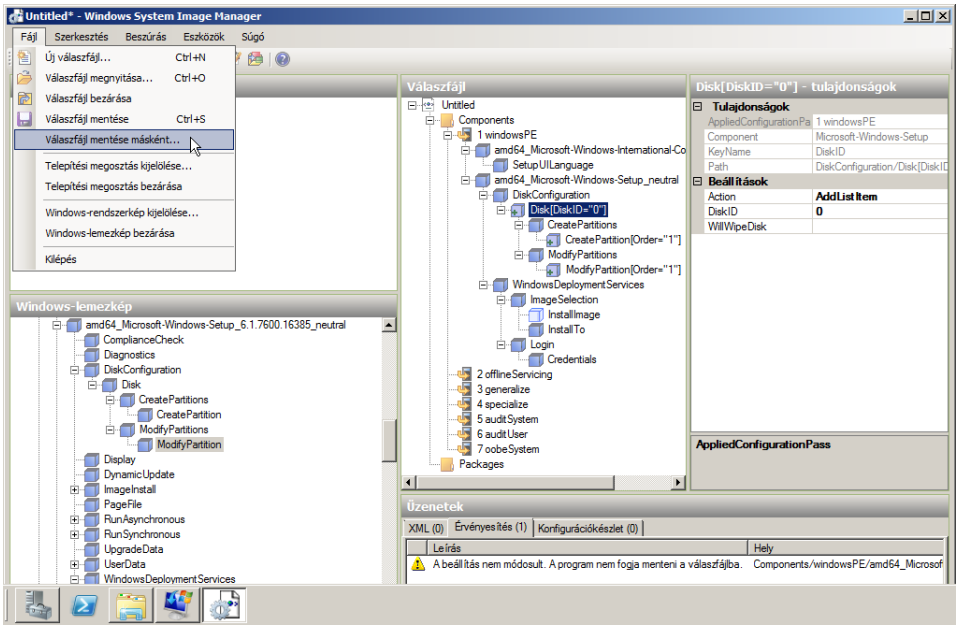
Hogy a telepítés közben a telepítő ne kérdezzen rá a választandó telepítési lemezképre, be kell azt állítani a válaszfájlba. Ezt a lehetőséget a **Microsoft-**

Windows-Setup\WindowsDeploymentServices alatt az **ImageSelection** jobb gombbal kijelölve, majd a beállítás hozzáadása: **1. fázist** választva lehet megtenni. Az **ImageSelection** alatt megjelenő **InstallImage beállításai** (Settings) közül mind a hármat meg kell adni. A **Filename** legyen **install.wim**, az **ImageGroup** a WDS-ben megadott telepítési képfájlok csoportjai közül az, amelyikben az aktuális telepítési képfájl található (ebben az esetben Win7x64), az **ImageName** pedig a telepítési lemezkép neve (ebben az esetben Windows 7 ENTERPRISE).



139. ábra: Válaszfájl érvényesítése

Ezzel elkészült a WDS kliens válaszfájl, már csak érvényesíteni kell, valamint elmenteni. Ehhez az eszközök menüből ki kell választani a **válaszfájl érvényesítése** (Validate Answer File) menüpontot. Ha ezek után az **üzenetek** (Messages) ablakban nem jelenik meg hibaüzenet, akkor a fájl menthető és használható. A mentéshez a fájl menüből a **mentés másként** (Save as) menüpontra kattintva megadható a fájl neve és helye. A fájl neve legyen **WDSClientUnattend.xml**, a helye pedig legyen a WDS távtelepítési mappájában található **WDSClientUnattend** mappa.
(Ebben az esetben C:\RemoteInstall\WDSClientUnattend.)



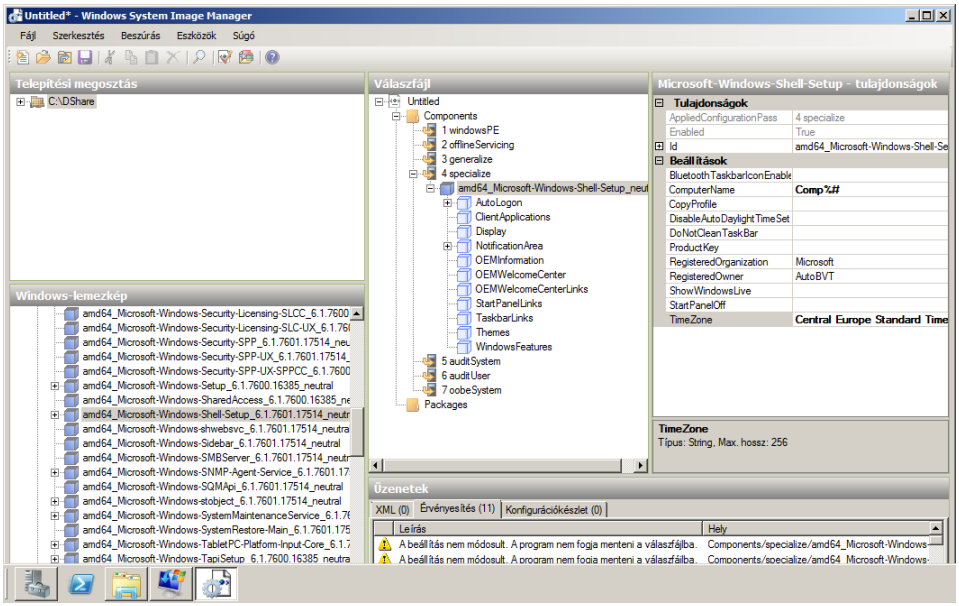
140. ábra: Válaszfájl mentése

Az abszolút beavatkozásmentes telepítéshez a második, telepítés utáni beállítások válaszfájlját is érdemes létrehozni. Ezeket a beállításokat **kezdőélmény** (Out-Of-Box Experience – OOBE) beállításoknak nevezi a gyártó. Az **OOBE** beállítások közül a következőket szükséges mindenképpen megadni az automatizált telepítéshez:

- A telepített **számítógép neve** és **időzónája**.
- A **licenszszerződés** (End User Licenc Agreement – EULA) elfogadásának kihagyása, valamint a hálózati kapcsolat típusának megadása.
- Egy a rendszerbe beléptethető **felhasználói fiókot**, **felhasználó névvel** és **jelszóval**.

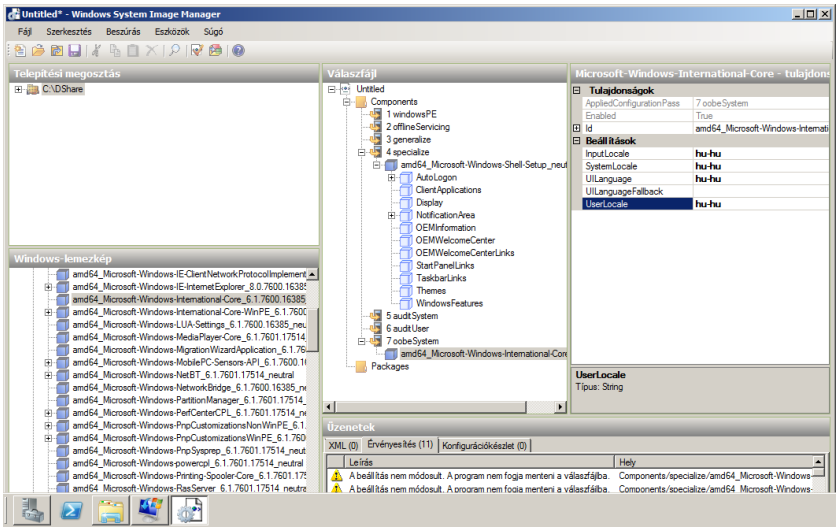
A beállításokhoz először is a **fájl** (File) menüből ki kell választani az **új válaszfájl** (New Answer File) menüpontot, ezzel együtt a már meglévő válaszfájlt, ha még nincs mentve a legutolsó állapot, akkor érdemes elmenteni. Következő lépésként ismét a **windows-lemezkép** (Windows Image) ablakban az előzőekben leírt ismertek szerint ki kell választani a **Microsoft-Windows-Shell-Setup** összetevőt az egér jobb gombjával és a megjelenő menüből a **beállítás hozzáadása: 4. fázis, specializálás (specialize)** (Add Setting to Pass 4 specialize) menüpontot választva hozzá kell adni az összetevő elemeit a válaszfájlhoz. (Termé-

szetesen itt is figyelni kell az összetevő előtagjára, amely 32 bites rendszer esetén x86, 64 bites esetén, mint itt is: amd64.)



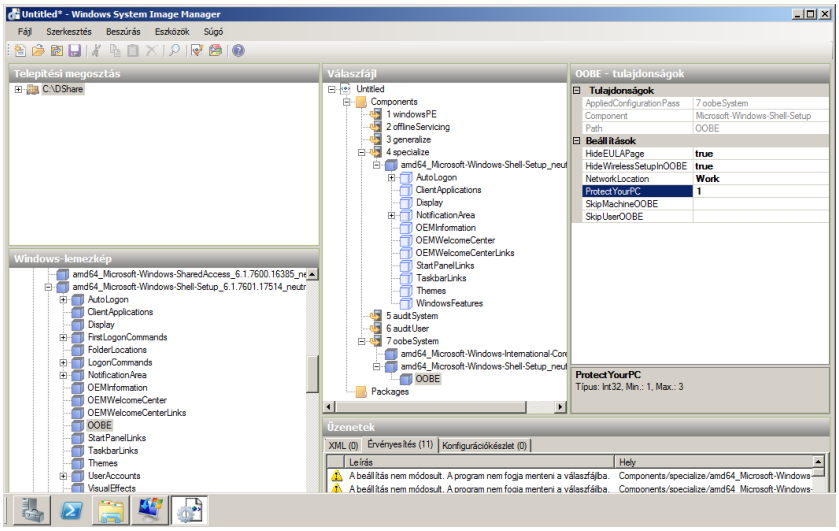
141. ábra: Számítógépnév és időzóna beállítások

A jobb oldali **tulajdonságok** (Properties) ablakban a **beállítások** (Settings) szakaszban megadható **számítógép neve** (ComputerName) és az **időzóna** (TimeZone). A **számítógép nevénél**, amely (egyébként ha hosszabb 63 karakternél, akkor a 63. karakter utáni karakterek elvesznek) használható a **„*”** karakter amelynek segítségével véletlen nevet lehet generálni. Az **időzóna** mezőjébe ha magyar időről van szó, akkor a **„Central Europe Standard Time”**-ot kell megadni.



142. ábra: Nyelvi beállítások

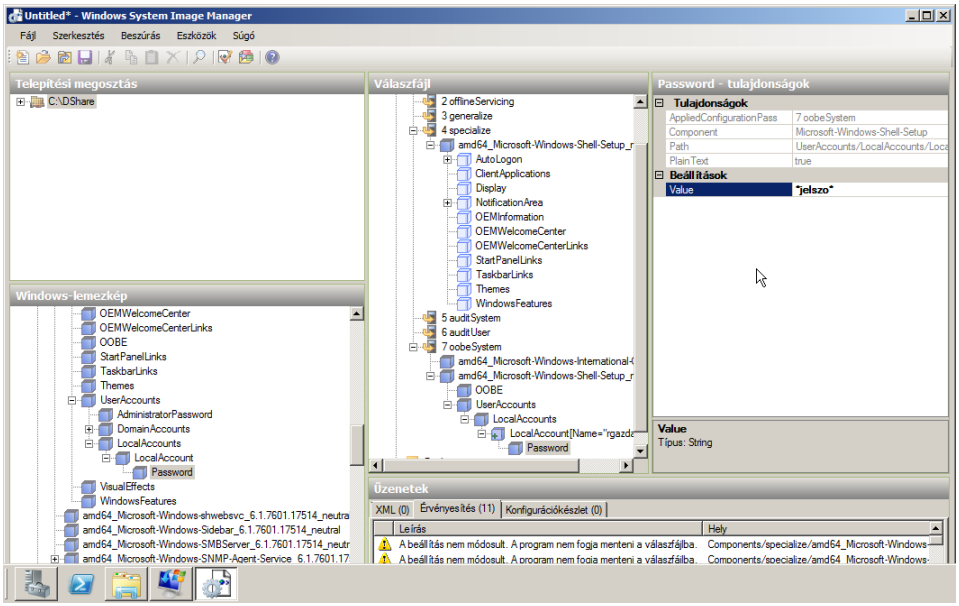
A következő összetevő, amelyet a válaszfájlhoz kell adni a **Microsoft-Windows-International-Core**. Erre jobb gombbal kattintva a 7. fázishoz adást kell választani (Add Setting to Pass 7 oobeSystem). Itt a UILanguageFallback mező kivételével mindhez be kell írni a nyelvi és helyi beállítást, amely itt most hu_hu (magyar).



143. ábra: Kezdőélménybeállítások

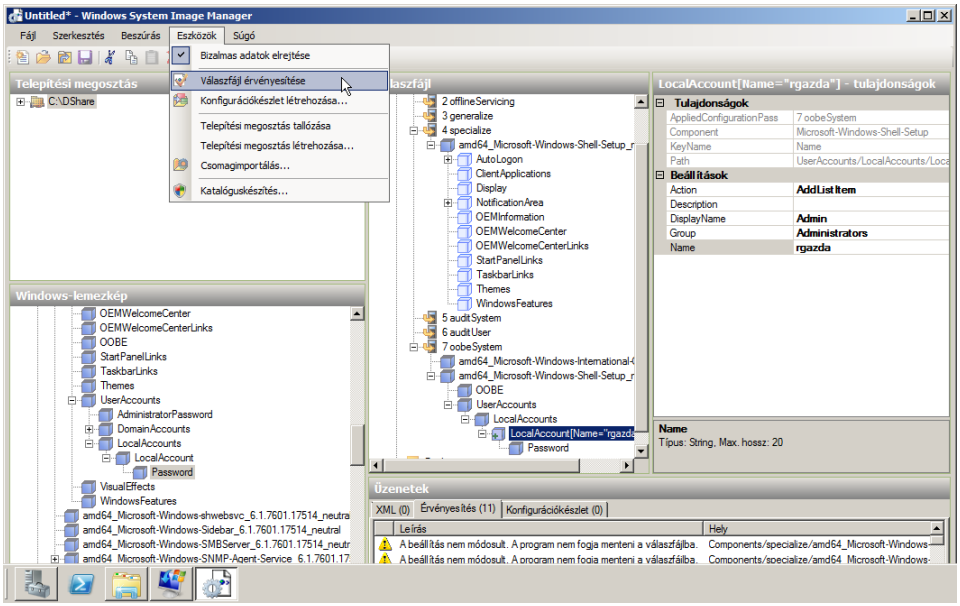
A **Microsoft-Windows-Shell-Setup** alatt az **OOBE** elemet kell kiválasztani és a válaszfájlhoz adni. Ehhez az elemhez tartozó beállítások a következők: **HideEULAPage** mező értéke legyen **igaz** (true), **HideWirelessSetupInOOBE** mező értéke legyen **igaz** (true), a **NetworkLocation** legyen **munkahelyi hálózat** (Work) a **ProtectYourPC** értéke pedig legyen **1**.

