
Gál Tamás
Microsoft
Windows Server 2008 R2
A kihívás állandó
Windows Server 2008 R2
J.O.S.

Készült a ***Microsoft Magyarország Kft*** *megbízásából*

A könyv nyomtatott verziója megvásárolható a http://joskiado.hu címen lévő webáruházban.

Gál Tamás

Windows Server 2008 R2

A kihívás állandó

TechNetKlub

Jedlik Oktatási Stúdió
Budapest, 2011

J.O.S.

Lektorálta:

Lepenye Tamás (rendszermérnök, Microsoft Magyarország)
Petrényi József (szakértő, Emaildetektív Kft)

Borító: Varga Tamás

Anyanyelvi lektor: Bonhardtné Hoffmann Ildikó

Kiadó: Jedlik Oktatási Stúdió Kft.
1215 Budapest, Ív u. 8-12.
Internet: http://www.jos.hu
E-mail: jos@jos.hu
Felelős kiadó: a Jedlik Oktatási Stúdió Kft. ügyvezetője

Nyomta: LAGrade Kft.
Felelős vezető: Szutter Lénárd

ISBN: 978-615-5012-12-9
Raktári szám: JO-0337

Köszönetnyilvánítás

Csak a korábbiakat tudom ismételni (lásd Forefront TMG könyv), azaz a 10 éves gyermek újra a voodoo könyvvel, a feleség pedig - kb. félúton - a következő halkan benyögött mondattal: *„…tudtam, hogy nehéz lesz, de nem gondoltam, hogy ennyire.”* Ekkor már sejtettem, hogy az éjjel-nappal írás közben valószínűleg elviselhetetlenül viselkedem Velük. De lesz kárpótlás, ígérem.

Emellett a lektorok segítsége is nagyon sokat jelentett. Számos kötelességük ellenére, első kérésre elvállalták a feladatot, majd zokszó nélkül, brutálisan rövid határidőre kényszerítve is megtették a kötelességüket, amit még egyszer köszönök.

És még egy dolog a végére: köszönöm az új munkahelyemen (IQSOFT-John Bryce Oktatóközpont) a kollégáknak, hogy augusztusban és szeptemberben türelmesek és megértőek voltak.

„A számítógépek használhatatlanok. Csak válaszokat adnak.”

Pablo Picasso

TARTALOMJEGYZÉK

1 BEVEZETÉS

Jelen könyv születésének elsődleges oka az, hogy a Microsoft Magyarország szervezésében lebonyolított, hagyományosan rendkívül sikeres „Informatika Tisztán” sorozat negyedik részében[1], 2010 őszén 12 - az interneten is közvetített - előadáson keresztül foglalkoztunk a Windows 7-tel, de főképp a Windows Server 2008-cal és az R2-vel. A TechNet program akkori szakmai vezetőjeként már akkor is - azaz az előadások tartalmának és sorrendjének tervezése közben - tudtam, hogy a letölthető prezentációk és screencast-ok sora önmagában kevés lesz, szükség lesz később egy részletesebb, papíralapú kivonatra is. De tudni egy dolog, megírni meg egy másik – aki írt már valaha 2 oldalnál többet, az tudja, hogy miről beszélek…

Aztán menet közben, a napi robot során már a legnagyobb probléma nem is maga az írás volt, hanem a könyv témája. Ugyanis az utolsó (félig) szerveres könyvünk a szintén szép sikerű, kivételesen kereskedelmi forgalomba is került *„Rendszerfelügyelet rendszergazdáknak”* című mű volt, amelyben a Windows Vista és az akkor legfrissebb szerver, a Windows Server 2003 R2 került terítékre. Ehhez képest mostanra kettőt léptünk előre, hiszen nemcsak az óriási változásokat hozó Windows Server 2008, hanem az utódja, a szintén sok új képességet felvonultató a Windows Server 2008 R2 is megjelent. Az Informatika Tisztán előadásaiban és demóiban csak az R2-t használtuk, de még ott is muszáj volt a Windows Server 2008-as alapokra visszautalni, hát még mekkora szükség van erre egy annál jóval részletesebb tartalmú könyvben! Nos, úgy érzem, ez néha felemásra is sikeredett, mivel van olyan fejezet, ahol teljesen szétválasztottam (például a címtárszolgáltatások), de van, ahol nem, mert nem volt annyi különbség, vagy éppenséggel nem egymásra épültek a változások.

A tervezett tartalmat tekintve a dolgom nem volt nehéz, mert ugye az volt a lényeg, hogy a kezdők számára is érthető legyen, de a haladóknak is nyújtson új információt, illetve akinek a Windows Server 2008 vagy éppen az R2 az első operációs rendszere, az is értsen mindent, de aki esetleg a Windows Server 2003-ról „jön”, annak is hasznos legyen. Nem is nehéz, ugye? ☺

Na nem sajnáltatom magam tovább, de azt azért megjegyzem, hogy egy darabig a tartalomjegyzék átírása napi szintű feladatnak bizonyult. A mélységet illetően - azt hiszem - általában tudtam tartani magam a kitűzött kezdő/középhaladó szinthez, bár néha *„elgurult a gyógyszer”*, mint pl. az AD vagy az RDS fejezetnél (ezek lettek a

[1] https://technetklub.hu/blogs/informatikatisztan/archive/2010/10/14/informatika-tiszt-225-n-ingyenes-szakmai-k-233-pz-233-s-kezd-233-s-halad-243-rendszergazd-225-knak.aspx

leghosszabbak és a legrészletesebbek). És szeretném megjegyezni, hogy azért többnyire valamilyen Windows Server alapismereteket feltételeztem, tehát ha valahol nagyon elvesztjük a fonalat, akkor a korábban emlegetett könyvet kapjuk elő bátran![2]

A könyv címválasztása nem véletlen, kiváltó érvként felhoznám egy hajdani, pont a Windows Server 2008 debütálásakor megjelent TechNet Magazin előszavát.

„Ha egy matematikus vagy egy történelem szakos tanár a szakmája alapjait vizsgálja, akkor nyugodt szívvel konstatálhatja, hogy nincsenek megrendítő változások. A Pitagorasz tétel működik ma is, és valószínűleg nem fog kiderülni hirtelen, hogy valójában Caesar szúrt, és Brutus hunyt el. Természetesen a rendelkezésre álló tudás elmélyítése az élet bármely területén egy valós lehetőség, de az alapok és az alapokból építkező tudásanyag általában nem vész el, stabilan rendelkezésre áll, akár évszázadokon át is. Anélkül, hogy beleesnék az elitizmus csábító csapdájába, bátran állíthatom, hogy mi, informatikai szakemberek egy másik világban élünk. Először is, ez egy rettentően gyors világ, a Moore törvény kiválóan állja az évtizedek sodrát és a processzorokon kívül több más területen is igaznak tűnik. De még ennél is fontosabb hogy „mifelénk" gyakorlatilag a változás tekinthető stabil tényezőnek, új termékek, új szolgáltatások, új komponensek, új elvek, se vége, se hossza nincs az újdonságoknak – tehát tényleg újratanuljuk a szakmát, sokszor beleértve ebbe az alapokat is."

Viszont az összes nehezítő körülmény ellenére remélem, hogy sokak számára jelent majd segítséget és útmutatást eme fércmű elolvasása és megértése (az előzetes, már az ITv4 óta tartó érdeklődésből ez azért sejthető), a benne lévő sok-sok, majdnem lépésről lépésre szintű leírás alkalmazása és a megszerzett tudás rutinná átalakítása. Ezért készült.

[2] A hivatkozást a 14. oldalon megtaláljuk.

2 RÉGEN ÉS MA

2.1 APRÓ MAGYARÁZAT AZ ELEJÉRE

A Windows Server 2008 a Microsoft hatodik generációs (6.0), hálózati kiszolgáló operációs rendszere, amely RTM (Release to Manufacturing) kiadásának dátuma 2008. február 27. De itt és most mi nem állunk meg a 6. generációnál, hanem kicsit még tovább megyünk, mégpedig a 6.1-es verziójú Windows Server 2008 R2-re[3], amely 2009. július 22-én jelent meg.

Az a helyzet, hogy létezik egy másik, véleményem szerint kissé téves megközelítés, amely szerint ez utóbbi csupán a Windows Server 2008 javítása - és ami a lényeg: sokak szerint nincs is igazán komoly, számottevő különbség. A Microsoft az egyszerű „R2", azaz „Release 2" rövidítéssel talán kissé segít is ezen vélemény kialakításában, ám a helyzet az, hogy maximum *„szaktudástól el nem vakítva*[4]*"* gondolhatjuk ezt komolyan. Természetesen nem óhajtom lebecsülni a Windows Server 2008-at, hiszen a stabil alapot és a képességek jelentős részét valóban ez a termék adja az R2 alá is, és a Windows Server 2003-hoz képest óriási ugrást jelentett, de az R2 még így is különlegesen sokat tesz hozzá a készlethez, elsősorban a funkcionalitás területén, miközben egyúttal rengeteg helyen praktikusan korrigálja a 2008-as változatot.

Talán a legkönnyebben úgy értjük meg ezt a helyzetet, hogyha szembeállítjuk a Vista SP1-et és a Windows 7-et. Ugyanis a Windows Server 2008 kódbázisa jelentős részben a Vista SP1-gyel [5] egyezik meg, ezért architektúrájukban és a funkcionalitásukban is sok közös vonás található, és ugyanez a helyzet az R2 és a Windows 7 esetén.

> A könyv szempontjából persze ez a vita magammal kissé akadémikus jellegű, hiszen az a határozott szándékom, hogy a Windows Server 2003-hoz képest adjak némi tudást az Olvasó kezébe, így aztán, ha úgy vesszük, akkor egyszerre két terméket fogok bemutatni ezen oldalakon. Mindemellett azért alapvetően az R2 felől közelítek minden témához (például az összes képernyőképen), még akkor is, ha az adott résznél nincs vagy nincs sok változás a Windows Server 2008-hoz képest – persze ilyen viszont igen kevés helyen van.