A **windows-lemezkép** (Windows Image) ablakban ugyanezen összetevő alatt a **UserAccounts/LocalAccounts/LocalAccount** alól ki kell választani a **Password** mezőt és hozzá kell adni a válaszfájl **7. fázisához**, az **oobeSystem**-hez. A **válaszfájl** (Answer File) ablakban ezek után a **LocalAccount** elemet kiválasztva a beállítások szakaszban meg kell adni a létrehozandó helyi **felhasználó nevét** (Name), **megjelenítési nevét** (DisplayName) és **csoportját** (Group).



144. ábra: Rendszergazdai felhasználó és jelszó beállítása

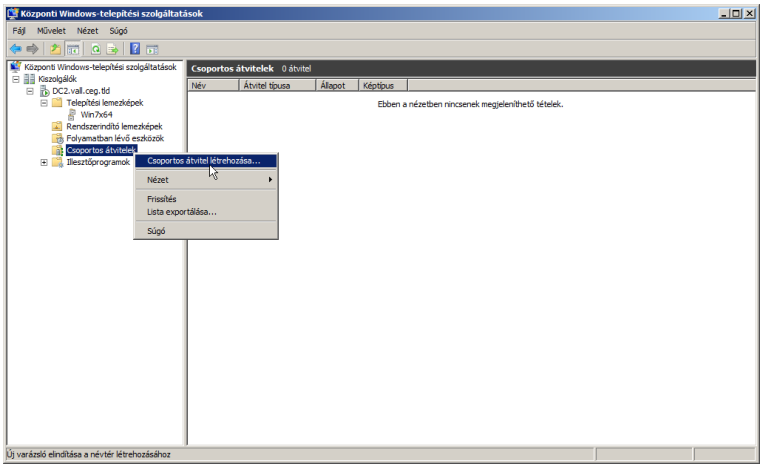
Fontos, hogy ebben az esetben figyelni kell a nyelvi verziókra. Azaz pl. magyar Windows 7 telepítése esetén, ha rendszergazdai jogokkal rendelkező felhasználóra van szükség, akkor a beépített csoport nevének (Group) Rendszergazdák csoportot kell megadni és nem az Administrators csoportot, mint az angol nyelvű verzió esetén.



145. ábra: A válaszfájl érvényesítése

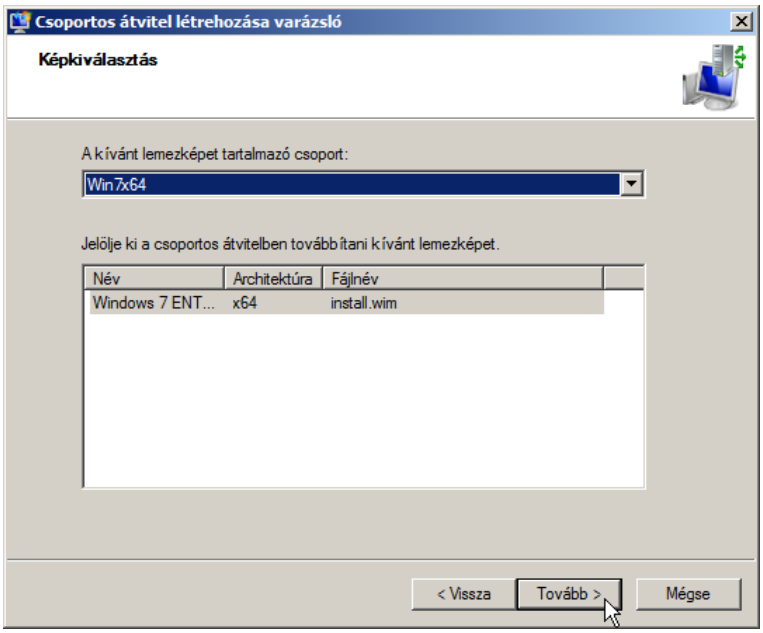
Ezek után már csak **érvényesíteni** kell a **válaszfájlt** (Validate Answer File) az **eszközök** (Tools) menüből és ha az **üzenetek** (Messages) ablakban nem jelez hibát a program, akkor ezt a válaszfájlt is el kell menteni a **fájl** (File) menü **mentés másként** (Save as) menüpontjával **OOBEUnattend.xml** néven, ugyanarra a helyre, mint a **WDSClientUnattend.xml** fájlt.
(C:\RemoteInstall\WDSClientUnattend)

A tömeges telepítés megkezdése előtt már csak annyi teendő van, hogy a válaszfájlokat hozzá kell rendelni a telepítendő lemezképekhez, illetve ha csoportos átvitellel lesz a telepítendő számítógépekre elküldve a telepítési lemezkép, akkor ehhez a folyamathoz egy csoportos átvitelt kell létrehozni és beállítani.



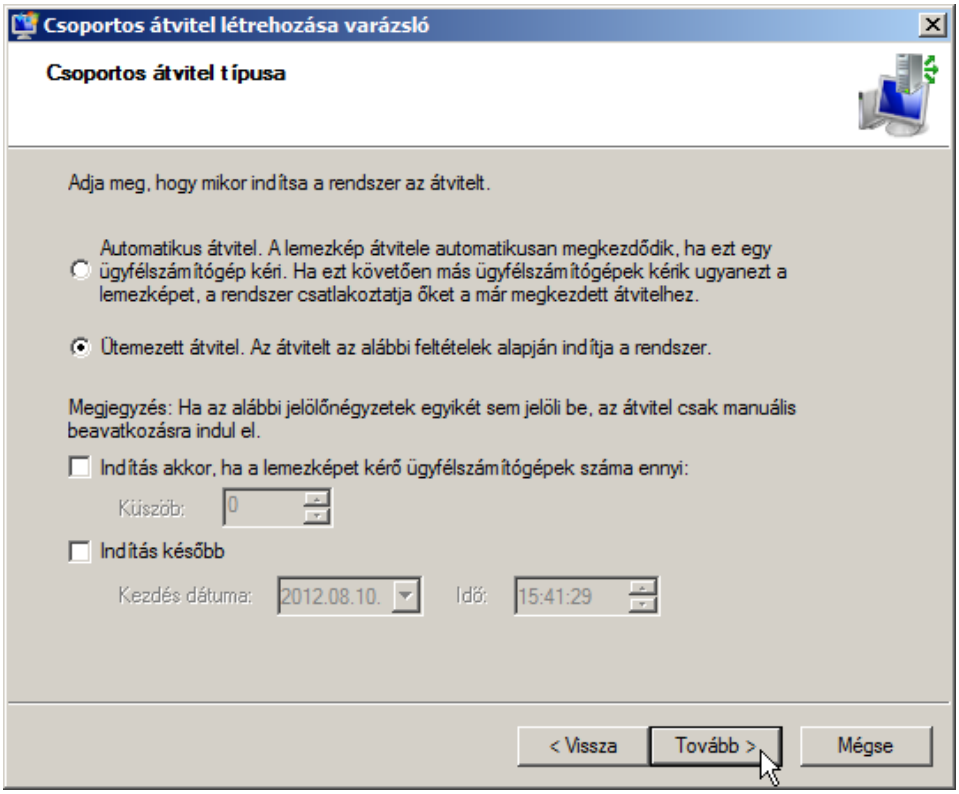
146. ábra: Csoportos átvitel létrehozása

Ez utóbbihoz a WDS konzoljában a **csoportos átvitelre** (Multicast Transmissions) jobb gombbal kattintva a **csoportos átvitel létrehozása** (Create Multicast Transmisson) menüpontot választva elindul a **csoportos átvitel hozzáadása** varázsló (Create Multicast Transmisson), amelyben elsőként az átvitelnek kell egy nevet választani. (Ebben az esetben ez a csWin7x64.)



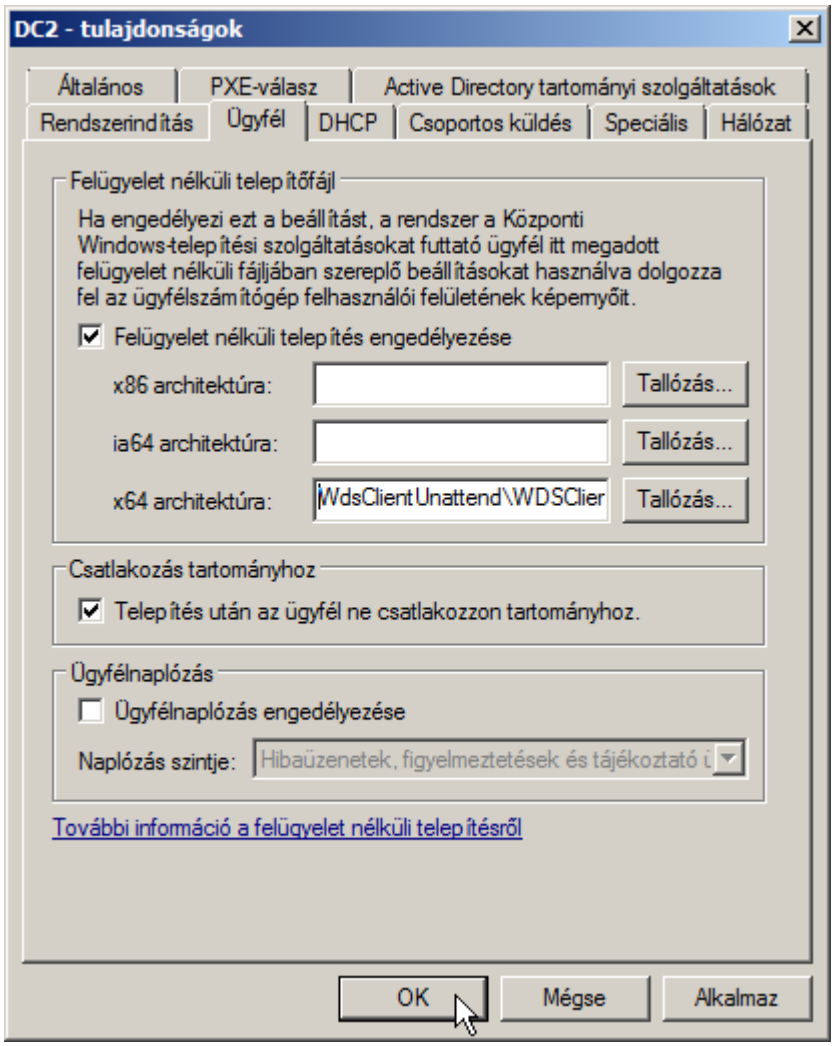
147. ábra: Lemezkép kiválasztása

A **tovább** (Next) gombra kattintva egy listából kiválasztható a már korábban telepített lemezkép csoport, azon belül pedig a telepítendő lemezkép. **Tovább** lépve a következő párbeszéd ablakra ki lehet választani, hogy a telepítés hogy induljon el. Ez azért fontos, mert egyszerre több számítógép indításának összehangolása nem egyszerű feladat, ha pedig teljesen már időben töltődik rájuk a telepítési lemezkép, akkor nincs értelme csoportos átvitelt használni.



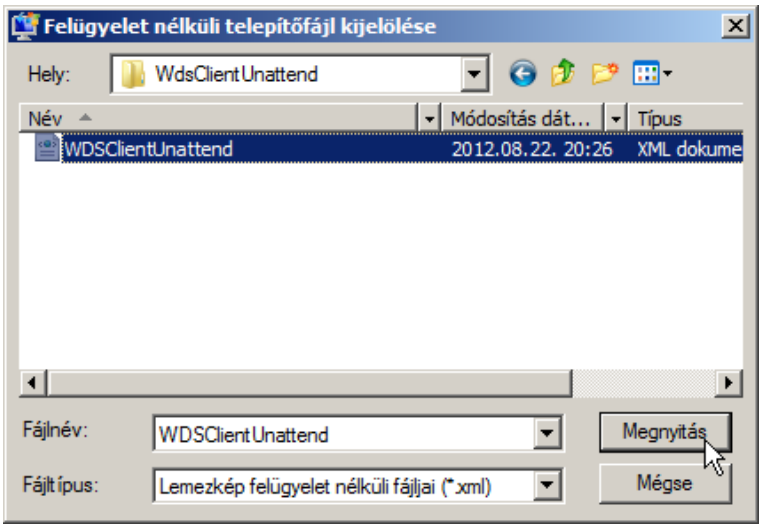
148. ábra: Átvitel típusának megadása

Éppen ezért itt választani lehet az **automatikus átvitel** (Auto-Cast), illetve az **ütemezett átvitel** (Scheduled-Cast) között. Az ütemezett átvitelnél olyan további beállítások lehetnek, mint a megfelelő kliens számítógép létszám elérési **küszöbe** (Threshold), vagy az **indítás** konkrét **időpontjának** (Start date) megadása. Az ütemezett átvitel választásánál, ha az utóbb említett két lehetőség egyike sincs kiválasztva, akkor a telepítés folyamata csak a rendszergazda kézi beavatkozására fog elindulni. A **befejezés** (Finish) gombra kattintva a csoportos átvitel létrejön.



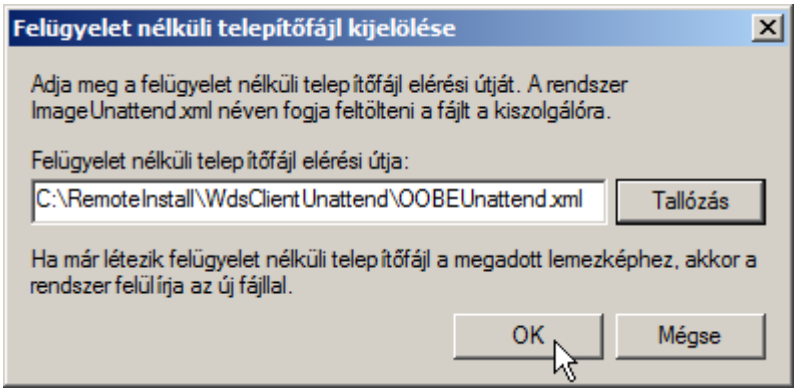
149. ábra: A felügyelet nélküli telepítés engedélyezése

A **WDSClientUnattend.xml** válaszfájl lemezképhez rendeléséhez a kiszolgáló kezelőben a WDS kiszolgáló nevére jobb gombbal kattintva ki kell választani a **tulajdonságok** (Properties) menüpontot. A megjelenő tulajdonságlapon az **ügyfél** (Client) fülön be kell kapcsolni a **felügyelet nélküli telepítés engedélyezését** (Enable unattended installation) és a választott architektúra melletti **tallózás** (Browse) gombra kell kattintani. (Ebben az esetben az x64 melletti gombra.)



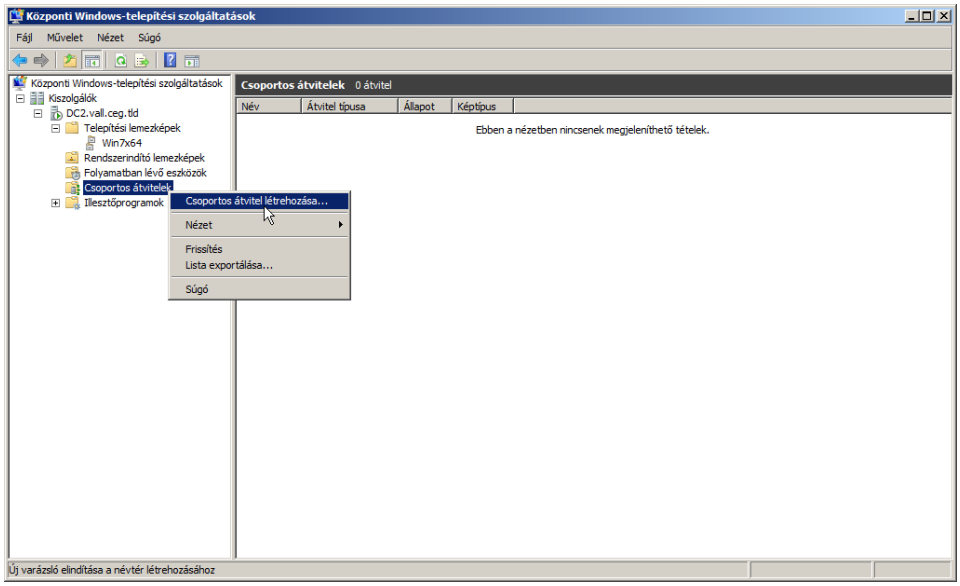
150. ábra: A válaszfájl megadása

A párbeszédablakban meg kell keresni és ki kell jelölni a fájlrendszerben a **WDSClientUnattend.xml** válaszfájlt, majd a **megnyitás** (Open) gombra kell kattintani. (A C:\RemoteInstall\WDSClientUnattend\ mappában van.) Mivel ez a válaszfájl csak architektúránként lehet más és más, könnyű kitalálni, hogy gyakorlatilag a rendszerindítási lemezképekhez lehet ezzel a művelettel hozzárendelni. Ugyanezen a tulajdonságlapon található a **csatlakozás tartományhoz** (Joining a Domain) szakasz, melynek kapcsolóját bekapcsolva a telepítés után a telepített számítógép nem lesz automatikusan a tartomány tagja. (Ebben az esetben be van kapcsolva.) A művelet végén az **Alkalmaz** (Apply) vagy az **OK** gombra kell kattintani.



151. ábra: A felügyelet nélküli kezdőélmény (OOBE) telepítőfájl

Az **OOBEUnattend.xml** válaszfájl, azaz a kezdőélmény beállításai már telepítési lemezképenként eltérő lehet. A lemezképhez rendeléshez a telepítési lemezképek közül ki kell választani a megfelelőt jobb gombbal, a megjelenő menüből pedig ki kell választani a **tulajdonságok** (Properties) menüpontot. A megjelenő adatlap alján be kell kapcsolni a **lemezkép felügyelet nélküli módban való telepítésének engedélyezését** (Allow image to install in unattended mode) és a **fájl kiválasztása** (Select File) gombra majd a **tallózás** (Browse) gombra kattintva meg kell keresni és ki kell választani az **OOBEUnattend.xml** válaszfájlt. (A C:\RemoteInstall\WDSClientUnattend\ mappában van.) A művelet végén fontos, hogy a tulajdonságlapon az **OK** gombot meg kell nyomni. Ezek után kezdődhet is a tömeges telepítés.

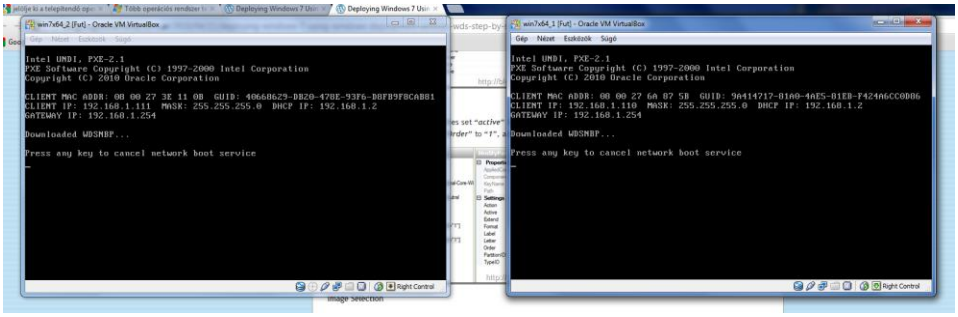


152. ábra: Lemezképhez rendelve

9.2.5 Tömeges telepítés WDS segítségével

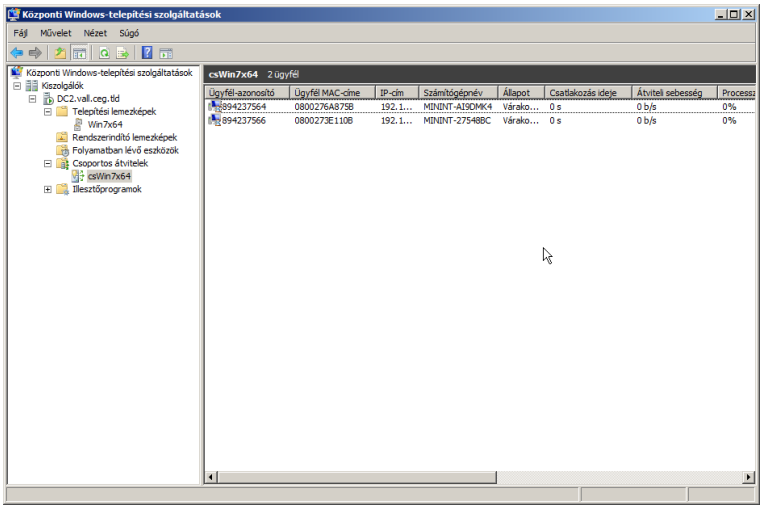
A telepítendő számítógépek indításánál arra kell odafigyelni, hogy mindenképpen hálózatról induljanak. Ez múlhat az **indítási sorrenden** (Boot Order), de azon is, hogy a WDS kiszolgáló tulajdonságlapjának **rendszerindítás** (Boot) lapján milyen PXE házirend van beállítva az ismert és ismeretlen ügyfelek esetében. Mindként esetben az az alapértelmezés, hogy miután a kliens megkapja IP beállításait a DHCP kiszolgálótól a folytatáshoz meg kell nyomni az **F12**-t. A másik két beállítási lehetőség egyike, hogy nem szükséges beavatkozás a folytatás-

hoz, a másik pedig hogy az automatikus folytatást meg lehessen szakítani az **ESC** billentyűvel.



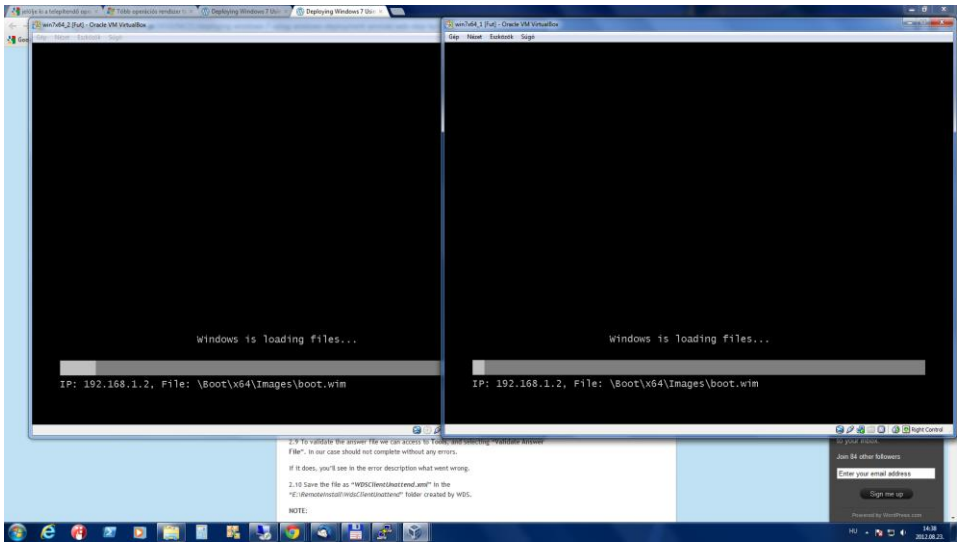
153. ábra: PXE boot az összes kliensen

- Természetesen feltétel a PXE indítás lehetőségével rendelkező Windows 7 kompatibilis hálózati interfész is, valamint hogy a meghajtó program elérhető legyen a telepítési lemezképben. Ellenkező esetben az illesztőprogramok mappában hozzá kell adni a kérdéses meghajtó programot a rendszerindítási lemezképhez, de lehetőség van ún. felderítő lemezkép (Discovery Image) létrehozására is, amelyet lemezre írva, vagy megfelelően egy pendrive-ra másolva, arról lehet indítani a telepítendő klienst. Ilyenkor a felderítő lemezkép az indítás után felderíti a hálózatban a WDS kiszolgálót és hozzácsatlakozik.



154. ábra: Várakoznak a kliensek

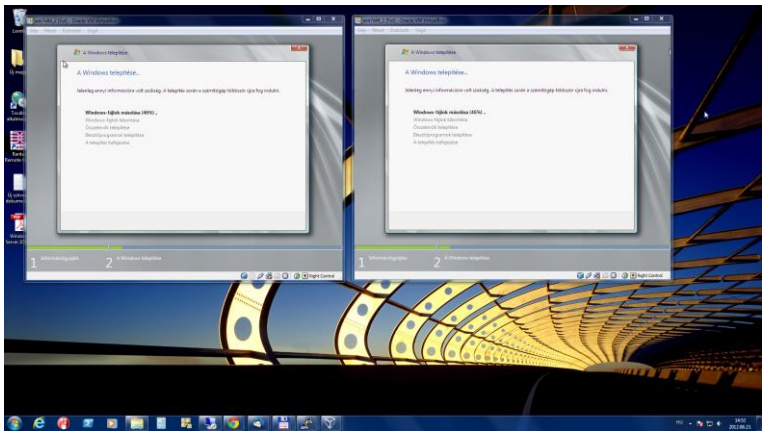
A telepítendő számítógépek megfelelő beállítás esetén megkapják IP beállításaikat a DHCP kiszolgálótól és a WDS **rendszerindítási** (Boot) tulajdonságaitól függően **F12**-es beavatkozással vagy anélkül a TFTP kiszolgálóról letöltik az architektúrának megfelelő rendszerindítási lemezképet. A letöltés után el is indítják a Windows előtelepítési környezetet (WindowsPE) és a WDS klienst, a telepítőt.



155. ábra: Indul a telepítő

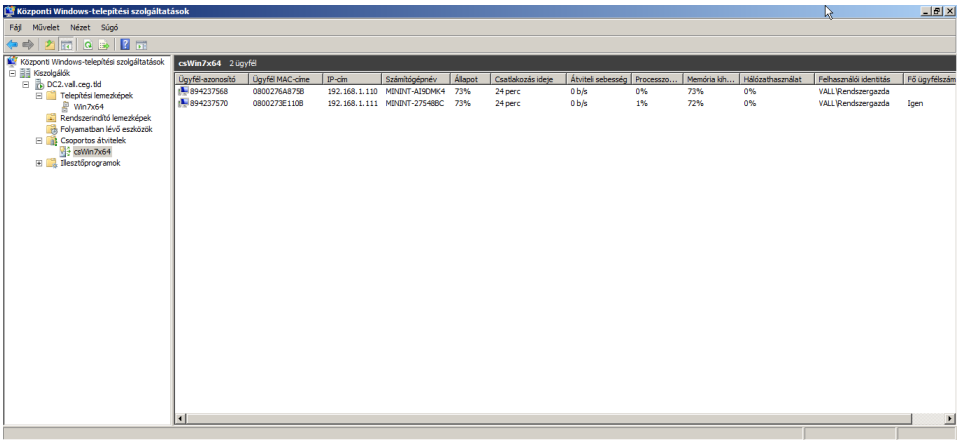
Az indulás utáni első lépésként a WDS kiszolgálón létrehozott csoportos átvitel beállításaitól függően (ütemezett, automatikus vagy kézi) várakozik a kiszolgálóra, majd elindul a telepítés.

Természetesen, ha jók a válaszfájlok, akkor közbeavatkozásra egyáltalán nem lesz szükség. A telepítő legalább egyszer újraindul, de előfordulhat, hogy többször is. Erre azért kell figyelni, mert ha az újraindítás után automatikusan megint hálózatról indul a számítógép, akkor a telepítés nem tud folytatódni. Többféle variációja is létezhet a megfelelő beállításoknak, és mindig az adott helyzethez leginkább illeszkedőt kell választani.

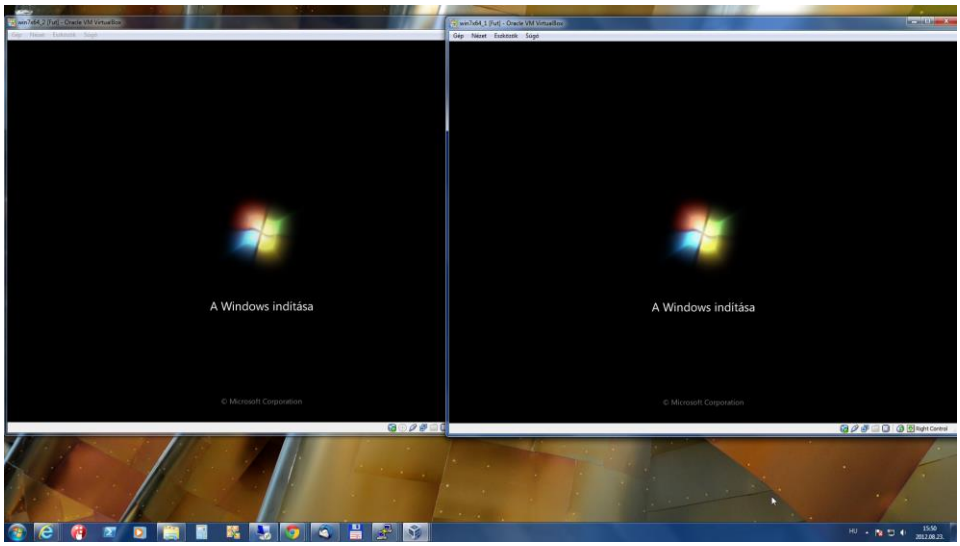


156. ábra: Fut a telepítő

- Az egyik szerint pl. teljesen új, üres (partícionálatlan) diszkekkel rendelkező számítógépek esetén az indítási sorrendben a merevlemez megelőzheti a hálózati indítást, hiszen amíg nincs rendszer a merevlemezen, addig úgyis a hálózatról fog megpróbálni elindulni. Ebben az esetben érdemes a rendszerindítás tulajdonságainál az alapértelmezettet (F12-re folytatódik a PXE indítás) megváltoztatni mondjuk arra, hogy automatikusan folytatódjon a hálózati indítás, kivéve ha az ESC billentyű lenyomásra kerül, így a gépek indításánál sem kell közbeavatkozni, elég lesz csak őket bekapcsolni. (Vagy ami még hatásosabb lehet, hálózaton keresztül felébreszteni őket a Wake On Lan funkcióval, egy megfelelő program segítségével.)