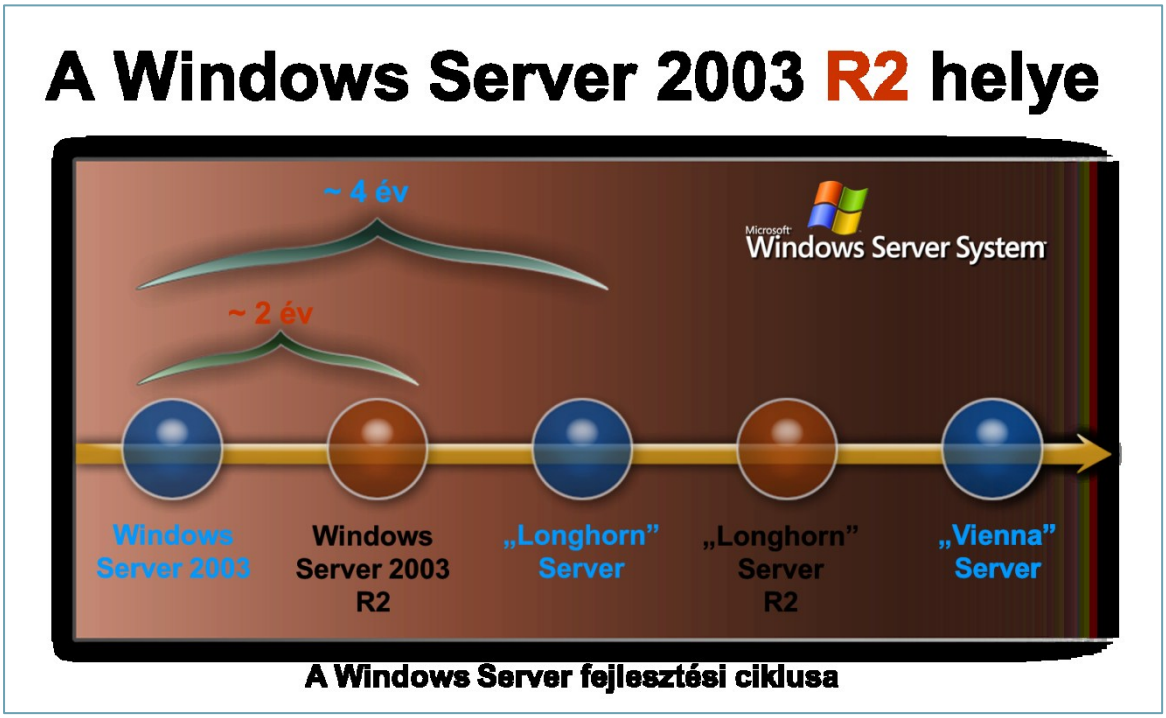
[3] Soha többet nem említem meg ebben a műben a teljes nevet, mivel borzasztó hosszú és többeknek könnyen összekeverhető pl. a Windows Server 2008-cal. Innentől általában R2 néven futunk, és ha esetleg majd a Windows Server 2003 R2-re utalok, akkor ezt külön jelzem.

[4] Hézagos ismereteim szerint több gazdája is van ennek a politikailag szerintem teljesen korrekt kifejezésnek (pl. Fóti Marcell), de én először, sok-sok éve Soczó Zsolttól hallottam és azóta is kéjes örömmel használom.

[5] És nem a Vista RTM-mel, ezt ne feledjük el!

De mi ez az R2 jelzés egyáltalán? Ez a kérdés azért ér egy *bögrét*, mert így kiderülhet az is, hogy hogyan alakult az elmúlt kb. 10 évben a Windows szerverek fejlesztési ciklusa.

Ugyanis a Windows Server 2003-tól kezdve két alapvető (de nem egyforma súlyú) formai dolog is változott a Microsoft hálózati operációs rendszer termékekkel kapcsolatban: 1. A „Server" szó előrecsúszott (lásd Windows 2000 Server, Windows NT Server); 2. A fejlesztési ciklus sűrűbb lett, azaz a 4-5 éves nagyobb intervallumba beesnek a köztes változatok, azaz a Release 2 jelű frissítési példányok. Ezek lényegesen, de tényleg lényegesen sokkal többet nyújtanak mint a szervizcsomagok (SP[6]).
A következő, még 2006-ból, a Lurdy-házból[7] való ábrán ez jól látszik, ugyanis akkor jártunk a Windows Server 2003 R2-nél, ami 2 évvel a Windows Server 2003 után érkezett, és telis-tele volt újdonsággal.



2.1 ÁBRA MÁR AKKOR MEGMONDTUK

> Az iparágunkba később érkezőknek azért elmondom, hogy a „Longhorn" kifejezés a későbbi Windows Server 2008-at és a Vistát jelölte, a „Vienna" pedig a jelenleg szintén még csak kódnévvel rendelkező (bár ez már egy másik) „Windows 8 Server"-t jelöli.

[6] Bár, tegyük hozzá, hogy az XP SP2 óta ezek a klasszikus szervizcsomagok is többet adnak a kezünkbe mint csupán egyszerű javítások sorozatát.
[7] A Microsoft Magyarország évekig a Lurdy-házban tartotta a nagy-nagy, sok száz résztvevős üzemeltetői (IT Pro) konferenciákat.

2.2 AZ ÚJDONSÁGOK DIÓHÉJBAN ÉS SORRENDBEN

Ez a rész kissé megnehezítette a szerző életét, hiszen ha két verzióról beszélünk egyszerre, akkor egyrészt komoly emlékkereső nyomozást kellett végrehajtani (a 2008-as verziót nem nagyon üzemeltetem már sehol), a *dióhéj* meg viccesen szánalmas az újdonságok képzeletbeli listáját tekintve.

Azért megpróbálom, igaz, csak két lépésben.

2.2.1 A WINDOWS SERVER 2008 ÚJDONSÁGAI

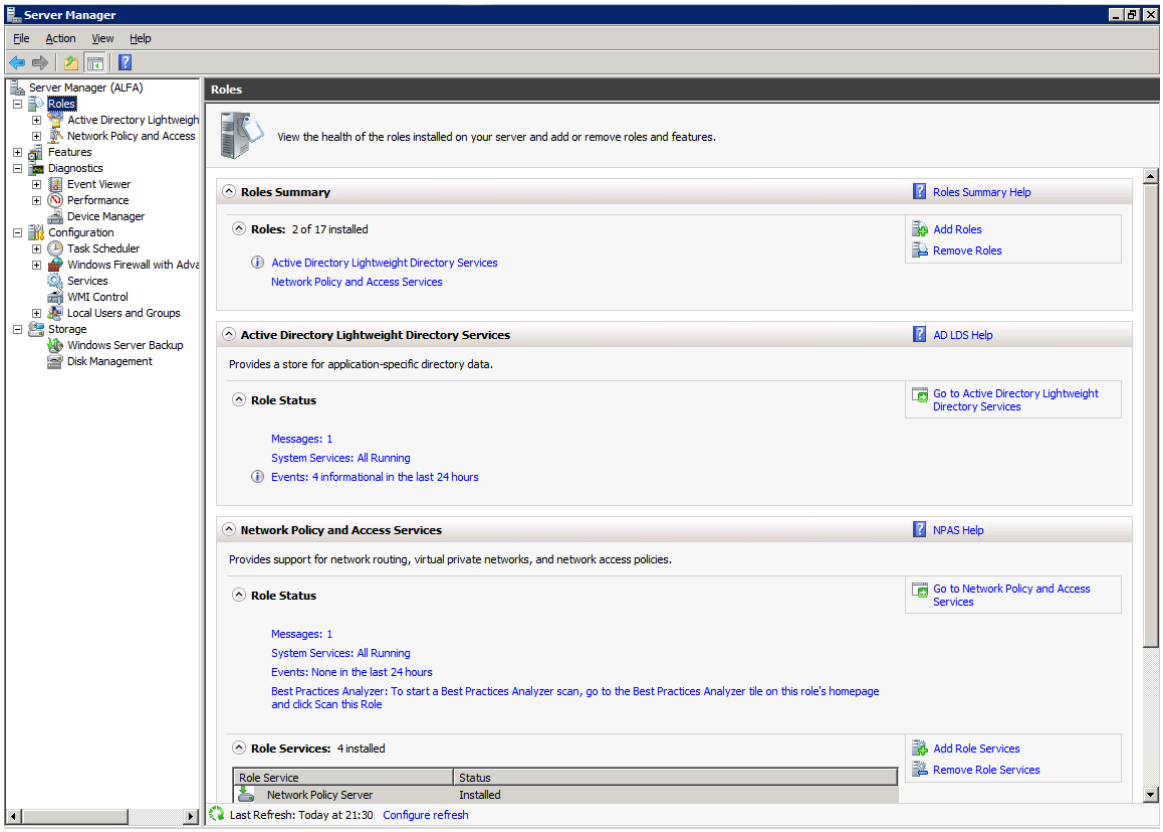
Tehát a Windows Server 2003 R2-höz képest a Windows Server 2008 - kis túlzással -, gyakorlatilag *minden részletében* megváltozott. A felhasználói felülettől kezdve az alapvető biztonsági, hálózati képességeken keresztül a hardver kezeléséig, és még ezen túl is érezhető a gyökeres változás. A Windows Server 2008 automatikusan tartalmazza a Vista SP1 olyan újdonságait, mint például az újraírt hálózatikezelési réteg (pl. natív IPv6, natív vezeték nélküli hálózat, biztonsági fejlesztések); lemezkép alapú telepítés, kiszolgáló konfigurálás és visszaállítás; diagnosztikai, rendszerfelügyeleti, naplózási és jelentéskészítő eszközök; új biztonsági funkciók, mint a DEP, a Bitlocker és az ASLR (véletlenszerű címterület-kiosztás); végre teljesértékű kétirányú tűzfal biztonságos alapértelmezett beállításokkal, megfelelő hardverrel a menet közbeni csere (hot-plugging), kernel-, memóriakezelési és fájlkezelési fejlesztések.

Ezekre az OS alapvető, kliensekre és kiszolgálókra egyaránt jellemző részletekre azért nem térek ki most, mert egyszer már leírtuk nagyon részletesen, három teljes fejezetben a Vista kapcsán, az e könyv elődjének számító *„Rendszerfelügyelet rendszergazdáknak”* című fércműben.

> Mivel rengeteget fogom még emlegetni ezt a forrást, ideje, hogy leírjam az elérhetőségét is (fejezetenként .pdf formátumban letölthető a linkről, de van itt még egy jó pár érdekesség is, pl. a témába vágó rövid videók (screencastok)):
> http://www.microsoft.com/hun/technet/article/?id=f0c8cf69-ae4c-4b1b-b333-9feeda419509

Szóval most (ahogyan ebben a könyvben gyakorlatilag végig) inkább a szerver változatok komponenseire és szolgáltatásaira koncentrálunk. Első nagy témakör a rendszerfelügyelet és a rendszer komponenseinek központi kezelő eszköze, a **Server Manager**, ami egy erősen integrált MMC konzol, a kulcsfontosságú teendők egy helyre koncentrálásával (szerepkörök és szolgáltatások telepítése, törlése,

konfigurálása, ellenőrzése), monitorozással és automatizálással és távoli eléréssel (Powershell[8], WinRM).



2.2 ÁBRA MINDENT EGY HELYEN - INTELLIGENSEN

A következő kiemelendő terület a **virtualizáció**, amely integráltan található meg a Windows Server 2008 óta a Microsoft kiszolgáló operációs rendszerekben. A Hyper-V - meglepő módon – egy hypervisor, ami lehetőséget nyújt olyan virtuális gépek létrehozására, amelyek jobban kihasználják a rendelkezésre álló hardvert, több és akár teljesen eltérő platformú operációs rendszer futtatására alkalmasak, illetve képesek a virtuális és a fizikai erőforrások önálló kezelésére, mindezt persze biztonságosan. Egy jól működő virtualizációs megoldás számos olyan üzemeltetési és technológiai problémát megold, amelyekre a múltban csak nagyon körülményesen tudtunk reagálni, ha sikerült egyáltalán[9].

A **címtárszolgáltatással** kapcsolatos változások és fejlesztések minden új Windows kiszolgáló esetén a fókuszba kerülnek. Nyilván nem véletlenül, hiszen a címtár

[8] Egy a Vista és a Windows Server 2008 érkezése körül megjelent univerzális parancshéj és feladatorientált technológia, amely alkalmazása azóta is töretlen, és ideális eszközként használható a különböző Microsoft szerverek (OS-ek, Exchange szerverek, stb.) felügyeletére és konfigurálására.

[9] És persze nem a klasszikus tételre gondolok ekkor, ami ugye nagyjából így hangzik: *'Az informatikával rengeteg olyan problémát megoldunk, amelyek az informatika nélkül nem léteznének"*. ☺

hierarchia rugalmassága és alkalmazhatósága miatt a tíz és a tízezer gépet tartalmazó hálózatok esetén egyaránt jól használható az Active Directory, mégpedig a minden szervezet számára legfontosabb célra: a felhasználók, a számítógépek és egyéb erőforrások tárolására és kezelésére. Persze, emellett a biztonsági „erőtér" megteremtése és egyéb fontos kiszolgáló alkalmazások, megoldások (Exchange, Csoportházirend, stb.) működésének támogatása is kritikusan fontos feladat. Kisebb és nagyobb változásokat egyaránt észrevehettünk a címtárszolgáltatások területén is a Windows Server 2008-ban. A legjobb ezekben a változásokban az, hogy valódi, életszagú igényeket fedtek le, illetve régóta elvárt, praktikus szolgáltatásokat valósítottak meg, pl. Read-Only tartományvezérlők (RODC), több tartományi jelszó- és kizárási házirend, az újraindítható címtárszolgáltatás vagy éppen a részletes auditálás. De semmiképp ne feledkezzünk meg a Csoportházirenddel kapcsolatos fejlesztésekről sem (erre egy jó péda a kiváló Group Policy Preferences)!

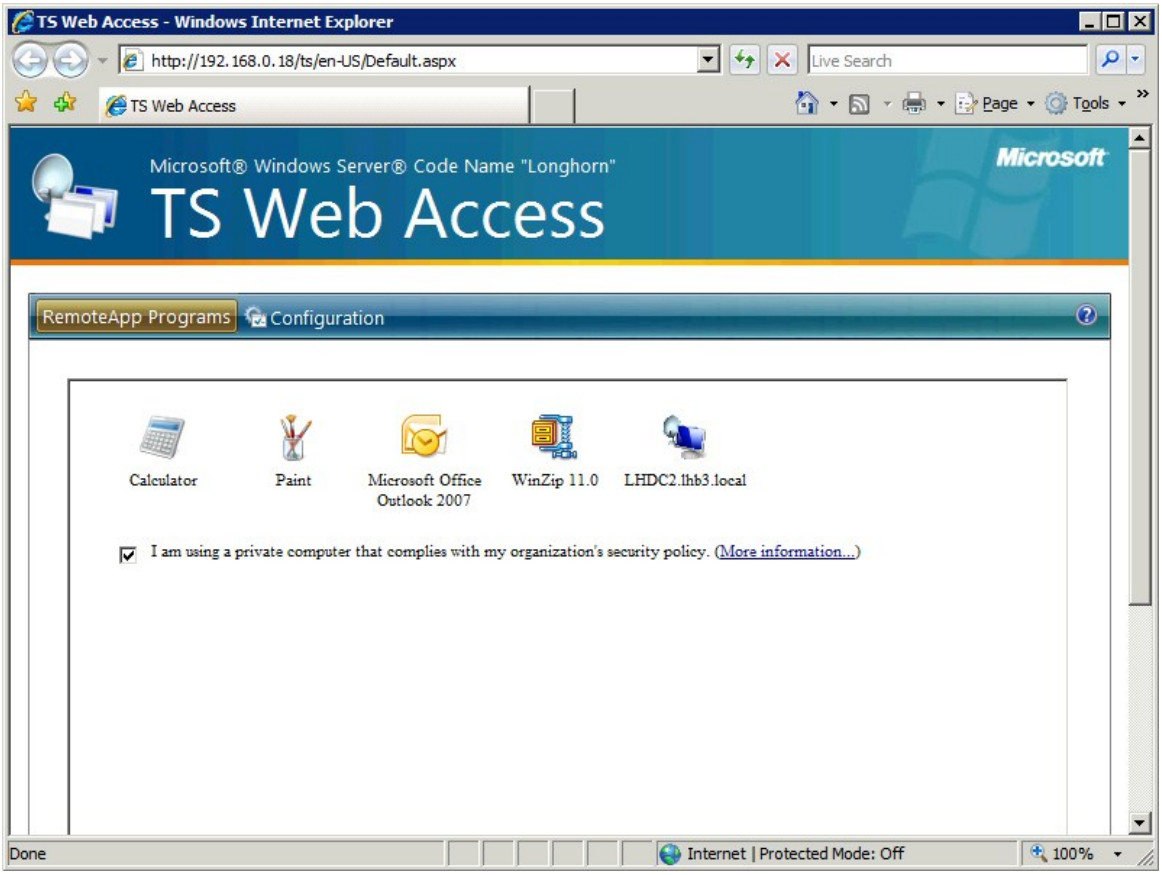
Egy újabb nagyon érdekes terület a **Server Core** nevű ún. telepítési mód (direkt nem kiadást vagy verziót írtam), ami gyakorlatilag egy olyan változata a Windows 2008-as szervereknek, amely majdnem teljes egészében parancssorból fut és a lokális kezelése is csak és kizárólag a parancssori eszközökkel történik. Ez az üzemmód, azáltal, hogy csak a szükséges összetevőket és alrendszereket tartalmazza a grafikus felhasználói felület nélkül, olyan különösen magas rendelkezésre állású kiszolgálót biztosít, amelyet ritkábban kell frissíteni és karbantartani. Elsőre ez biztosan meghökkentőnek tűnik, de működik és nem is akárhogyan.

A Windows Server 2008 rendszerben meghonosított egyik legizgalmasabb új technológia a Microsoft soron következő webkiszolgálója, az **Internet Information Services 7.0**. Az IIS7 valójában több mint egy hagyományos webkiszolgáló – olyan fejlett biztonsági funkciókkal rendelkező és könnyen felügyelhető, ráadásul erősen modularizált platform, amely webalkalmazások és -szolgáltatások fejlesztésére és megbízható üzemeltetésére szolgál. Az IIS7 egyúttal támogatja és egységbe fogja a Windows web platform különböző generációinak technológiáit, köztük az ASP.NET 2.0 keretrendszert, a Windows Communication Foundation webszolgáltatásokat, és persze rengeteg beépített és önálló Microsoft kiszolgáló szerepkört, mint pl. a tanúsítványkiadó szolgáltatást, a Terminal Services komponenst, a Windows SharePoint Services szolgáltatást, vagy akár az Exchange kiszolgálókat is.

A NAP, azaz a **Network Access Protection** valószínűleg a Windows Server 2008 legnagyobb - biztonsággal kapcsolatos - „dobása" volt. Ugyanis a legtöbb szervezet esetén jelentős igény mutatkozik egy olyan megoldásra, amely már a fizikai hálózat szintjén elválasztja az alkalmi csatlakozású vagy kevésbé megbízható illetve kevésbé felügyelhető számítógépeket a belső hálózatba tartozó, ártalmatlan és értékes kliensektől és szerverektől. Erre a láthatóan nehezen megoldható helyzetre nyújthat gyógyírt a NAP, azaz egy olyan szerver-kliens megoldás, amely a védett hálózatunkba

alapértelmezés szerint még az IP kapcsolatot sem engedi meg, és amely csak egy alapos, az üzemeltetők által részletesen hangolható „vizsga” sikeres teljesítése esetén adja meg a hozzáférést a belső hálózathoz kapcsolódni szándékozó gépeknek.

Amikor az emberfia már a bétatesztelés során számba vette, hogy a **terminálszolgáltatások** területén mennyi változás és újdonság jelent meg, akkor arra gondolt, hogy a TS fejlesztő csapat valószínűleg roppant kreatív üzemmódban működött ☺. A Windows Server 2008-nál új képességnek számít – a teljesség igénye nélkül - a RemoteApp, a Web Access, az Easy Printing, sőt, a sorba beletartozott a TS Session Broker és például a Terminal Services Gateway is. Később részletesen kifejtem az újdonságokat, de elöljáróban csak annyit, hogy ha szemléltetni szeretném a változásokat, akkor azt mondanám, hogy ez nagyjából olyan, mintha egy *Suzuki*[10] helyett egyik napról a másikra egy *Maserati Quattroporte*-be ülnénk be.