157. ábra: A futás nyomonkövetése a szerveren



158. ábra: Először indulnak a frissen telepített windowsok

9.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

9.3.1 Összefoglalás

Ebben a leckében a vállalati környezetben végezhető és végzendő feladatok kerültek ismertetésre. A vállalati környezet jellemzői közé tartozik, hogy sok, homogén, vagy kisebb homogén csoportokból álló kliens számítógép alkotja, amelyeknek hardver és szoftverkörnyezete egységesen, és ez által központosítottan is könnyen kezelhető. A központosítottan ellátható feladatok közül itt a számítógépek telepítésének különböző módszerei kerültek tárgyalásra.

A Windows Server 2008 megoldása a központosított telepítések elvégzésére a központi Windows-telepítési szolgáltatások (WDS). A WDS telepítése és konfigurálása egyszerű, főleg ha a hálózatban található DNS és DHCP szerverek Windows kiszolgálókon működő natív Windows-os kiszolgálók.

A WDS segítséget nyújt a hálózaton keresztül történő számítógép telepítésekben. A legegyszerűbb megoldás a számítógépek hálózaton keresztüli indítása, hiszen ezzel elhárul a számítógépek helyszínére történő kiszállás problémája, ehhez viszont a számítógépek hálózati interfészének támogatnia kell a PXE hálózati indítást. A telepítéshez több dolog is szükséges, de elsősorban egy olyan telepítési lemezképfájlra van szükség, amely tartalmazza az operációs rendszert, a telepítendő számítógép hardverelemeinek meghajtóprogramját, és esetlegesen felhasználói programok telepítőkészletei is részei lehetnek.

Az egyszerre több számítógép telepítését tömeges telepítésnek nevezik. Ennek egyik feltétele az eddig ismerteteken túl, hogy a kiszolgáló és a hálózat támogassa a csoportos átvitelt, valamint hogy a telepítő programok kérdéseit ne kelljen a helyszínen „megválaszolnia” egy felhasználónak. Ez utóbbi kiküszöbölésére való a válaszfájl, melynek segítségével, adott számítógépekre lehet szabni a telepítés során feltett kérdéseket. Ezeknek a kérdéseknek a válaszfájl által megadott válaszai között, olyan kérdések is lehetnek, hogy a telepítő és az operációs rendszer nyelvi beállításai, hálózati beállítások, alapértelmezett felhasználók beállításai.

9.3.2 Önellenőrző kérdések

1. Melyek a vállalati informatikai infrastruktúra fő jellemzői?
2. Melyek a központosított számítógép-kezelés előnyei?
3. Mi a WDS és mire jó?
4. Ismertesse a WDS konfigurációjának főbb lépéseit!
5. Mi a távtelepítés? Melyek az előnyei?
6. Mire jó a csoportos átvitel?
7. Mi a WAIK?
8. Mire jó a válaszfájl? Milyen fajtái vannak?
9. Mire kell odafigyelni tömeges telepítés esetén?

10 ÜZEMELTETÉS, MONITOROZÁS, MOBIL INFORMATIKA

10.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Ebben a leckében a számítógép rendszerek és az azokat alkotó számítógépek üzemeltetésével kapcsolatos tudnivalók kerülnek ismertetésre. Bemutatásra kerülnek a rendszergazda munkáját megkönnyítő olyan eszközök, alkalmazások, programok, mint az eseménynapló, a teljesítményfigyelő, vagy az erőforrás-figyelő.

A lecke második részében néhány mobil informatikai tudnivaló kerül ismertetésre, amely nagy segítség lehet a vállalati rendszerben mobil-eszközét is használni akaró felhasználónak.

A tananyag elsajátítása után a hallgató képes lesz hálózatba szervezett számítógépek olyan üzemeletetési feladatainak ellátására, mint az eseménynaplók vizsgálata, a teljesítményfigyelő vagy az erőforrás-figyelő használata, és ezek segítségével képes lesz különböző hibák felderítésére és elhárítására.

A lecke második részének áttanulmányozása után a hallgató képes lesz Windows mobil eszközének használatára vállalati környezetben.

10.2 TANANYAG

10.2.1 Az üzemeltetés általános feladatai

A szájhagyomány szerint az informatikusokat azért nem szokták túldicsérni, mert ha jól dolgoznak, akkor gyakorlatilag észrevehetetlen a munkájuk és csak akkor van rájuk szükség, ha előbukkan valamilyen hiba. Ez részben igaz, azonban rengeteg olyan feladat van, amely a normál üzemmenet megkövetel. Ezeknek egyik nagy csoportja a karbantartási munkák, amellyel majd a következő lecke foglalkozik.

Az üzemeltetési feladatok másik nagy csoportját meghatározni nem is olyan egyszerű feladat. Ide tartozik ugyanis minden olyan feladat, amely az informatikai rendszer használata során felmerül a felhasználó adminisztrációtól, vagy a hozzáférésvezérléstől kezdve a különböző új szoftverek telepítésén, vagy a meglevő szoftverek (az operációs rendszert is beleértve) a mindig változó igényekhez történő beállításán keresztül egészen a felhasználók szűnni nem

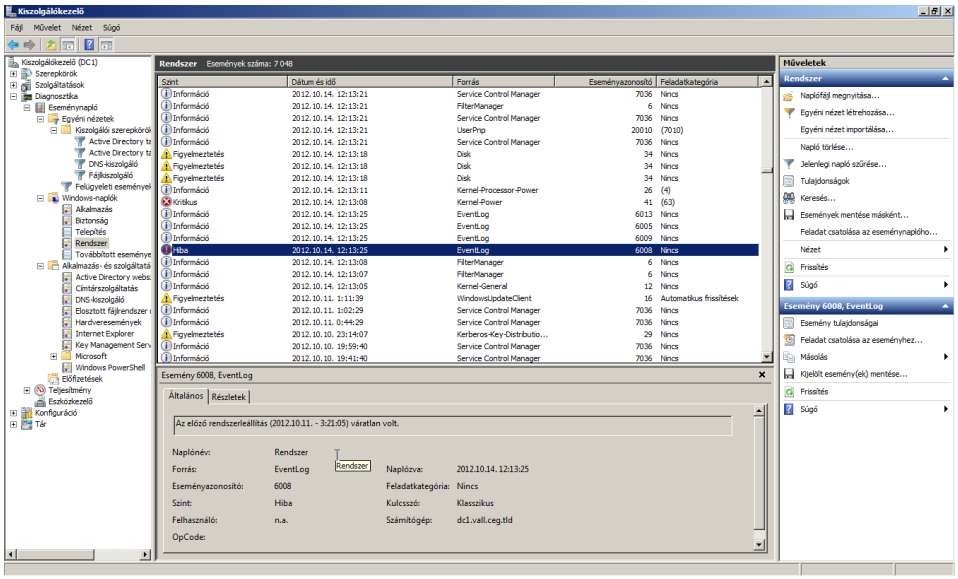
akaró problémáinak kezeléséig. Látható tehát, hogy nem egyszerű az üzemeltetést végző személyzet feladat, ha mindezekkel meg akar birkózni.

A tervezhető elvégzendő feladatok jórésze tulajdonképpen már ismertetésre került korábbi leckékben (pl. felhasználói adminisztráció, hozzáférésvezérlés, telepítések stb.), azonban még jócskán vannak olyan feladatok, amelyeket üzemeltetés címén meg kell tenni. Ilyen feladatok például a különböző erőforrások és események figyelése (pl. a merevlemezeken a szabad hely, a processzor vagy a memória kihasználtságának, a különböző **események** (Events) vagy a felhasználók tevékenységének figyelése), az újonnan telepített programok, vagy új beállítások tesztelése, ez utóbbiak természetesen nem az éles, hanem egy erre a célra beállított teszt szerveren.

Látható, hogy a karbantartási feladatok kivételével a feladatok nagy része különböző dolgok figyelésén alapul. Itt kell megemlíteni a különböző figyelő szolgáltatásokat, mint a teljesítményfigyelő, vagy az erőforrás-figyelő. Azonban az üzemeltető legnagyobb segítsége az üzemeltetéshez kapcsolódó figyelésben a **rendszernaplózás** (System Logging) szolgáltatás, amelynek feladata a különböző események, tevékenységek naplózása. A naplókhoz az eseménynapló alkalmazáson keresztül lehet hozzáférni, amely felügyeleti konzol beépülő modulként (MMC Snap-in) a kiszolgálókezelőben is megtalálható.

10.2.2 Az eseménynapló

Egy rendszerben elengedhetetlen a különböző események rögzítése. Elég, ha csak a hibakeresésre gondol az ember, már a hibát is könnyebben határolhatja be a rendszergazda, ha a feljegyzett események között böngész. Hogy melyek legyenek a feljegyzett események, a rendszer beállításaitól függ, de egészen olyan mélységig is el lehet menni, mint a felhasználók be- és kijelentkezése a rendszerbe, jelszóváltoztatás időpontja, illetve hogy mikor élt bizonyos jogaival. De nem csak a felhasználókra vonatkozó események kerülhetnek rögzítésre. Ha pl. egy szolgáltatás vagy illesztőprogram nem indul el, vagy az operációs rendszer működése közben valamilyen hiba történik, és ez az esemény nem kerülne rögzítésre, akkor a rendszergazda nagy bajban lenne a hiba felderítésével és kijavításával kapcsolatban.



159. ábra: Hibajelzés az eseménynapló rendszernaplójában

Előfordulhat, hogy egy hálózati kártya pl. megszakítások ütközése miatt nem indítható el. Ilyenkor semelyik tőle függő szolgáltatás nem fog megfelelően működni. Ebben a példában ez az összes hálózati szolgáltatást érinti, azaz nem lehet a kiszolgálót a hálózaton elérni, a számítógépet nem fog látszani a hálózat többi számítógépéről és a címtárszolgáltatás sem lesz elérhető.

A Windows Server 2008 az események rögzítésére ún. eseménynaplókat használ, melyekbe különféle eseményeket jegyez fel a rendszerindításával és leállításával kapcsolatos problémás eseményektől kezdve egészen a felhasználó által végzett egyes műveletek rögzítéséig. Az események különböző szintűek lehetnek, attól függően, hogy mennyire kritikusak a rendszer működésével kapcsolatban. Alapértelmezés szerint a rendszer három eseménynaplót használ, amely különböző alkalmazások telepítésével tovább bővülhet. A három napló a következő:

Rendszernapló (System log): ebben a naplóban kerülnek rögzítésre a teljes rendszerrel, illetve az egyes szolgáltatásokkal és illesztőprogramok indításával, működésével és leállításával kapcsolatos események. Itt az események három szintje kerül rögzítésre. Ezek a **hiba** (error), a **figyelmeztetés** (warning) és az **információ** (information). A **hiba** kritikus műveletek meghiúsulásáról vagy rendszerelemek működésképtelenségéről tájékoztat. A **figyelmeztetés** olyan hibajellegű esemény, amely az adott időpontban nem okoz adatvesztést vagy valami-

lyen rendszerfunkció kimaradását, de a későbbiekben vagy áttételesen ezt eredményezheti. Az **információ**, valamilyen művelet végrehajtásának sikeres eseménye.

Biztonságinapló (Security Log): felhasználók és programok műveleteinek eseményeit rögzíti. Ide sorolhatók azoknak az eseményeknek a naplózása, mint hogy a felhasználók vagy a programok megkíséreltek-e meghatározott műveleteket elvégezni, illetve az elvégzéshez rendelkeztek-e a megfelelő hozzáférési engedélyekkel. Kétféle szintű eseményt tartalmazhat. Az egyik a sikeres események naplózása (Success Audit), amely arról tájékoztat, hogy az adott felhasználó az adott műveletet sikeresen végrehajtotta, illetve rendelkezett hozzá a megfelelő jogosultsággal. A másik a sikertelen események naplózása (Failure Audit), amely jelzi, hogy a rendszer a megfelelő jogosultságok hiányában megtagadta a művelet elvégzését.

Alkalmazásnapló (Application Log): itt alkalmazások, kiszolgáló programok működésével kapcsolatos hibák, figyelmeztetések és információs bejegyzések kerülnek rögzítésre. A különböző programok ebbe a naplóba írhatják saját bejegyzéseiket, de a Windows számos összetevője is ebbe a naplóba dolgozik. A bejegyzett események szintjei megegyeznek a rendszernaplóban ismertetett esemény szintekkel.

Az eseménynaplók a Windows Server 2008 és Windows 7 rendszerekben az **eseménynapló** (Event Viewer) alkalmazással tekinthetők meg.

10.2.3 Az eseménynapló használata

Ahogy fentebb is említésre került, az eseménynaplók megtekintése, vizsgálata az **eseménynapló** (Event Viewer) programmal történik. A program a **start** menü **felügyeleti eszközök** (Administrative Tools) almenüjéből indítható, de elérhető a **vezérlőpultból** (Control Panel) és a **kiszolgálókezelőből** (Server Manager) és a **számítógép-kezelőből** (Computer Manager) is. Parancssorból az eventvwr.exe programmal indítható.

Az alkalmazás ablakának bal oldalán található konzolfán a megfelelő napló kiválasztásához a **Windows naplók** (Windows Logs) elem melletti háromszögre kell kattintani, majd a kívánt naplót ki kell választani.

160. ábra: Kritikus hibabejegyzés részletei

A megfelelő naplót kiválasztva a konzol közepén egy táblázat jelenik meg a naplóban található eseménybejegyzésekről. A táblázat oszlopai sorrendben a következők: **esemény szintje** (Level), **dátuma és ideje** (Date and time), **forrás** (Forrás), **eseményazonosító** (Event ID), **feladatkategória** (Category). Ezek közül az első három a legfontosabb, amelyek közül az időpont és a forrás nem került eddig még ismertetésre. Az időpont, az esemény időpontja, amikor az időpont történt. A megfelelő hibakereséshez és naplózáshoz elengedhetetlen a számítógép rendszerórájának pontos működése. A forrás annak az alkalmazásnak, szolgáltatásnak vagy egyéb rendszerösszetevőnek a megnevezése, amely az eseménybejegyzést generálta. A rendszernaplóban megtalálható bejegyzések nagy része pl. a **szolgáltatásvezérlő szolgáltatástól** (Service Control Manager) származik.