2.3 ÁBRA EGY FURA ÚJDONSÁG: TS WEB ACCESS A WINDOWS SERVER 2008 EGYIK BÉTÁJÁBAN

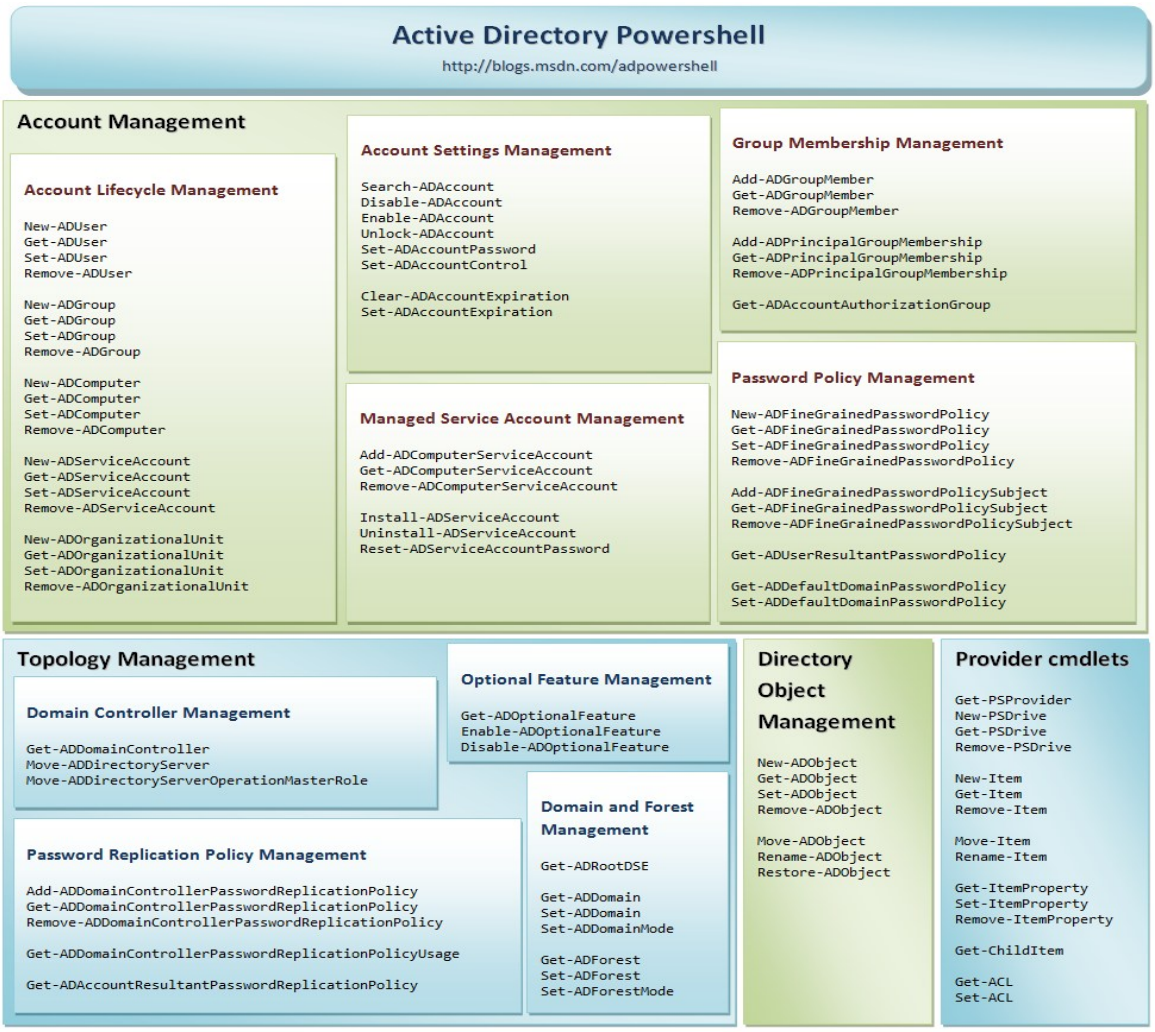
2.2.2 A WINDOWS SERVER 2008 R2 ÚJDONSÁGAI

[10] Nem bántom a Suzukit, a feleségem is egy Ignisszel jár, de muszáj volt egy példa ☺

Erőteljes **hardveres támogatás**, olyan képességekkel, mint például a maximum 256 logikai processzor vagy a SLAT (Second Level Address Translation) támogatás[11], illetve az energiatakarékos működés biztosítása olyan extrákkal mint a Core Parking (a processzor magok dinamikus, használatfüggő ki-be kapcsolása), valamint pl. az OS memóriakezelésének több mint 400 ponton történt korrekciója. Meg kell említeni azt is, hogy az R2 az első olyan operációs rendszer a Microsoft palettáján, amelyből már csak és kizárólag 64 bites változat készült.

A **felügyeleti eszközök** közül elsődleges fontosságú a Server Manager továbbfejlesztése, azaz például a távoli szerverek ezen eszközön keresztüli felügyelete (így a Server Core módú gépeké is), másrészt a PowerShell 2.0 verzióval új eszközökkel is bővült a paletta, amelyek már használhatóak a Server Core, az IIS és az AD alatt is, hiszen az R2-től kezdve ezeken a területeken is van PowerShell támogatás.

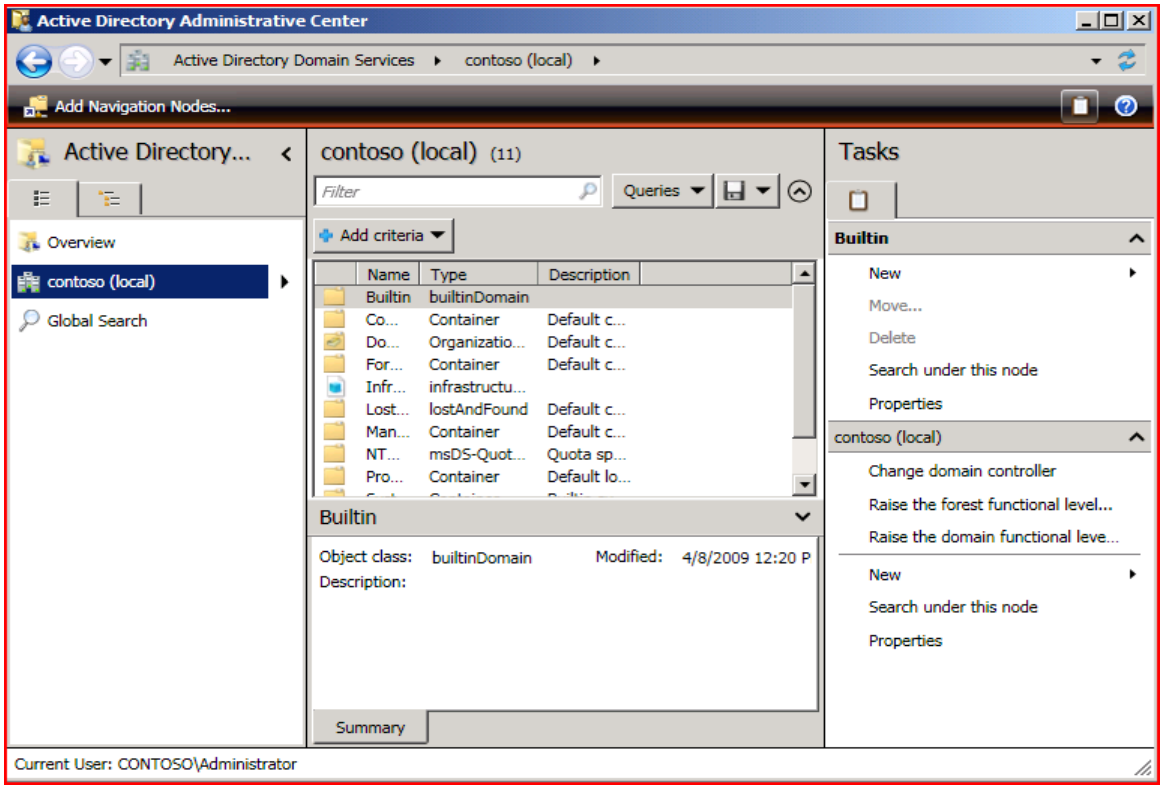
[11] Ez a megoldás a CPU használat optimalizálására törekszik elsősorban a virtualizációnál, ráadásul RAM-ot is megtakarít. Gyártónként más és más egyébként a neve, az Intelnél Extended Page Tables (EPT), az AMD-nél meg Rapid Virtualization Indexing (RVI, korábbi nevén a Nested Page Tables azaz az NPT).



2.4 ÁBRA POWERSHELL MINDENHOL, ÍGY AZ AD-VEL IS

Sőt, ha már itt tartunk, a Server Core alatt a .NET Framework és a tanúsítványszolgáltatások is használhatóak. De megjelentek a Server Manager-be integrált BPA (Best Practice Analyzer) komponensek is, amelyek a hibafelderítésben és problémamegoldásban segítenek rengeteget az üzemeltetőknek.

A **címtárszolgáltatások** területén több nagy durranás is elérhetővé vált, pl. a Recycle Bin, azaz az AD Lomtár, vagy az Offline Domain Join (a kliensek fizikai kontaktus nélküli beléptetése a tartományba), vagy a teljes új felületen, azaz egy webszolgáltatáson keresztül elérhető AD Administrative Center, de nem maradhat ki az egy régi-régi problémára megoldást nyújtó Managed Service Accounts (felügyelt szolgáltatás fiókok) sem, és persze a Csoportházirendbe is kerültek új technikai megoldások.



2.5 ÁBRA AD AC (MAJDNEM AC/DC, DE AZÉRT NEM)

Az R2-ben már a **Hyper-V második generációs** változata érhető el, több kulcsfontosságú területen is továbbfejlesztették, így aztán lényegesen nagyobb rendelkezésre állást és teljesítményt biztosít (pl. 64 logikai processzor támogatás a host gépen, illetve 384 db egyprocesszoros virtuális gépet is futtathatunk), miközben izmosabb felügyeleti és egyszerűsített rendszerbe állítási eljárásokat kínál, és olyan új szolgáltatásokat is tartalmaz, mint a működés közbeni, „élő" áttelepítés (Live Migration) vagy a lemezek dinamikus hozzáadása és elvétele.

A **hálózati szolgáltatásokkal** kapcsolatos szerver technológiák vagy praktikus továbbfejlesztéseken mentek át, mint pl. a DNS vagy a DHCP szerver, az SSTP VPN, vagy éppen új megoldások születtek, mint az IKEv2 VPN vagy egy szenzációs technikai megvalósítású újdonság a távoli elérés területén, a DirectAccess. Ez utóbbi egy IPv6 és IPSec alapokon nyugvó, állandó távoli elérést jelent elsősorban a mobil felhasználók esetén, és úgy VPN, hogy nem is az ☺

A korábbi Terminal Services névváltozáson ment keresztül, immár **Remote Desktop Services** a neve, és megint csak újabb megoldásokkal és eszközökkel egészült ki, amelyek közül kimagaslik a Hyper-V-vel és az Active Directory-val együttműködő VDI (Virtual Desktop Infrastructure) infrastruktúra építésének támogatása, ami egy olyan központosított munkaállomás-szolgáltató architektúra, amely lehetővé teszi a Windows és más munkaállomás-környezetek futtatását és felügyeletét a központi kiszolgálón található virtuális gépeken, többek között például az RD Web Access felületén keresztül.

A **telephelyes környezetek** támogatása is gőzerővel zajlott, ennek folyománya lett az egészen zseniális megoldású BranchCache képesség és a read-only DFS-R, azaz a replikációs szolgáltatások RODC-khez passzoló változata.

Ennyi a rövid és abszolúte nem teljes képesség felvezetés, de talán már most is látszik, hogy a következő majdnem 300 oldalon lesz miről olvasni.

3 TERVEZÉS ÉS TELEPÍTÉS

3.1 KIADÁSOK ÉS FELTÉTELEK[12]

Az összes kiadás tekintetében felforgató jellegű változás nincs, de azért akad egy-két érdekesség. Íme a lista:

- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter
- Windows Web Server 2008 R2
- Windows Server 2008 R2 for Itanium-Based Systems
- Windows Server 2008 R2 Foundation

A klasszikus Standard, Enterprise és Datacenter mellett a Web Server is lassan szokásossá válik. Ennél a négy változatnál a Server Core telepítési mód is „jár" (de vagy-vagy tehát nem pluszban kapunk hozzá egy licencet). Az Itanium kiadásról maximum azt kell tudni, hogy elvileg ez lesz az utolsó verzió ebből a típusból. A Foundation kiadás teljesen új, és a Small Business változatok[13] alá „lövi be" a Microsoft, tehát egészen kis cégeknek. Ez nagyon szépen látszik a szép mennyiségű szoftveres és hardveres korlátból is, viszont a jelentősen alacsonyabb ár szimpatikusabb tényező ebben a szegmensben, mint az elérhető szolgáltatások széles választéka.

A 3.1-es ábra megér pár misét, ergo összefoglalnám a lényeget egy felsorolásban:

- Az „X64 Sockets" egyértelműen jelzi, hogy az R2-nél csak és kizárólag 64 bites kiadásaink vannak (a Windows Server 2008-nál még volt 32 bites is).
- A foglalatok (és nem magok!) sorában maximum a Foundation érdekes, azaz a maximum 1 CPU korlát.
- A memóriánál szintén, bár ha a virtualizáció is lényeges (és ha még az elejénél, azaz a tervezésnél még nem is, később tuti az lesz :D), akkor az Enterprise-ig tartó 32 GB-os RAM korlát adott esetben szűk is lehet, persze ebben az esetben más oka is lesz majd az Enterprise kiadásnak, lásd később.
- A „Hot…" részeket átugorva vegyük figyelembe, hogy a Failover Cluster szolgáltatás az Enterprise-nál kezdődik (viccesnek és kitaláltnak tűnhet, de láttam már olyat, ahol ezt nem sikerült figyelembe venni).

[12] Még egyszer felhívnám a figyelmet, hogy innentől – ha külön nem említem - akkor csak az R2-vel foglalkozunk, hiszen úgyis minden benne van, ami a közvetlen elődjében.

[13] Ha a Small Business Server kategóriában szeretnénk az R2-es verziójú operációs rendszert használni, akkor a SBS 2011 lesz a mi barátunk (no és persze az Exchange 2010 és még 1-2 további dolog miatt egyébként is).

- A Network Access Connections korlátnál gondoljunk először a VPN-re, azaz ha például a kiváló Forefront TMG-vel VPN szervert tervezünk, és 250-nél több felhasználót kell majd kiszolgálnunk, akkor az Enterprise kiadás a jó választás. Ugyanennél a témánál maradva, ha a RADIUS klienseink száma is több lesz, mint 50, akkor még egy érvünk van a magasabb kiadás alkalmazására, és persze az RD Gateway-nél is van egy hasonló korlátunk, amit épp ezért lehetséges, hogy figyelembe kell majd vennünk. Ugyanezen korlátok lényegesen szigorúbbak a Foundation kiadásnál, de hát valamit valamiért.

Specification	Web	Standard	Enterprise	Datacenter	Itanium	Foundation
X64 Sockets	4	4	8	64	○	1
IA64 Sockets	○	○	○	○	64	○
X64 RAM	32 GB	32 GB	2 TB	2 TB	○	8 GB
IA64 RAM	○	○	○	○	2 TB	○
Hot Add Memory	○	○	●	●	●	○
Hot Replace Memory	○	○	○	●	●	○
Hot Add Processors	○	○	○	●	●	○
Hot Replace Processors	○	○	○	●	●	○
Failover Cluster Nodes (Nodes)	○	○	16	16	8	○
Fault Tolerant Memory Sync	○	○	●	●	●	○
Cross-File Replication (DFS-R)	○	○	●	●	●	○
Network Access Connections (RRAS)	○	250	Unlimited	Unlimited	○	50
Network Access Connections (IAS)	○	50	Unlimited	Unlimited	2	10
Remote Desktop Services Gateway	○	250	Unlimited	Unlimited	○	50
Virtual Image Use Rights	Guest	Host + 1 VM	Host + 4 VM	Unlimited	Unlimited	○
Remote Desktop Admin Connections	2	2	2	2	2	2

3.1 ÁBRA CSAK KARIKÁK ÉS GOLYÓK, DE A LÉNYEG AZÉRT BENNE VAN

- Az utolsó előtti sor kifejezetten fontos, ha virtualizációt tervezünk, és nem óhajtunk *bebukni* a licencelésen. A Standard verziónál a „Host + 1 VM” azt jelenti, hogy maximum 1 virtuális gépet állíthatunk munkába, de csak akkor, ha a host gépnek nincs semmilyen szerver szolgáltatása (a Hyper-V nem az ebből a szempontból). Tehát ha pl. tartományvezérlő vagy éppen egy NAP szerepköre van, akkor már nem lehet pluszban legálisan egy virtuális szerverünk. Az Enterprise-nál ugyanez a helyzet, csak a képlet végeredménye más: a használandó virtualizált gépek száma a host párhuzamos használata (úgy értem, valamilyen szerepkörrel a Hyper-V-n kívül) mellett maximum 4 lehet. Ha sok virtuális gépünk van, akkor egyértelműen a Datacenter kiadás lesz a nyerő a korlátlan virtuális gép licence-szel[14], de persze ahogy itt is, a többi esetben is ki kell számolni, hogy melyik a megfelelő konstrukció.
- A Remote Desktop Admin Connections, az admin tehát a felügyeleti RDP kapcsolatok maximális számát jelentik, ami egységesen és összesen 2 darab a Windows Server 2008 óta.

[14] Vigyázat, a Datacenter kiadás licenszelése - a többi kiadástól eltérően - processzorszám alapján történik (a lektor megjegyzése).

Az egyéb, főképp hardveres telepítési előfeltételek (most a „clean”, azaz a tiszta vagy szűz telepítésről beszélünk) hivatalos listája a következő:

Komponensek	Követelmények
CPU	• Minimum: 1.4 GHz (x64 processzor) • Ajánlott: 2 GHz vagy gyorsabb Megjegyzés: Ha az Itanium platform a célpont, akkor az Intel Itanium 2 típusú CPU lesz a minimum követelmény
RAM	• Minimum: 512 MB RAM • Ajánlott: 2 GB RAM vagy több
Tárhely	• Minimum: 10 GB • Ajánlott: 40 GB vagy több Megjegyzés: Ha minimum 16 GB RAM van a rendszerünkben, akkor ezt figyelembe kell venni a tárhelynél is a pagefile, a hibernálás vagy a memória dump fájlok miatt, tehát ezek apropóján pluszban számoljunk tárhellyel
Lemezmeghajtó	Csak DVD-ROM
Monitor és perifériák	• Super VGA (800 x 600) vagy nagyobb felbontás • Billentyűzet, egér

3.2 ÁBRA A KÖVETELMÉNYEK LISTÁJA

Ennek a táblázatnak (ahogy mindegyik ilyesfajta követelménylistának) jó néhány része egészen vicces[15], és kissé ellentmond a hétköznapi gyakorlatnak, de egy biztos, tökéletesen általános recept nincs, gyakorlatilag minden esetben egyedileg kell megterveznünk a hardver eszközöket - az elvárásokkal szinkronban. Még egy fontos és ez esetben ténylegesen életszagú tapasztalatra hívnám fel a figyelmet: annak ellenére, hogy újabb, „többet tudó” és több mindenre használható az R2 verzió az elődjével szemben, a hardverigénye kevesebb vagy legalábbis megegyezőnek bizonyul majd. Ez a rengeteg ponton (CPU, memória, diszk, hálózat) korrigált rendszernek köszönhető. [16]

A jogtiszta használat apropóján jegyezzük még meg azt a tényt is, hogy a Windows Server 2003-hoz képest drasztikusan, de a Windows Server 2008-hoz képest is jelentősen enyhült az aktiválással kapcsolatos kemény hozzáállás a gyártó cég

[15] Viszont a minimum feltételek negligálása egy bejelentett PSS hiba esetén nagyon is számít, tehát a támogatás elveszítésével jár (a lektor megjegyzése).
[16] És még egy fontos dolog: mivel egy 64 bites rendszerről van szó, minden meghajtóprogramnak (driver, hogy értsük) rendelkezni kell digitális aláírással.

részéről. Ennek egyik következménye az, hogy a telepítés után 60 napig aktiválás és termékkulcs bevitel nélkül, teljes értékű üzemmódban használhatjuk a szervert. Egy másik fejlemény pedig az, hogy teljesen legálisan kiterjeszthetjük ezt az üzemmódot további 180, tehát összesen 240 napig. Ezután viszont muszáj lesz egy érvényes termékkulccsal aktiválnunk, vagy ennek híján el kell távolítanunk az operációs rendszert.

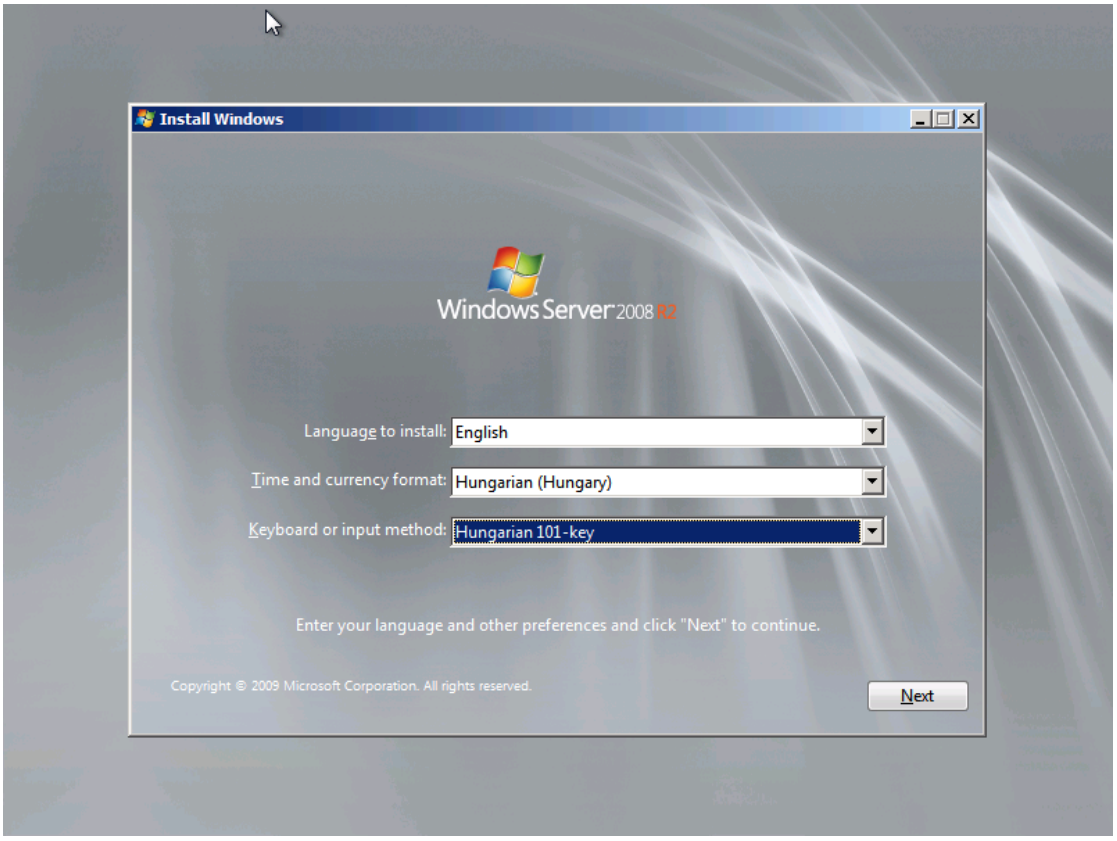
> Ha erről a speciális használat kiterjesztésről többet szeretnénk tudni, akkor nézzük meg a részleteket a következő hivatkozáson:
> A Windows Server 2008 próbaidejének meghosszabbítása
> http://support.microsoft.com/kb/948472