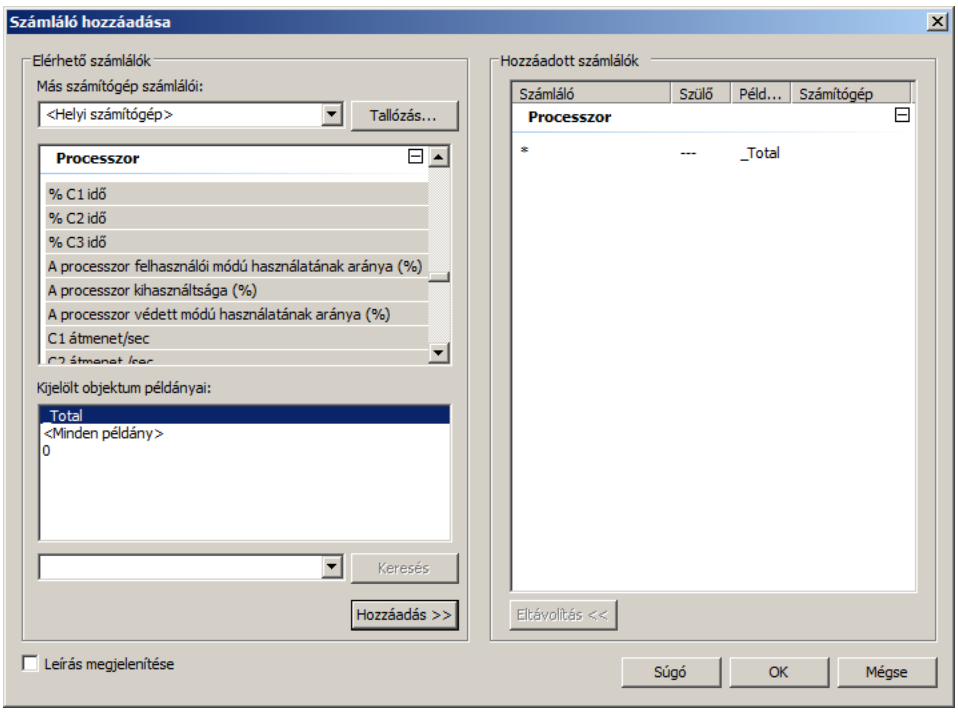
Az esemény bejegyzés részleteinek megjelenítéséhez az eseményre duplán kell kattintani. A megjelenő párbeszédablakban az általános lapon megjelennek az eseményhez kapcsoló adatok. További részletek a **részletek** fülre kattintva érhetőek el. A párbeszéd ablak jobb szélén található nyilakkal lépkedni lehet az események között a táblázatban látható sorrend alapján.

10.2.4 A teljesítmény megfigyelése

A kiszolgáló hatékony üzemeltetéséhez és a jövőbeni bővítések megtervezéséhez elengedhetetlen a működés ellenőrzése. Célszerű a kiszolgáló terhelésének rendszeres ellenőrizése és a változások figyelemmel kísérése. Az összegyűjtött adatok alapján a későbbiekben előre megbecsülhető lesz, hogy mikor jön el a hardver bővítésének ideje.

A teljesítményfigyelő

A működés, valamint a teljesítmény figyelése a **teljesítményfigyelő** (Performance Monitor) felügyeleti konzollal követhető nyomon, melyet az eseménynaplóhoz hasonlóan a start menü **felügyeleti eszközök** (Admimistrative Tools) menüjéből, vagy a vezérlőpult felügyeleti eszközök mappájából lehet indítani, de akár a **kiszolgáló kezelő** (Server Manager) **diagnosztika** (Diagnostics) konzol-részfájában a teljesítmény szakasz alatt, illetve a **számítógép-kezelő** (Computer Management) hasonló szakaszában is megtalálható.



161. ábra: Először hozzá kell adni a megfelelő számlálót

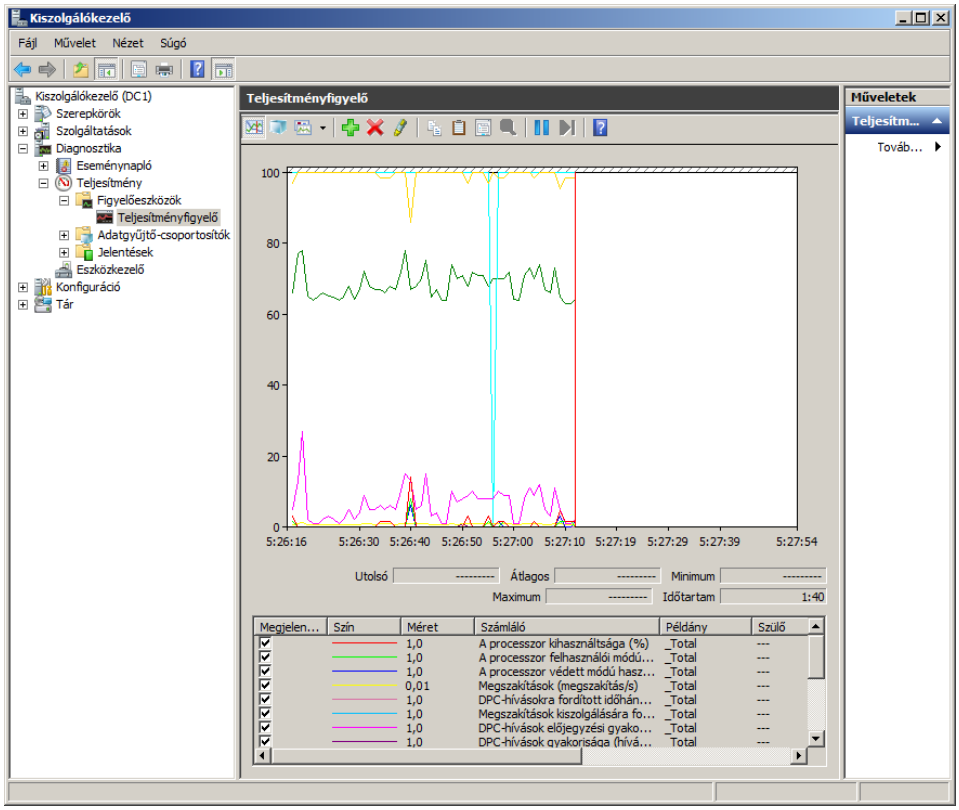
A **teljesítményfigyelő** grafikonon jeleníti meg a számítógép egyes alrendszereinek kihasználtságát. A program az ábrázolható objektumokat **számlálók-**

nak (Counter) hívja. Ezek közül a kategóriákba sorolt számlálók közül kell kiválasztani az ábrázolandó objektumokat (pl. CPU kihasználtság).

A számlálók kiválasztása és a grafikonhoz történő hozzáadása a következőképpen történik.

A grafikon felett található menüsorban a **+** jelű ikonra kell kattintani. A megjelenő **számláló hozzáadása** (Add Counters) ablakban, az **elérhető számlálók** (Available Counters) listájából ki kell választani a kívánt számálót, majd a hozzáadás gombra, majd az **OK** gombra kell kattintani.

Ha a szabad memóriát kell figyelni, akkor az elérhető számlálók közül a memória (Memory) kategória melletti nyílra kattintva a kategória tartalma kifejtése után a rendelkezésre álló memória (megabájt) (Available MBytes) sorra kell kattintani.

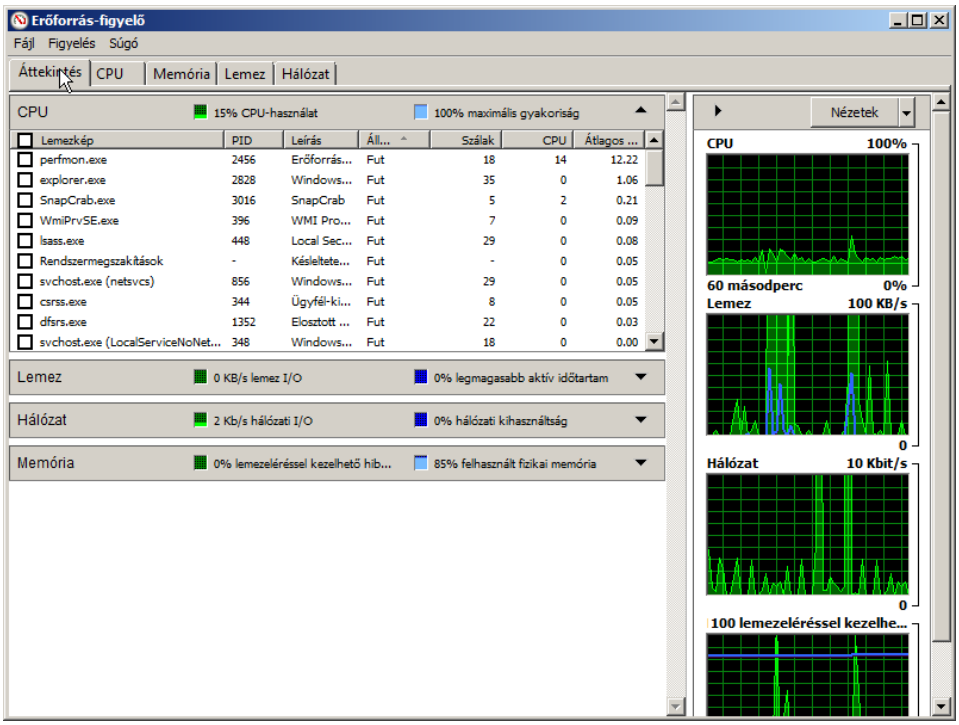


162. ábra: A hozzáadott számlálók értékének megjelenítése

Az erőforrás-figyelő és a megbízhatóság figyelő

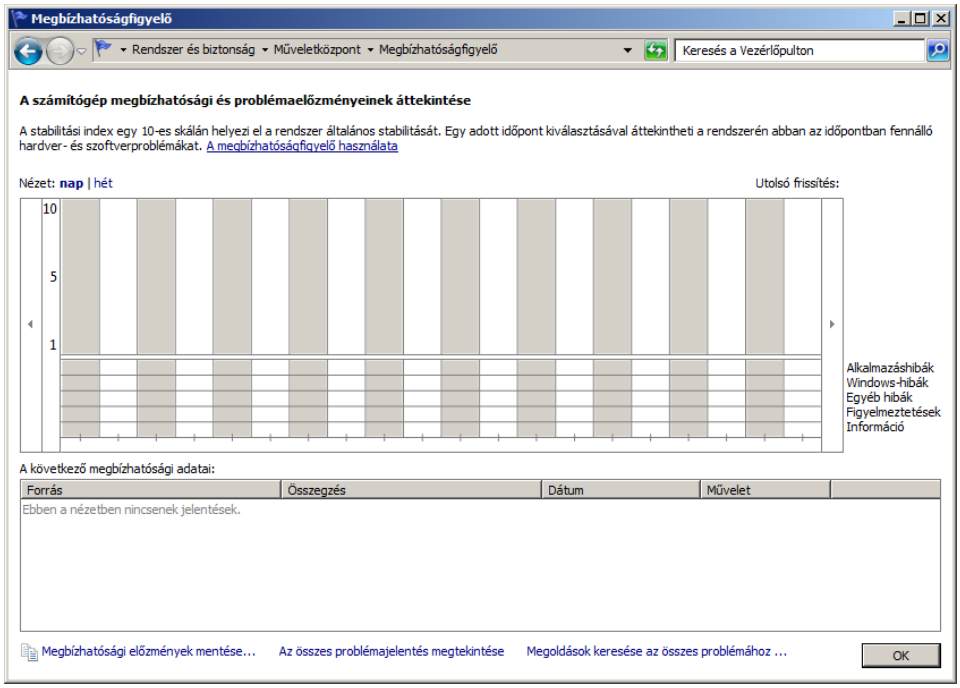
A másik figyelő eszköz a **start** menü, **minden program** (All Programs), **kellékek** (Accessories) menüpontjának **rendszereszközök** (System Tools) almenüjéből indítható az **erőforrás-figyelőre** (Resource Monitor) kattintva.

Az **erőforrás-figyelő** képernyőjén áttekinthetők az olyan erőforrások kihasználtsága, mint a processzor, a memória, a háttértár (lemez) vagy a hálózat. A szürke vízszintes sávokra kattintva megjelennek az erőforrásokat használó folyamatok.



163. ábra: Az erőforrásfigyelő

A **megbízhatóságfigyelő** (Reliability Monitor) egy a **vezérlőpultból** (Control Panel) elérhető eszköz, amely napokra lebontva mutatja meg a számítógépre telepített, illetve eltávolított programokat, valamint az alkalmazás és a hardverhibák előfordulását a számítógép telepítése óta. A megbízhatóságfigyelő régebben rész volt a teljesítményfigyelő rendszernek, azonban a Windows Server 2008 R2-ben már a **vezérlőpult** (Control Panel) **műveletközpontjából** (Action Center) indítható a karbantartás szakában a **megbízhatósági előzmények** (View reliability history) szövegre kattintva.



164. ábra: A megbízhatóságfigyelő

10.2.5 Mobilinformatika

A Microsoft – azon túlmenően, hogy asztali számítógépekre gyárt operációs rendszereket a nyolcvanas évek közepétől – a mobil eszközök piacán is jelen van már a kilencvenes évek elejétől. Azonban míg korábban, a kezdeti rendszereknél – mind desktop, mind mobil OS – oldalról a különféle eszközök szinkronizálása nem volt alapkövetelmény, a kétezres évek elejétől egészen napjainkig ez egyre nagyobb hangsúlyt kap.

Történeti áttekintés

Amikor 2001-ben megjelent a Windows XP, még nem számított alap tartozéknak szoftverei körében a mobil eszközök szinkronizációja. Pedig igény lett volna rá, főként mikor megjelentek az első igazi PDA-k (Personal Digital Assistant – Személyi Digitális Titkár) és okostelefonok, melyek Windows Mobile 2002-vel üzemeltek. Ezt a rendszert követte a Windows Mobile (WM) 2003, 2003SE majd a WM 5, 6, 6.5, 7, 7.5 és a 8.

Ahogy ezek a rendszerek kezdtek terjedni, és lehetővé vált a pocket outlookban a levelek elérése, a címjegyzék feltöltése, a naptárbejegyzések és különféle események rögzítése, a Microsoft rájött, hogy ezeket az asztalai gép-

pel szinkronizálva sokkal hatékonyabban lehet kezelni, elmenteni, konvertálni, felhasználni. Erre hozta létre az XP alá telepíthető Windows Mobile Eszközközpontot.

Az eszközközpont lényege, hogy segítségével a mobil készülék szinkronizálható az asztali (vagy notebook) géppel, egy ún. partnerségen keresztül. Kezdetben maximum 2 partnerség volt létrehozható, így maximum két asztali eszközön lehetett az adatokat szinkronizálni. Ezzel a szoftverrel vált lehetővé a programok és szolgáltatások szinkronizációja, a képek, videók, hang- és egyéb fájlok áttöltése a számítógépről az eszközre, illetve fordítva. Kapcsolódás szempontjából már az első programváltozatok is több lehetőséget kínáltak fel:

- infravörös porton át IR kapcsolat
- Bluetooth kapcsolat
- kábeles (USB vagy COM porton keresztüli) kapcsolat.

Egy másik fontos kérdés a mobilé eszközökkel kapcsolatban a különböző programok mobil eszközökre történő telepítése. Erre két lehetőség adódott:

Az egyik lehetőség, hogy a letöltött/létrehozott .cab kiterjesztésű fájlt rá kellett másolni az eszközre (vagy arra lett közvetlenül letöltve), majd futtatni kellett rajta, így a program települt.

A másik, hogy a Mobile-eszközközponton keresztül a mobilkészülék csatlakoztatása után az asztali gépen futtatni kellett egy exe fájlt, amely programként felkerül az asztali gépre és a mobil eszközre is. Innentől a program adatai szinkronizáltak mindkét eszközzel. Ha az asztali gépről törölve lett a program a mobil eszköz távollétében, a következő szinkronizálásnál a mobilról is törlődött az alkalmazás.

A Windows Vista megjelenését követően 2007-ben már az OS részeként jelen volt a Szinkronizáló Központ, de még mindig külön le kellett tölteni a program összetevőit. Sok mindenben nem változott funkcióját tekintve, hiszen akkoriban a legnagyobb elérhető WM eszköz 6.5-ös szoftverrel rendelkezett – és nem mellesleg már képes volt Exchange szerveren keresztül kommunikálni, így szinkronizálva az adatokat.