3.2 TELEPÍTENI KÖNNYŰ

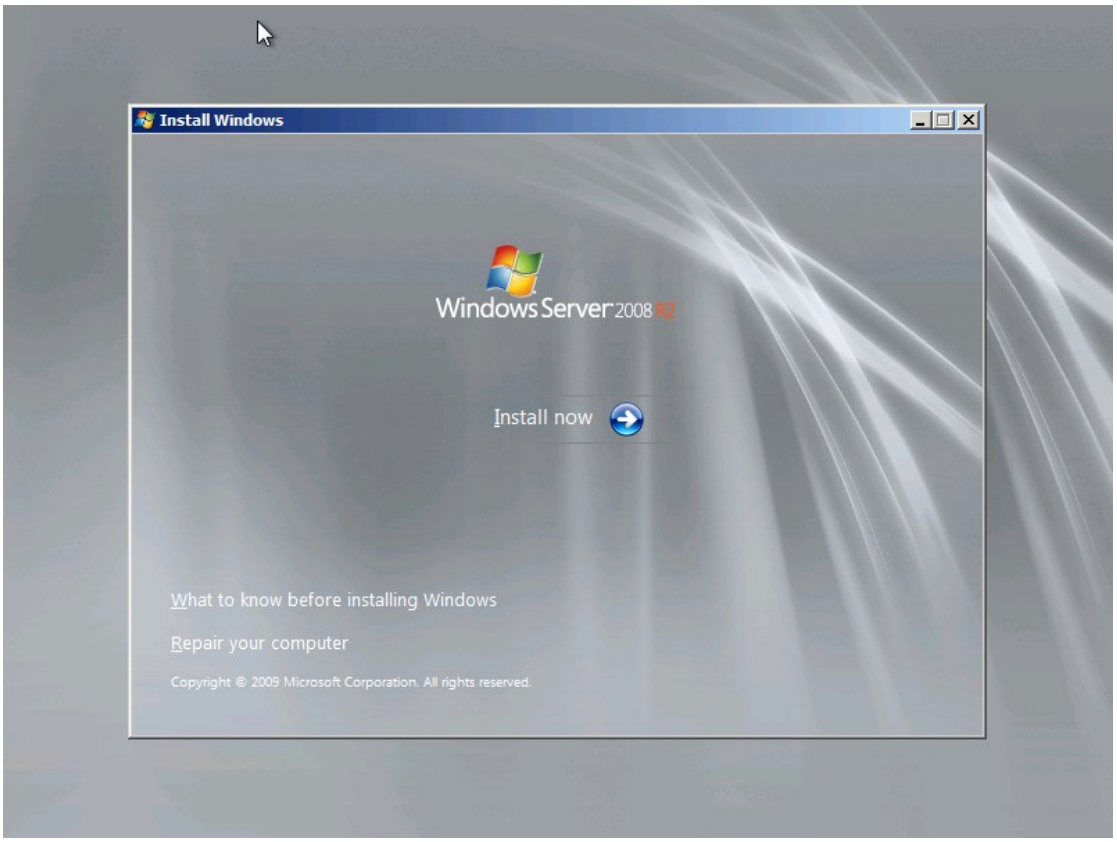
És tényleg az, mégpedig egyre könnyebb. A Vista óta az OS telepítés jelentősen egyszerűsödött, minimális beavatkozást igényel, és adott esetben nem akad meg, ha valamit nem tudunk azonnal beadni a telepítőnek (pl. termékkulcs a klienseknél) illetve a komponensekkel telepítés közben nem kell foglalkoznunk. De azért tekintsünk végig egy komplett folyamatot, mert minimum egyszer azért meg kell ismernie mindenkinek a lehetőségeket!

Szóval rendszert indítunk a DVD-vel (egy darab van jellemzően az összes kiadással, de ez sem újdonság már) vagy egy .iso fájlból Hyper-V alatt - mint az én a példámban - vagy esetleg VHD boot-tal, amiről viszont majd később lesz szó.

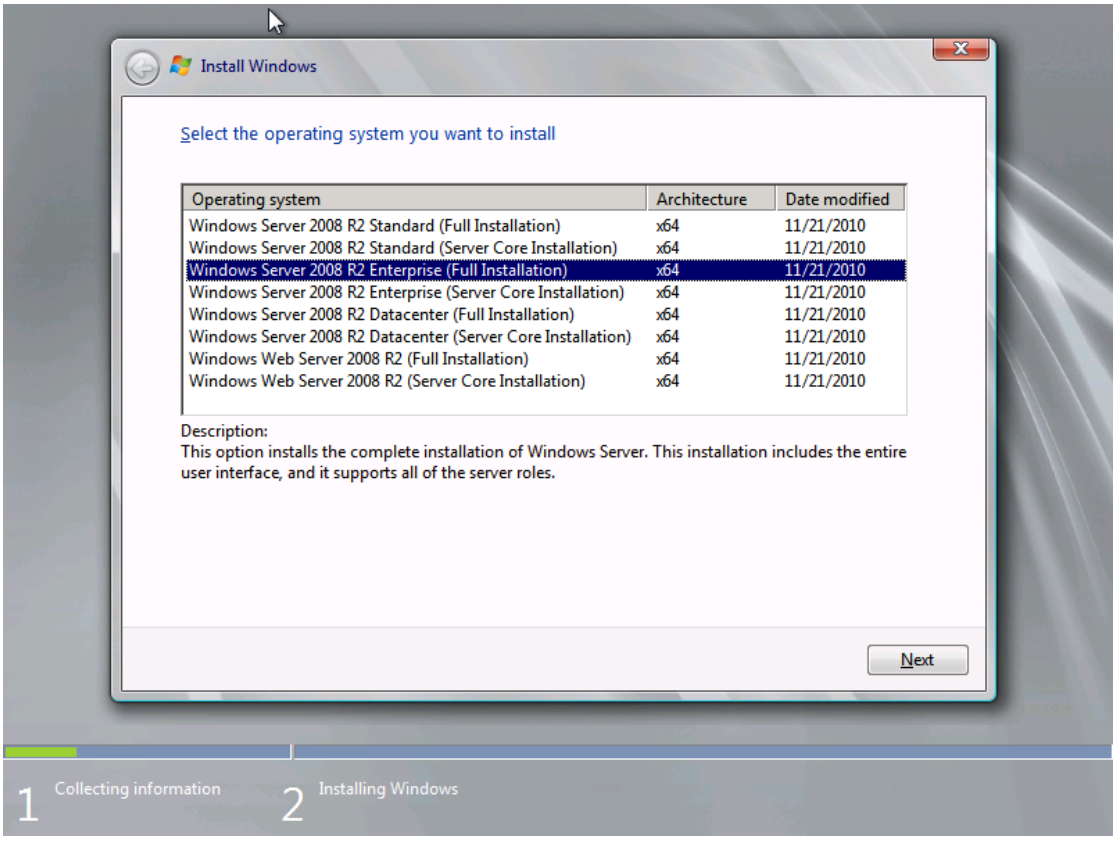
3.2.1 A KLASSZIKUS TISZTA TELEPÍTÉS LÉPÉSEI