A mobilinformatika jelenlegi támogatása

Igazi változásról a Windows 7-nél sem lehet még beszélni, azonban a kezelőfelület már fejlődött. Egyszerűsödött az eszközfelismerés és csatlakoztatás, valamint a start menüben a kellékek (Accesories) menüpont alatt helyet kapott a Windows Mobilközpont (Windows Mobile Device Center) elnevezésű programcsomag. Ez már többet nyújt, mint elődei, mivel már nem csupán a kézi

eszközökre vonatkozik (PDA, mobiltelefon), hanem magára a notebookra is, így lehetőség van a laptop paramétereinek beállítására és a szinkronizálás beállítására külső eszközzel.

165. ábra: A Windows Mobil-eszközközpont

A Windows Server 2008 hasznos szolgáltatása hordozható számítógépek felhasználói számára a hálózati fájlok kapcsolat nélküli kezelése. Ez tulajdonképpen azt jelenti, hogy a hálózatról használt fájlok azután is elérhetőek maradnak, hogy a felhasználó számítógépét leválasztották a hálózatról, vagy a kiszolgáló bármi más ok miatt nem érhető el. Ez úgy lehetséges, hogy a felhasználó számítógépén másolat készül azokról a fájlokról, amelyekhez a felhasználó a hálózaton keresztül hozzáfér, és amikor a fájlok eredetijét tartalmazó kiszolgáló elérhetetlenné válik, a Windows a helyi másolatot használja.

A fájlok kapcsolat nélküli használatát azonban mind a kiszolgáló, mind az ügyfél oldalán elő kell készíteni. A kiszolgáló oldalán minden mappamegosztás esetén engedélyezni kell az oda kapcsolódó felhasználók számára a benne levő fájlok kapcsolat nélküli használatát.

166. ábra: Csatlakoztatott eszköz elérhető funkciói

10.2.6 Az új generáció

A Windows 7 és Windows Server 2008 ilyen lehetőségei nem hordoztak sok újdonságot a korábbiakhoz képest, emiatt a Microsoft jól érezte, hogy változtatnia kell. Apró, de fontos megjegyzés, hogy az eszközközpont csak Windows Mobile eszköz csatlakoztatására lett tervezve. Más eszköz (pl. Android OS telefon, Blackberry, iPhone, iPad – azaz iOS, normál mobil, stb.) csatlakoztatásakor annak saját, típusspecifikus szoftverét szükséges használni a szinkronizáláshoz (pl.: iOS – iTunes).

Emiatt egészen más a Windows 8. Itt már egy Microsoft Live ID fiókkal bejelentkezve lehet szinkronizálni az eszközöket, legyen szó tabletről, mobilról vagy asztali gépről. Ha ugyanazon Live ID van használva bejelentkezéskor a különféle eszközökön, a levelek, naptárbejegyzések, sőt az asztali témák és séma, valamint színbeállítások is szinkronizálódnak. A különféle programokat már a Microsoft saját online áruházából lehet letölteni bármely eszközre, így egy megvett és letöltött program azonnal megjelenik a többi eszközön is.

Ugyanilyen elv alapján működik a Google és az Apple szolgáltatása is. (bővebben[70])

10.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

10.3.1 Összefoglalás

A számítógéprendszerek üzemeltetése nem egyszerű feladat, főleg azért mert eléggé szerteágazó. Ezeket a feladatokat két nagy csoportra lehet osztani, melyek közül az egyik a karbantartás, amely gyakorlatilag a hibák megelőzését szolgálja, a másik a monitorozás, azaz a különböző (éles és teszt) rendszerek figyelése, illetve a már létrejött hibák felderítése és javítása.

A monitorozás fő eszköze a Windows eseménynapló szolgáltatása, amely alapértelmezésben három naplót tartalmaz, amelyek száma növelhető. A három napló a rendszernapló, a biztonságinapló és az alkalmazásnapló. Ezekbe a naplókba a rendszer olyan eseményeket rögzít, amelyek kritikusak lehetnek a rendszer működésével kapcsolatban. A rögzített eseményeknek különböző szintjei lehetnek, melyek közül a leggyakoribbak a hibák, a figyelmeztetések vagy az információk.

A Windows olyan eszközökkel is támogatja a monitorozást, mint a teljesítményfigyelő, vagy az erőforrás-figyelő, mely eszközökkel a különböző erőforrások terheltsége monitorozható.

A mobil eszközök használatára egyre növekszik az igény. Ráadásul ezen eszközöknek a vállalati hálózatban ki kell tudnia szolgálni az adott környezethez szokott felhasználókat. A mobil eszközök és az asztali gépek közötti szinkronizációt már régóta fejleszti a Microsoft. A jelenlegi rendszerben a Windows Mobil központ segítségével lehet ezeket a műveleteket megtenni. A jövőben viszont úgy tűnik, hogy ez az irány is a felhőtechnológia felé mozdul el.

10.3.2 Önellenőrző kérdések

1. Melyek a rendszergazda üzemeltetési feladatai?
2. Mire jó a monitorozás?
3. Miért szükséges az események naplózása?
4. Milyen naplókat használ az eseménynapló?
5. Ismertesse naplónként a különböző eseményszinteket!

[70] Nyeste Gábor: Telekommunikáció, Eger, EKF, 2012

6. Mire lehet használni a teljesítményfigyelőt és hogyan kell a célnak megfelelően beállítani?
7. Mire lehet használni az erőforrásfigyelőt?
8. Milyen eszköz segítségével lehet a mobil eszközök és az asztali számítógépek közötti szinkronizációt megvalósítani?
9. Hogyan működik a Windows kiszolgáló a hordozható számítógépek számára kitalált hálózati fájlok kapcsolat nélküli kezelése szolgáltatása?

11 KARBANTARTÁS, MENTÉS ÉS VISSZAÁLLÍTÁS

11.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Az előző leckében az üzemeltetés mindennapi dolgaival foglalkozott, és így monitorozásra esett a hangsúly, ebben a leckében pedig az megelőző műveletekről szól. A karbantartás feladatainak ismertetése után, a Windows kiszolgáló biztonsági másolat szolgáltatásai kerülnek ismertetésre. A lecke végén pedig a biztonsági mentés és visszaállítás funkcióinak bemutatása következik.

A tananyag áttanulmányozása után a hallgató képes lesz olyan feladatok ellátására, mint az egyszeri vagy ütemezett biztonsági mentés készítése, valamint az mentésekből történő visszaállítás művelete.

11.2 TANANYAG

11.2.1 A karbantartás

A karbantartás a megbízható üzemeltetés elhagyhatatlan része. Általánosságban elmondható, hogy a karbantartás gyakorlatilag a hibák megelőzése és elhárítása. Ez egy nagyon sokrétű feladat.

A megelőzést vizsgálva ide tartozhat a tűzvédelemtől, a katasztrófahelyzetekre való felkészüléstől, vagy az illetéktelen behatolóktól való fizikai és szoftveres védelemtől kezdve a szünetmentes tápegységek használatán, a hardver megfelelő felügyeletén, a szoftver és a vírusirtó vírusadatbázisának naprakészen tartásán keresztül a biztonsági mentésekig elég sok minden. A lista jóval bővebb az említett feladatok felsorolásánál.

A hiba elhárítása és az üzemmenet megszokott, normális helyzetbe való visszaállítása igen komoly felkészültséget kíván meg az üzemeltető személyzettől. A hiba elhárításához először is a hiba igazi okát kell megtalálni és elhárítani. Előfordulnak azonban olyan esetek, amikor az ügymenet folyamatossága miatt áthidaló, ideiglenes megoldásként a hiba valódi okának elhárítása és a normál üzem visszaállítása helyett, más megoldásra van szükség. Ezekre az esetekre nem mindig van recept, szükséges egyfajta kreativitás és problémamegoldás az üzemeltető részéről, amely képességek segítségével, sokat improvizálva sikerülhet áthidalni a nehézségeket.

11.2.2 Biztonsági mentés és visszaállítás

Manapság, amikor az informatika, a számítógép és a hálózat már közműnek számít, alapvető igény, hogy egy számítógéprendszer merevlemezének tartalmáról rendszeresen **biztonsági mentés** (Backup) készüljön. Ha mást nem is, de legalább azokat a mappákat érdemes menteni, amelyek fontos dokumentumokat, nem reprodukálható anyagokat tartalmaznak.

Alapkövetelmény, hogy a mentéseket nem a számítógépekkel azonos helyen kell tárolni, mert a telephelyet érintő elemi csapás esetén nem csak a számítógépek, hanem a biztonsági mentés is megsérülhet. Továbbá arra is oda kell figyelni, hogy a mentett anyagok védelme is megfelelő legyen. Védeni kell többek között szintén az elemi csapásoktól, de az illetéktelen személyek hozzáférése ellen is.

A mentés és visszaállítás tervezést igényel, a tervek elkészítése pedig mindig valamilyen stratégia mentén történik. Ezt nevezik mentési stratégiának. A mentési stratégiának több összetevője, melyeket nagyon sok tényező befolyásol, kezdve a mentendő anyagok típusától, az elfoglalt tárterülettől, a rendelkezésre állás fontosságától egészen a mentési kapacitásig vagy akár a jogi szabályozásokig. Látható tehát, hogy a stratégia megtervezése komoly feladatot ró a rendszergazdákra. A téma terjedelme miatt a tankönyv ennek bemutatására nem vállalkozik, azonban egy kisvállalati rendszert alapul véve néhány szempont említésre kerül a következőkben.

A mentés indításának szempontjából kétféle mentés létezik. Az egyik a kézi mentés, melyet a felhasználó (rendszerint a rendszergazda) állít be és indít. Ezt egyszeri mentések készítésekor, vagy speciális esetekben célszerű alkalmazni. A másik az automatikus vagy más néven ütemezett mentés. Ilyenkor a mentési stratégia szerint beállításra kerülnek a mentés tulajdonságai. Általában a menteni szokás egy teljes rendszert, de előfordul, hogy bizonyos mappák külön mentést igényelnek, mert pl. a benne tárolt tartalom mentése nagyobb gyakoriságot kíván. Alapvetően kétféle mentési eljárás kombinációit szokták alkalmazni. Az egyik a **teljes mentés** (Full Backup), amikor is a megadott mappa (kötet, vagy akár a teljes rendszer) összes fájlja mentésre kerül. A másik eljárás, amikor egy kiinduló állapothoz képest (amely rendszerint egy teljes mentés) történt változásokat menti. Ennek a típusnak inkrementális mentés a neve. Rendszerint ezt a kettőt kombinálják valamilyen stratégia szerint, amely függ a mentendő mappák, fájlok tartalmától, felhasználásától és mennyiségétől is. A mentési stratégia része az is, hogy a mentést meddig kell tárolni.

Gyakori mentési stratégia, a teljes rendszer heti mentése, a hét többi napján pedig inkrementális mentés követi a változásokat. A mentés

időpontjának célszerű olyan időpontot választani, amikor a kiszolgáló a legkevésbé kihasznált (pl. éjfél és hajnal között), de figyelembe kell ilyenkor azt is venni, hogy mennyi idő alatt fut le a mentés, nehogy a reggeli csúcsba is belefusson. Általános anyagok, pl. levelezés, általános fájlkiszolgáló esetén a gyakorlat azt mutatja, hogy általában 1 hónapnál tovább nem szükséges a mentések megtartása.

A mentési stratégia része az ún. katasztrófa terv, mely olyan nem várt eseményekre reagál, mint a teljes rendszert érintő hardverhibák, vagy a természeti katasztrófák (árvíz, tűzkár, földrengés), amikor is a rendszer működésképtelenné válik, vagy megsemmisül. Ekkor a mentésekből a teljes rendszert kell helyreállítani, gyakran egy teljesen új hardverre. A mentési stratégiának tehát fel kell készülnie ilyen esetekre is.

11.2.3 A Windows Server biztonsági másolat szolgáltatásai

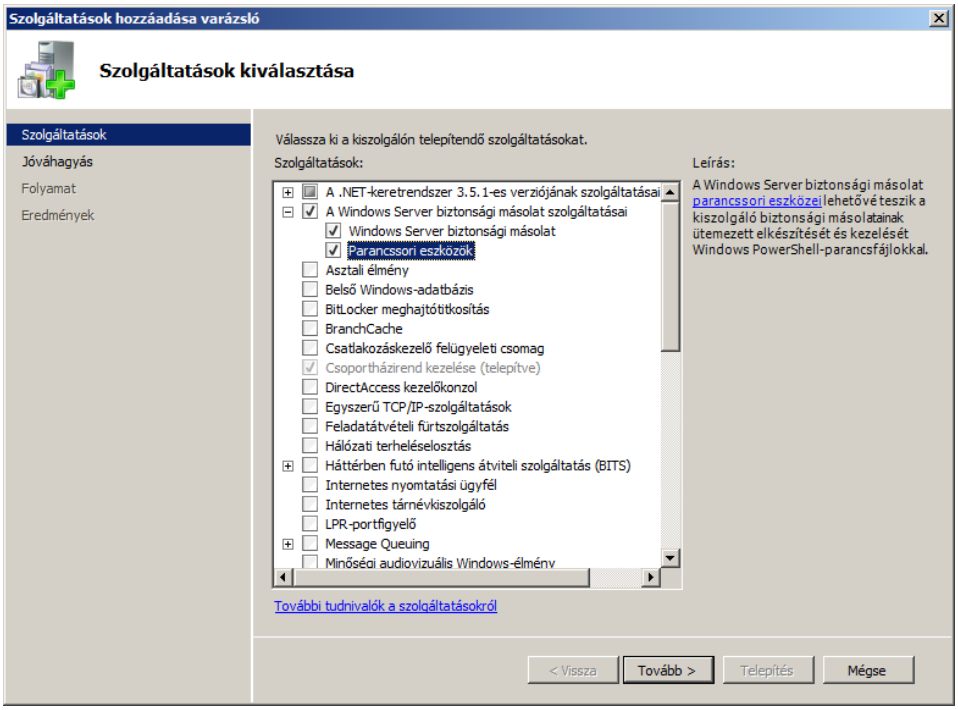
A Windows Server 2008 mentőprogramjával, amely a **Windows Server biztonsági másolat szolgáltatásai** (Windows Server Backup Features) része, tetszőleges adathordozóra (nagy kapacitású cserélhető lemezek, memóriakártyák, helyi merevlemezek, hálózati tárhelyek, CD és DVD lemezek) készíthető biztonsági mentés.

Biztonsági mentés készítésekor a rendszer a kijelölt fájlokat tulajdonképpen lemásolja egy másik adathordozóra. Ilyen művelet esetén gyakran előfordul, hogy egy adott fájlhoz vagy mappához nincs meg a megfelelő engedély. Ennek a problémának a megkerülésére a Windows Serveren léteznek olyan csoportok, amelyeknek tagjai biztonsági mentés céljából hozzáférhetnek a lemezeken tárolt fájlokhoz. Ilyen engedéllyel automatikusan rendelkeznek a **rendszergazdák** (Administrators) és a **biztonságimásolat-felelősök** (Backup Operators) csoportok. A biztonsági másolat készítéséhez a megfelelő engedélyt így a biztonsági másolatot készítő felhasználó **biztonságimásolat-felelősök** csoportba történő felvételével lehet megadni.

A biztonsági másolat készítésének és a visszaállításnak a joga külön is kezelhető. A kijelölt felhasználóknak a biztonsági mentésről a **biztonsági másolat készítése fájlokról és könyvtárakról** (Back up files and directories) jogot kell megadni, a visszaállításhoz pedig a fájlok és **könyvtárak helyreállítása** (Restore files and directories) jog szükséges. Előfordulhat, hogy szét kell választani ezeket a funkciókat és ehhez a lehetőség adott.

11.2.4 A Windows Server biztonsági másolat szolgáltatásainak telepítése

A Windows Server telepítésekor a **biztonsági másolat szolgáltatás** alapértelmezetten nem kerül telepítésre, csak a felügyeleti eszközök között található **Windows Server biztonsági másolat** (Windows Server Backup) program, amely a mentési szolgáltatásokat használni tudó grafikus felületű kliens program. A telepítés legegyszerűbben a **kiszolgálókezelőn** (Server Manager) keresztül végezhető el. Itt a jobb oldalon a **szolgáltatásokra** (Services) jobb gombbal kattintva, a megjelenő helyi menüből ki kell választani a **szolgáltatás hozzáadása** (Add Feature) menüpontot kell választani, amelynek hatására elindul a **szolgáltatások hozzáadása varázsló** (Add Feature Wizard).



167. ábra: A szolgáltatás telepítése

A megjelenő listából a **Windows Server biztonsági másolat szolgáltatásai** (Windows Server Backup Features) elem előtt ki kell jelölni a jelölőnégyzetet, ezzel kiválasztva magát a szolgáltatást és **a Windows Server biztonsági másolat** kliens eszköz MMC beépülő modulját, amely egy grafikus felületen használható mentés és visszaállítás kezelő. Ezekkel együtt telepítésre kerül az említett kliens program parancssoros megfelelője a **wbadmin.exe** is. Ha ezenkívül szükség van

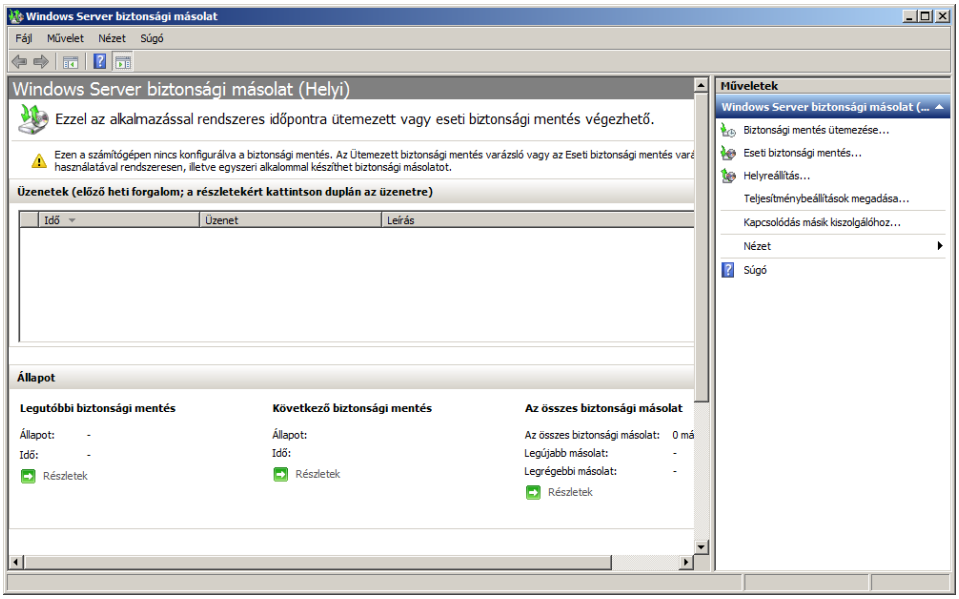
parancssoros megoldásokra is, mert pl. az rugalmasabban konfigurálható, akkor a pluszjelre kattintva, és ezzel a szolgáltatáshoz tartozó részfát kinyitva, ki kell választani a **parancssori eszközöket** (Command-line Tools) is. Ezek után a **tovább** (Next), majd a **telepít** (Install) és végül a **bezár** (Close) gombra kattintva a szolgáltatás igénybevehető.

A **Windows Server biztonsági másolat** program indításához a **Start menü**, **felügyeleti eszközök** (Administrative Tools) almenüjének **Windows Server biztonsági másolat** (Windows Server Backup) menüpontját kell választani. Az elinduló program alapértelmezetten a helyi mentési szolgáltatásokhoz kapcsolódik. Mivel a mentő eszköz az összes Windows Servert futtató számítógépen alapértelmezetten telepítésre kerül, így a hálózatban elég egy dedikált mentőkiszolgálót telepíteni. (Természetesen a mentő kiszolgáló mentése is kívánatos.) Ha más számítógépen futna a mentési szolgáltatás, akkor itt annak a mentési kiszolgálónak a nevét, vagy IP címét kéne megadni. Ez a beállítás a későbbiekben is elvégezhető a **művelet** (Action) menü **kapcsolódás másik kiszolgálóhoz** (Connect To Another Computer) menüpontja segítségével.

A **műveletek** menüpontjai megjelennek a megjelenő ablak jobb oldalán is, segítve az eszköz használatát. Az ablak fő része egy **üzenetek** (Messages) és egy **állapot** (Status) mezőre van bontva. Ezek felett megjelenik egy figyelmezető (sárga felkiáltójeles) üzenet, miszerint a számítógépen nincs konfigurálva biztonsági mentés. Ez a mentés beállítása után eltűnik. Az említett két mező az első biztonsági mentés beállítása és lefutása után fog információkat szolgáltatni.

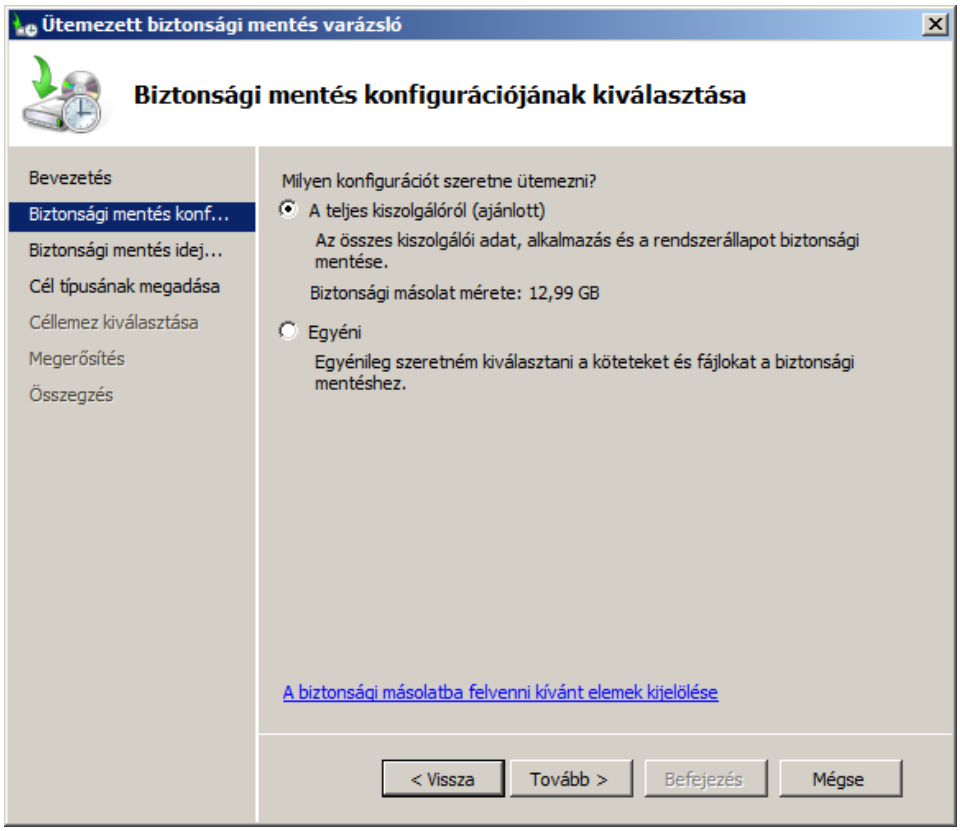
11.2.5 Mentés a Windows Server biztonsági másolat alkalmazással

Automatikus vagy ütemezett mentés beállításához a **biztonsági mentés ütemezése** (Backup Schedule) elemet kell kiválasztani a jobb oldalon a **műveletek** (Actions) mezőben, vagy a **művelet** menüből. Az elinduló ütemezett biztonsági mentés varázsló először a lehetőségekről ad tájékoztatást. Itt a **tovább** (Next) gombra kattintva a megjelenő **biztonsági mentés konfigurációjának kiválasztásánál** (Select Backup Configuration) el kell dönteni, hogy a **teljes rendszerre** (Full server) vonatkozó mentésre vagy **egyénileg megadott** (Custom) mentendő kötetek, mappák, fájlok mentésére van e szükség.



168. ábra: A Windows Server biztonsági másolat alkalmazás

A **teljes kiszolgálóról (ajánlott)** (Full Server (recommended)) opciót választva, amely a legtöbb esetben a helyes választás, további konfiguráció hiányában a **tovább** (Next) gombra kattintva az mentés időpontjánál beállítása következik. Az **egyéni** (Custom) lehetőséget választva azonban a **tovább** gombra kattintás után meg kell adni azokat a köteteket, mappákat, fájlokat, amelyek mentése kívánatos. A megjelenő listába az **elemek hozzáadása** (Add Items) gombra kattintva böngészhető és választható ki a mentendő elem, az elem neve előtti jelölőnégyzet kipipálásával. Itt az előbb említett elemeken kívül választható a **rendszerállapot** (System state) és az **operációs rendszer nélküli visszaállítás** (Bare metal recovery) is, gondolva a katasztrófa tervben megkövetelt mentés-visszaállításra is. A listába felvehetők kivételek is, amelyek a **speciális beállítások** (Advanced Settings) gombra kattintva a **kizárások** (Exclusions) lapon, a **kizárás hozzáadása** (Add Exclusion) gombra kattintva lehet böngészni és kiválasztani. Itt nem csak helyek, hanem fájltípusok is megadhatók, amely igen hasznos lehet, ha pl. a felhasználó mp3 gyűjteményét nem kívánja a rendszergazda menteni. Az elemek eltávolítása, illetve a speciális beállítások között a kizárás eltávolítása gombok mindig az éppen kijelölt elemet távolítják el a listából. A megfelelő elemek kiválasztása után a **tovább** (Next) gombra kattintva a már említett mentés időpontjának beállítása.



169. ábra: Biztonsági másolat létrehozása

A mentés időpontjának megadásakor először el kell dönteni, hogy **naponta egyszer** (Once a day) vagy **többször** (More than once a day) van szükség mentésre. A választás után meg kell jelölni az időpontokat, majd a **tovább** (Next) gombra kell kattintani.

A következő beállítást igénylő lépés a mentés helyének kiválasztása. Itt háromféle lehetőség közül lehet választani. A **biztonsági mentés egy külön erre a célra fenntartott merevlemezre (ajánlott)** (Back up to a hard disk that is dedicated for backups (recommended)) lehetőség a mentés legbiztosabb módja, rendes, ütemezett mentésre gyakorlatilag ez az egyetlen használható lehetőség. A **biztonsági mentés kötetre** (Back up to a volume) lehetőség talán a legszerencsétlenebb választás, ugyanis a mentés esetén elég nagy az I/O kihasználtság, és emiatt ha ugyanazon a merevlemezen egy másik kötetet is használ a rendszer, annak teljesítménye jelentősen le fog csökkeni (gyakorlatilag használhatatlan lesz). Ennek használata csak kivételes esetekben javallott. A **biztonsági mentés megosztott hálózati mappába** (Back up to a shared network

folder) lehetőség választása esetén rendelkezésre kell álljon egy hálózati megosztás, amelyhez a megfelelő felhasználónak, jelszónak és engedélyeknek is rendelkezésre kell állni. Ennek egyetlen hátránya ütemezett mentés esetén mindig felül fogja írni az előző mentést, amely nem túl jó dolog, főleg ha a mentési stratégia több tárolási időt ír elő, mint a mentési ciklus. Dedikált mentő kiszolgáló esetén tehát az első opció a megfelelő választás és érdemes nagy kapacitású merevlemezeket használni erre a célra.

A következő **céllemez kiválasztása** (Select destination disk) oldalon az **összes elérhető lemez megjelenítése** (Show All Available Disks) gombra kattintva, ki lehet jelölni azokat a meghajtókat, amelyek bekerülhetnek a választható listába. Ezek után az **OK** gombra kattintva már csak ki kell jelölni azokat a meghajtókat, amelyekre a biztonsági mentés készülni fog. A **tovább** (Next) gombra kattintás után egy figyelmezető ablak fog felugrani, amely jelzi, hogy jelenleg a lemezen lévő összes adat törlődni fog. Ha a meghajtón semmilyen fontos adat nincs, akkor ki lehet választani az **igent** (Yes). Érdemes feljegyezni a lemez címkét a céllemez **felcímkézése** (Label destination disk) oldalon, amely a **címke** (Label) oszlopban látható, ugyanis a Windows visszaállításkor erre a címkére fog hivatkozni.

Ha az előző résznél a megosztott hálózati mappás lehetőség lett választva, akkor annyi teendő van még, hogy meg kell adni a megosztás UNC nevét, majd a felugró ablakban a felhasználó nevet és jelszót, ha az különbözik a jelenleg használttól.

Ezek után már csak át kell tekinteni az összesítést a beállításokról és **befejezés** (Finish) gombra kattintva jóváhagyhatóak a mentési beállítások.

Eseti mentés beállításai nem sokban különböznek az ütemezettétől. Az egyik nyilvánvaló különbség pl. az, hogy nem kell beállítani mentési időpontot.