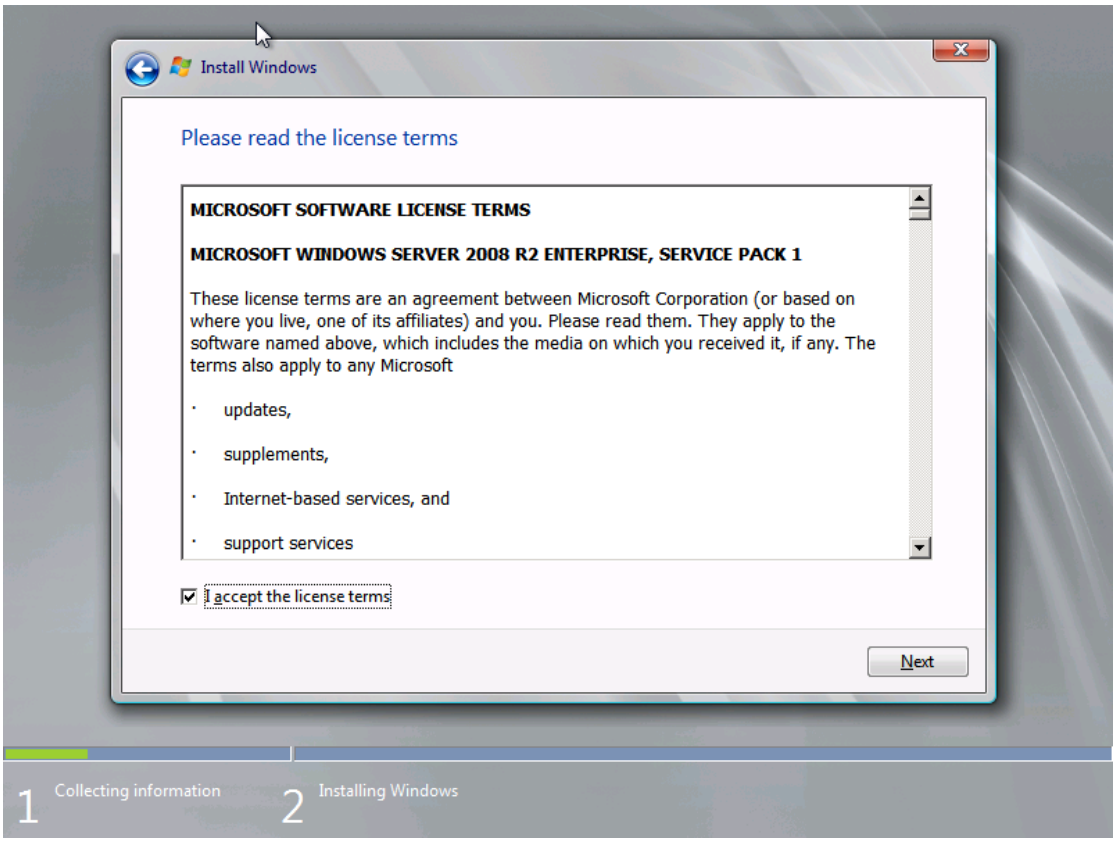
3.3 ÁBRA A 16 ÉVE DOLGOZÓ RENDSZERGAZDA A 101 GOMBOS BILLENTYŰZET HÍVE



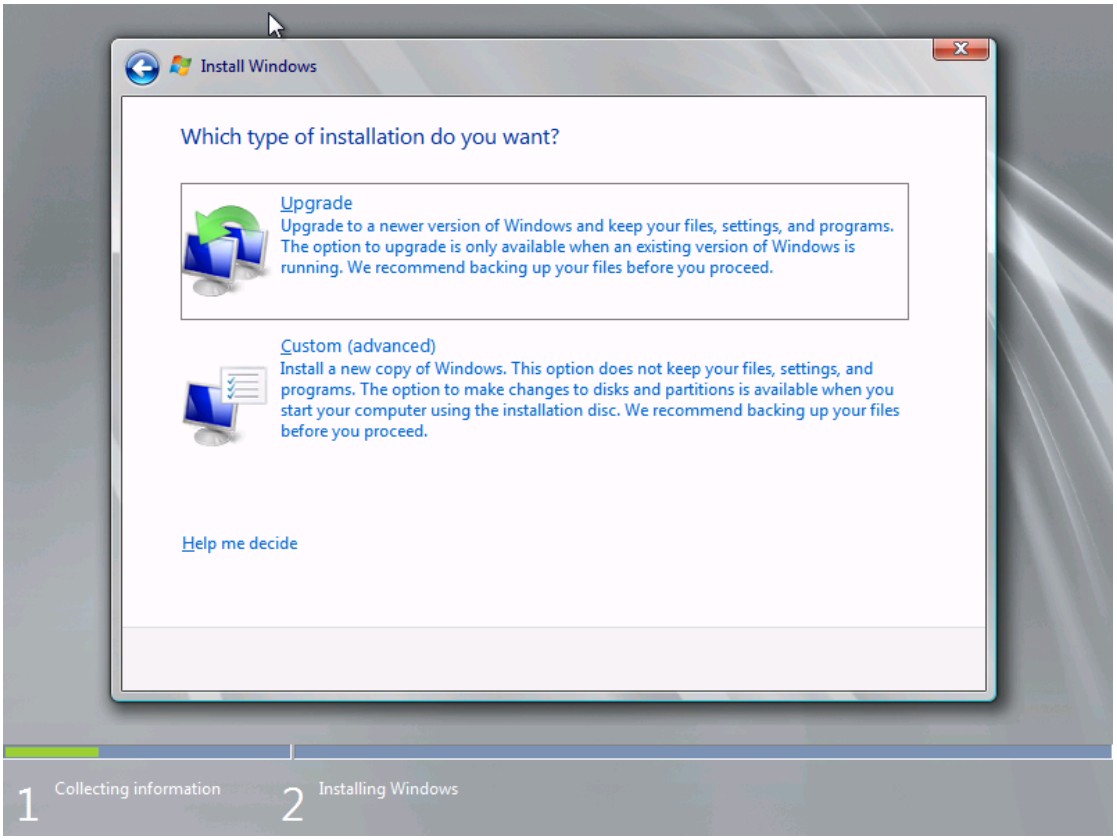
3.4 ÁBRA BALRA LENT EGY OLVASNIVALÓ ÉS A MENTÉS FEJEZETBEN KITÁRGYALT WRE INDÍTÁSI LEHETŐSÉGE



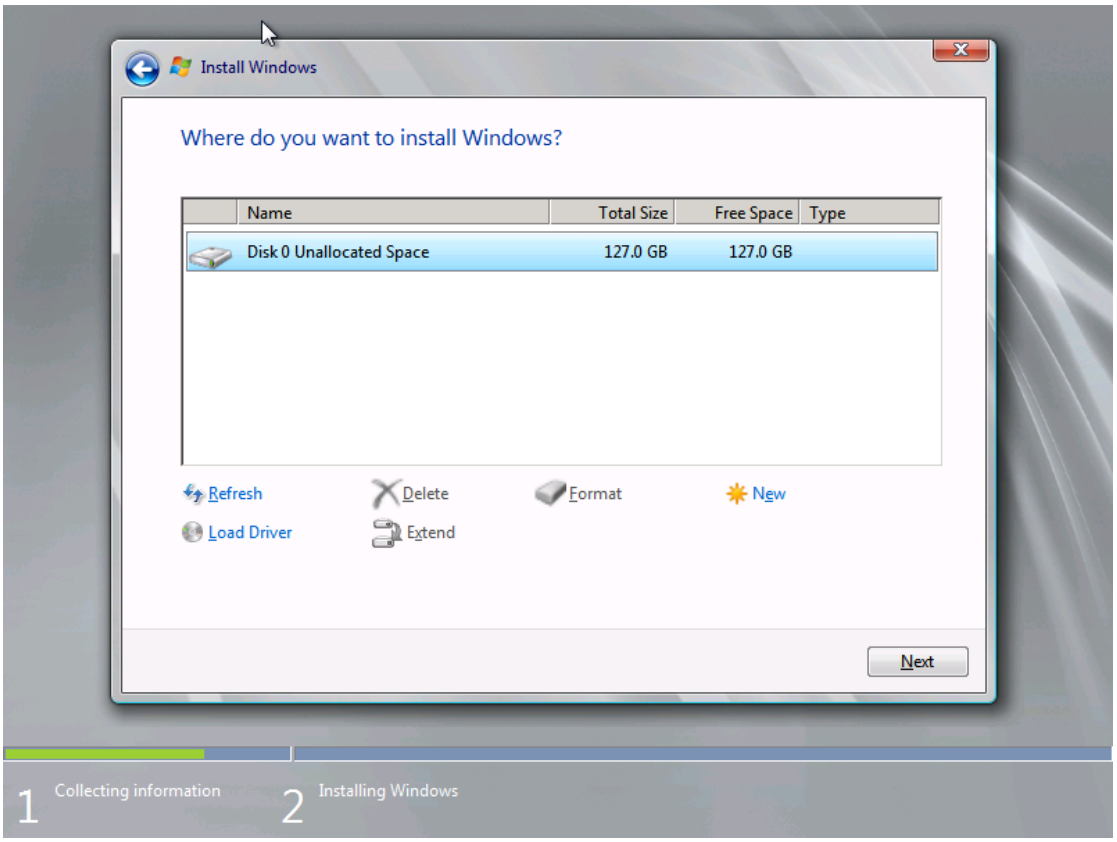
3.5 ÁBRA 4 SIMA, 4 SERVER CORE (DE JEGYEZZÜK MEG ÚJRA: VAGY-VAGY)



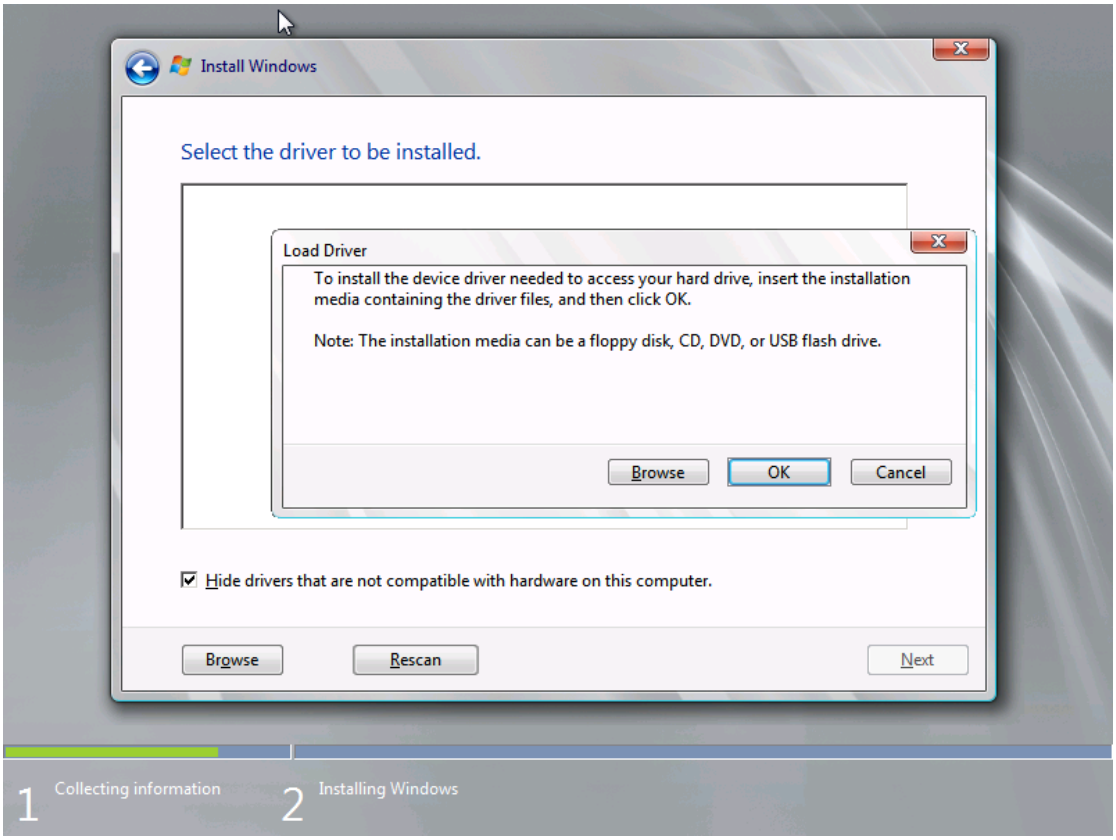
3.6 ÁBRA AZ EULA (MAXIMUM AZ AZ ÉRDEKES, HOGY EZ MÁR EGY SP1-ES INTEGRÁLT EULA ☺)



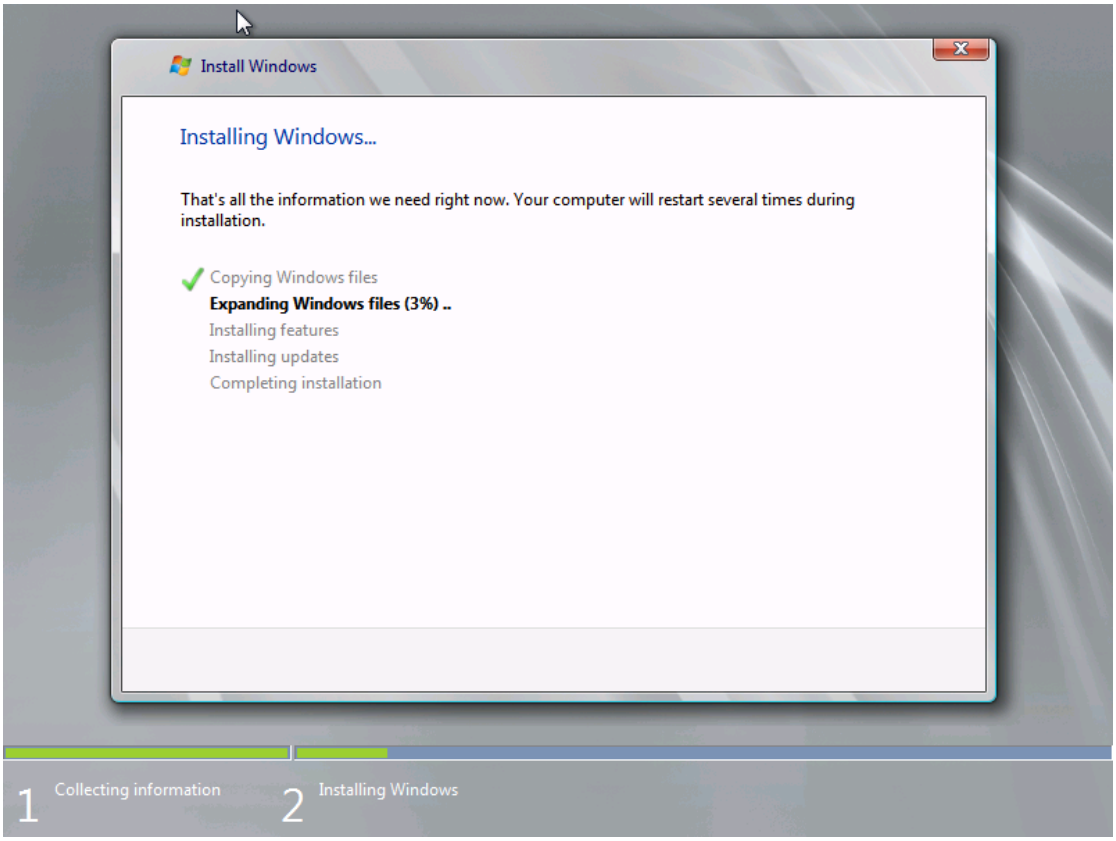
3.7 ÁBRA EZ ITT A NAGY KÉRDÉS (95%-BAN AZ ALSÓ LESZ, RÉSZLETEK KÉSŐBB)