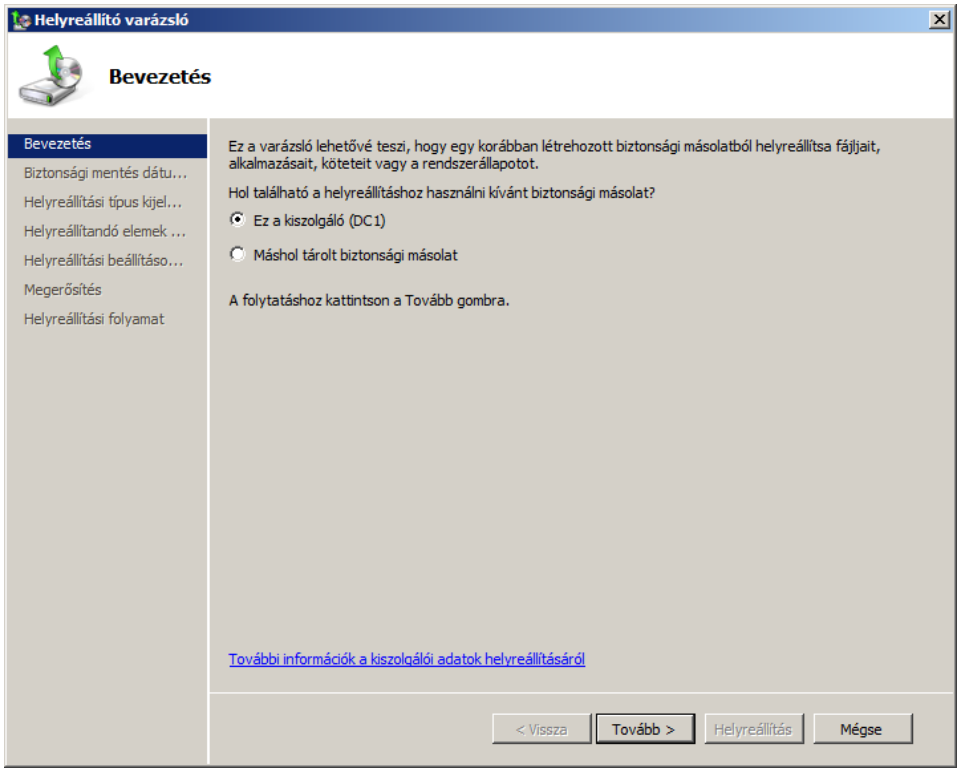
A mentés jobb testreszabhatóságát parancssoros eszközök is támogatják, azonban ha ez nem került telepítésre, akkor is van lehetőség a wbadmin.exe parancs segítségével, illetve kis parancsfájl hegesztéssel olyan mentő-szkriptet készíteni, amely pl. ütemezetten ment hálózati megosztásra és a mentés nevét pl. a dátum és idő információból alakítja ki, így a mentések nem lesznek felülírva.

- A biztonsági mentés nem tévesztendő össze az archiválással, amikor a fájlok azzal a céllal lesznek valamilyen adathordozóra írva, hogy ne foglalják a helyet munkalemezen, azonban ezekre a fájlokra még valamikor szükség lehet. Ezek a fájlok többnyire régi munkák fájljai, amelyekre az aktuális feladathoz nincs szükség, ám később bármikor előfordulhat, hogy elő kell venni őket.

11.2.6 A visszaállítás

A mentésekhez egészen addig nem kell nyúlni, amíg valahol valamilyen adatvesztés nem történik. Ilyen esetben következik a visszaállítás művelete, amely a következő lépésekből áll:

A visszaállításhoz a **Windows Server biztonsági másolat** programot elindítva a **művelet** (Action) menüből ki kell választani a **helyreállítás** (Recover) menüpontot. A megjelenő **helyreállító varázsló** (Recovery Wizard) párbeszédpanel első lapján ki kell választani **ezt a kiszolgálót** (This server), majd a **tovább** (Next) gombra kell kattintani.



170. ábra: A visszaállítás

A következő lapon a **biztonsági mentés dátumának kijelölésénél** (Select backup date) meg kell adni a dátumot, amelyik mentésből a visszaállítás történni fog. Ezután a **helyreállítási típust** (Select recovery type) kell megadni. Itt a **fájlok és mappák** (Files and folders) opciót csak bizonyos fájlok vagy mappák visszaállítása esetén kell választani. Az **alkalmazások** (Application) opciót választva a **Windows Server biztonsági mentés** program által ismert alkalmazások

adatainak (pl.: Exchange vagy Microsoft SQL Server) visszaállítására is van lehetőség. A harmadik **kötetek** (Volumes) opció kiválasztásával a rendszerkötet kivételével bármelyik kötet teljes helyreállítása megtörténhet.

- A rendszerkötet visszaállítása a Windows Server 2008 R2 telepítő lemezéről elérhető **Windows helyreállítási környezet** (Windows Recovery Environment) felületén végezhető el. A katasztrófaelhárítási tervben vázolt katasztrófa utáni teljes rendszervisszaállítás pl. ilyen módon történhet.

A legtöbb esetben tehát a **fájlok és mappák** opció kerül kiválasztásra. A **tovább** (Next) gombra kattintva a helyreállítandó elemek kijelölése (Select items to recover) lapon meg kell adni azokat a fájlokat illetve mappákat, amelyeket vissza kell állítani, majd a tovább gombra kell kattintani.

A **helyreállító varázsló** következő lapján lehet megadni, hogy a visszaállítandó fájlokat illetve mappákat eredeti helyükre vagy egy másik helyre kell visszaállítani. A **tovább** (Next) gombra kattintva már csak az összegző lapon kell egy jóváhagyás a visszaállítási művelet elvégzésére, amelyet a **helyreállítás** (Recovery) gombra való kattintással meg is lehet tenni.

11.3 ÖSSZEFOGLALÁS, KÉRDÉSEK

11.3.1 Összefoglalás

Az utolsó leckében az olyan karbantartási munkák kerültek ismertetésre, mint az operációs rendszer frissítése, vagy a biztonsági mentés és visszaállítás. A karbantartási munkák gyakorlatilag megelőző jellegű műveletek, melyekre pont azért van szükség, hogy a lehetséges hibák elkerülhetőek legyenek, illetve ha elkerülhetetlenek, akkor a hiba kiküszöbölésével, a rendszer előző állapotba történő visszaállításával lehessen rájuk reagálni.

Előbbihez tartoznak a frissítések, töredezettségmentesítések, utóbbihoz pedig a biztonsági mentések és visszaállítás funkciója. A frissítés a Windows Update szolgáltatás segítségével történik, a mentés és visszaállítás pedig a Windows Server biztonsági másolat szolgáltatás segítségével történhet. A mentés lehet egyszeri manuális, vagy rendszeres, automatikus, ütemezett feladat, valamint lehet menteni csak bizonyos fájlokat vagy mappákat, vagy akár a teljes rendszert. A rendszergazda feladata a mentés megtervezése, amelynek központi eleme a mentési stratégiák kialakítása.

A visszaállítás műveletére minden rendszergazda reménye ellenére sajnos mindig sor kerül. Ha más miatt nem is, de a felhasználók figyelmetlenségéből történő törlés miatt biztosan. Érdemes azonban katasztrófaelhárítási tervvel is

rendelkezni, hogy egy katasztrófa szintű rendszerösszeomlás esetén a rendszer, megadott lépések szerint újraépíthető legyen a mentésekből.

11.3.2 Önellenőrző kérdések

10. Melyek a karbantartás feladatai?
11. Mit jelent az, hogy a karbantartás megelőző jellegű feladat?
12. Milyen tulajdonságokat kell vizsgálni egy mentési stratégia felállításánál?
13. Milyen típusú mentéseket támogat a Windows Server biztonsági másolat szolgáltatásai?
14. Mire kell odafigyelni a különböző típusú mentési célok esetén?
15. Hogyan történik a visszaállítás művelete fájlok és mappák, illetve teljes rendszer mentés esetén?

12 ÖSSZEFOGLALÁS

12.1 TARTALMI ÖSSZEFOGLALÁS

A vállalati rendszerek esetén a Windows alapú kiszolgálók elterjedtsége továbbra is jelentős. Köszönhető ez egyrészt a nagyon népszerű Windows kliens operációs rendszereknek is, de nagyrészt a központosított felügyeletet és kezelést erőteljesen támogató Windows kiszolgálókkal kialakított címtárstruktúrának is.

A Windows címtár, az Active Directory (röviden AD) használata nélkül ma már nem nagyon lehet pár gépesnél nagyobb, jól karbantartható Windows számítógépekből álló hálózatot építeni és üzemeltetni. A különböző funkciók mind erősen címtárfüggőek, azaz az AD megkerülhetetlen.

A tankönyvben arra történt próbálkozás, hogy az olvasókkal megismertesse a címtárat, a címtár struktúrát, és a címtár leggyakrabban használt szolgáltatásait.

Tárgyalásra került a Windows operációs rendszerek telepítése, frissítése és migrációja, valamint a tananyagban használt VirtualBox virtualizációs technológia, amelynek segítségével a tananyag tesztrendszerei elkészültek.

Ismertetésre kerültek a különböző hardvereszközök kezelésének eszközei, az alkalmazások beállításai, valamint a hálózati konfiguráció, amely különösen fontos, hiszen hálózatos környezetről van szó.

Bemutatásra került a címtár infrastruktúra, különös tekintettel az AD felépítésére továbbá szolgáltatásaira, valamint az AD működési szintek közötti különbségekre.

A címtár nem létezhet DNS kiszolgáló nélkül, együttműködésük natív DNS kiszolgálók esetében a legzökkenőmentesebb. Ez utóbbi a telepítés során derül ki, hiszen ilyen DNS kiszolgáló esetén gyakorlatilag automatikus a DNS konfigurációja.

Az olyan címtár objektumok, mint a felhasználói fiókok, a csoportok, vagy a szervezeti egységek mind olyan AD objektum, amelyek nélkül az AD rendszere nem működhet. Ezeknek kezelése, illetve hatásuk a csoportházirendekre és a hozzáférés-vezérlésre került ismertetésre.

A modern hálózatok nem létezhetnek a biztonság alapját jelentő titkosítási technológiákkal. A Windows kiszolgálók által támogatott és megépíthető nyilvános kulcsú infrastruktúra is ilyen. Bemutatásra került egy ilyen egyszerűbb infrastruktúra létrehozásához szükséges hitelesítésszolgáltató telepítése, valamint a tanúsítvány igénylés folyamata AD környezetben.

A csoportházirend szolgáltatás segítségével a felhasználók munkakörnyezetének, helyi házirendjének, valamint jogainak kiosztása történhet meg. A szolgáltatás az AD objektumaira, azok közül is a szervezeti egységekre, valamint a tartományokra, telephelyekre épül, amelyekhez ún. csoportházirend-objektumok rendelhetők, melyeknek hatásai különböző szabályok mentén összeadódhatnak.

Az AD különböző objektumai mind rendelkeznek ún. hozzáférésvezérlési listával, melynek elemei a különböző csoportok és felhasználók hozzáférési engedélyeinek szabályozását tárolják. Különböző típusú objektumokhoz különböző típusú engedélyek tartoznak. Itt bemutatásra kerültek a NTFS fájl és mappaengedélyek, a megosztott mappák és nyomtatók engedélyei. Ezenkívül ismertetésre kerültek a különböző módon kapott engedély-szabályozások együttes eredménye kiszámításának szabályai is.

Hiába az AD, önmagában egy nagyobb vállalati rendszer üzemeltetése már a telepítés feladatánál elakadhat, mivel a hagyományos úton történő telepítésekhez nincsen elég humánerőforrás, és valószínűleg a folyamat idő tényezője is nagyon kritikus lenne. A központi Windows-telepítési szolgáltatások segítségével tömeges telepítések hajthatók végre, számos könnyítéssel kiegészítve.

A rendszergazda állandó feladatai a telepítés és a rendszerek alapvető beállításai után a rendszerek üzemeltetése és karbantartása. Ezek nélkül a feladatok nélkül az informatikai rendszer nem tartható fenn, ismeretük és alkalmazásuk elkerülhetetlen. A feladatok egyrésze monitorozáson alapul úgy, mint az eseménynapló, a teljesítményfigyelő vagy az erőforrásfigyelő használata, más része pedig az olyan megelőző folyamat, mint a frissítések kezelése valamint a biztonsági mentés és visszaállítás.

A jövő a mobil technológiákban rejtőzik, melyeknek kitörése éppen folyamatban van. A Microsoft és a Windows megpróbálja ezeket a folyamatokat meglovagolni. Következő operációs rendszerűkben a Windows Server 2012-ben, illetve a Windows 8 kliens operációs rendszerben a mobil technológia támogatása már jóval komolyabb, mint elődeiben.

12.2 ZÁRÁS

Az informatika területén csaknem bármilyen témára igaz, hogy a tananyag megfelelő elsajátítása nem elég ahhoz, hogy az ember naprakész legyen. A dinamikusan fejlődő ágazatokra ez különösen igaz. Nagyon fontos ebben a témában is, hogy az érdeklődő folyamatosan fejlessze tudását és képességeit, valamint legyen nyitott az új dolgok iránt. Az addig elsajátított tudást pedig úgy tudja átültetni az új rendszerekre, hogy azok megfelelő elméleti és gyakorlati alapot adjanak az új ismeretek elsajátításához.

13 KIEGÉSZÍTÉSEK

13.1 IRODALOMJEGYZÉK

13.1.1 Hivatkozások

Könyv

GÁL Tamás: Windows Server 2008 R2, A kihívás állandó. Budapest, Jedlik Oktatási Stúdió, 2011.

Kis Balázs – Szalay Márton: Windows Server 2008 rendszergazdáknak, Bicske, Szak Kiadó, 2008

Gál Tamás – Szabó Levente – Szerényi László: Rendszerfelügyelet rendszergazdáknak, Bicske, Szak Kiadó, 2007

William R. Stanek: Windows Server 2008, a rendszergazda zsebkönyve, Redmond, Washington, USA, Microsoft Corporation, 2008 (Magyar kiadás, Bicske, Szak Kiadó, 2008)

Kerecsendi András: Hálózati Operációs Rendszerek, Eger, EKF, 2013

Petrényi József: Windows Server 2008, TCP/IP alapok, I. kötet, v2.0, Budapest, Microsoft Magyarország, 2010

William R. Stanek: Microsoft Windows 2000 Administrator's Pocket Consultant, Redmond, Microsoft Corporation, 1999

Nyeste Gábor: Telekommunikáció, Eger, EKF, 2012

Elektronikus dokumentumok / források

Trina Gorman: Windows Deployment Services Getting Started Guide. Elektronikus kiadvány, Redmond, Microsoft Corporation, 2009

Wikipedia: A Microsoft Windows története. Online enciklopédia, Wikipedia, 2004-2012 <http://hu.wikipedia.org/wiki/A_Microsoft_Windows_t%C3%B6rt%C3%A9nete>, 2012.09.11

Sting: 20 éves a Windows - történelmi áttekintést az elmúlt két évtizedről. Online cikk, PC Fórum, 2005 <http://pcforum.hu/cikkek/115/20+eves+a+Windows-tortenelmi+attekintest+az+elmult+ket+evtizedrol.html>, 2012.09.11

Wikipedia: VirtualBox. Online enciklopédia, Wikipédia, 2007-2012 <http://en.wikipedia.org/wiki/VirtualBox>, 2012.09.13

Microsoft Corporation: Frissítés Windows Vista rendszerről Windows 7 rendszerre. Online cikk, Microsoft Corporation <http://windows.microsoft.com/hu-hu/windows7/help/upgrading-from-windows-vista-to-windows-7>, 2012.09.15

Microsoft Corporation: Windows áttelepítő. Online cikk, Microsoft Corporation. <http://windows.microsoft.com/hu-hu/windows7/products/features/windows-easy-transfer>, 2012.09.15

Microsoft Corporation: Migrate Server Roles to Windows Server 2008 R. Online cikk, Microsoft Corporation <http://technet.microsoft.com/en-us/library/dd365353(v=ws.10).aspx>, 2012.09.16

Kovács Attila: Active Directory alapfogalmak dióhéjban, Online cikk, KF GAMF Info, 2011, <http://gamfinfo.hu/halozatok/201103/active-directory-alapfogalmak-diohejban>, 2012.09.19>

William R. Stanek: File and Folder Permissions. Online cikk, Microsoft Corporation,1999 <http://technet.microsoft.com/en-us/library/bb727008.aspx>, 2012.09.25