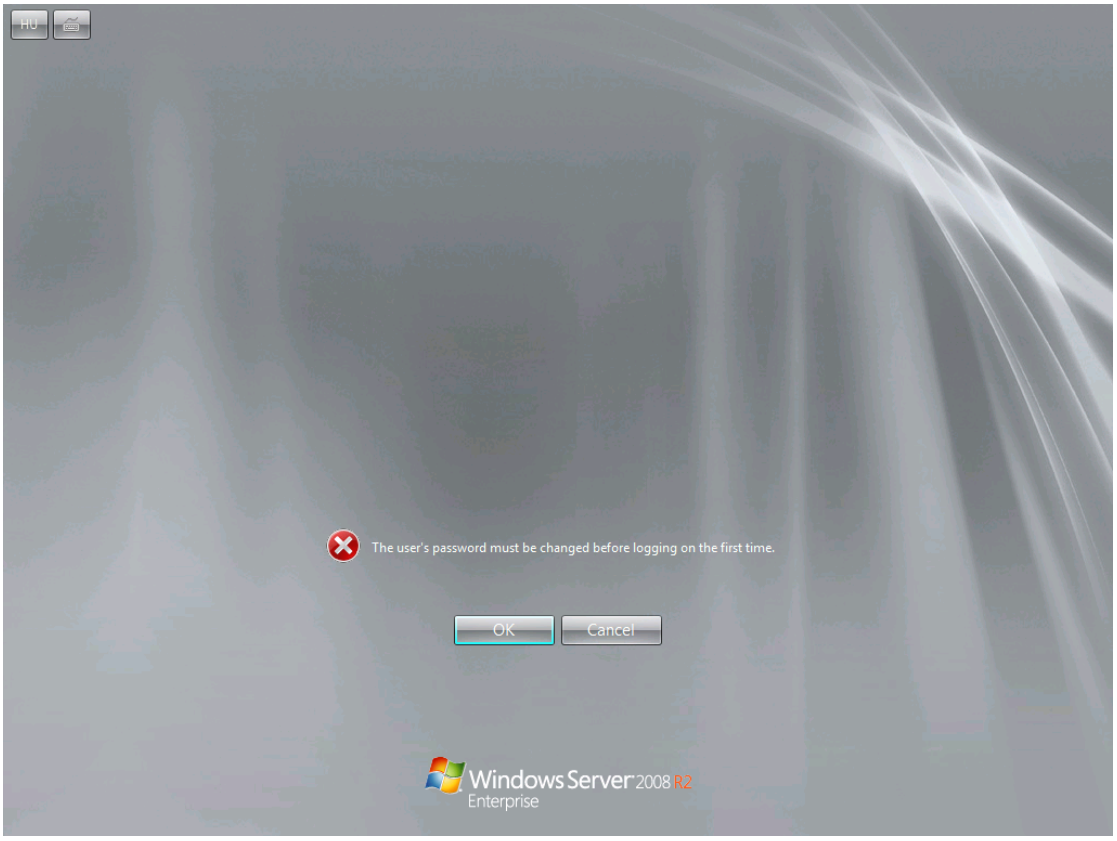
3.8 ÁBRA LEMEZKEZELÉS EGYSZERŰEN, AZ EGYETLEN ISMERETLEN A KÖVETKEZŐ KÉPEN (LOAD DRIVER)



3.9 ÁBRA HA MEGHAJTÓ PROGRAMOT KELL BEILLESZTENÜNK, PL. A RAID VEZÉRLŐHÖZ AKKOR ITT AZ IDEJE



3.10 ÁBRA MÁSOLÁS, KICSOMAGOLÁS, KONKRÉT TELEPÍTÉS, FRISSÍTÉS ÉS KÖZBEN ÚJRAINDÍTÁS IS LESZ, KÉTSZER IS – ÚGYHOGY MENJÜNK KÁVÉZNI

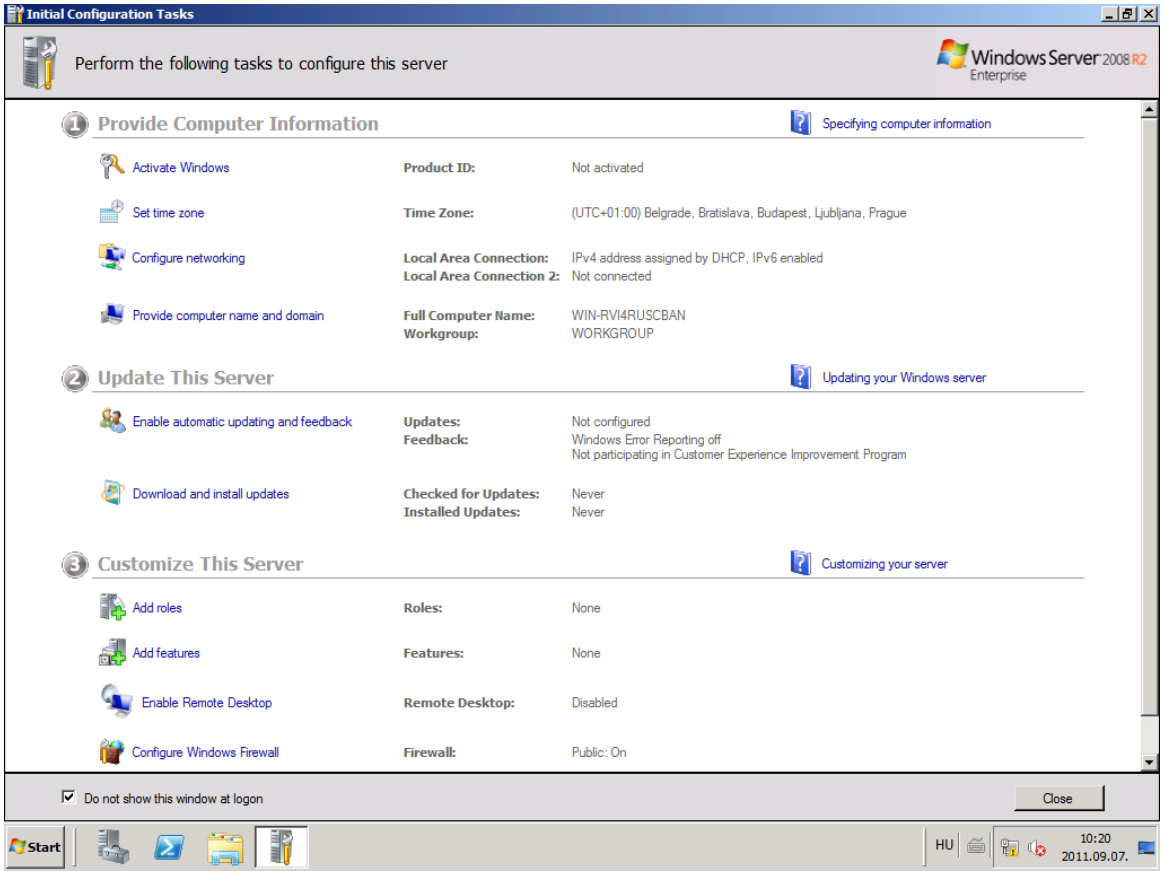


3.11 ÁBRA AZ ADMIN JELSZÓ BEÁLLÍTÁSÁVAL VÉGE IS A FOLYAMATNAK

Szemben a Windows Server 2003-mal, az admin jelszó megadásánál ügyeljünk arra, hogy már itt is (lokális gépen, tartomány nélkül is) működik a kemény jelszóházirend, azaz minimum 7 karakter, és a kisbetű, nagybetű, szám, jel négyesből háromnak szerepelnie kell a jelszóban, valamint 42 nap múlva lejár az alapértelmezés szerint[17].

A telepítés tényleg egyszerű, de ezzel még teljesen nem ér véget, hiszen a jelszóváltoztatás és a profilunk betöltése után következő lépés is egy varázslás, azaz az „Initial Configuration Tasks”.

[17] No és persze, ha a gépet tartományba léptetjük, akkor a tartományi jelszóházirend lesz az érvényes az odatartozó, de az ezen a gépen belépő felhasználók esetén.



3.12 ÁBRA AZ ALAPVARÁZSLÁS INDUL

Hasznos dolog ez a felület, mert a legfontosabb alapbeállításokat (hálózat, gépnév, tartományi tagság, Windows Update, Remote Desktop, tűzfal) itt azonnal és egy helyen megtehetjük, ha viszont csak egyszer akarjuk látni, azaz elegünk lett belőle, akkor a bal alsó sarok fontos lesz („Do not show this window at logon").[18] De ha szükséges, akkor az alapbeállítások nyomtatása, emailben elküldése vagy lementése sem okoz gondot.

De ezek után még mindig nincs vége a varázslásnak, hiszen azonnal megkapjuk a Server Managert, ahol szintén van pár teendőnk a folyamat elején is, és persze később is rengetegszer ellátogatunk majd még ide. Azonban ez már a 4. fejezet anyaga, ergo lépjünk vissza kicsit!

3.2.2 A CSENDES (UNATTENDED) TELEPÍTÉS

Akadhat olyan szituáció, amikor nem tudjuk (vagy nem akarjuk) a kattintgatást művelni telepítés közben, illetve az egyik legfontosabb okként inkább azt hoznám fel, amikor is rengeteg szervert kell azonos módon telepítenünk. Erre egy egyszerű megoldás általában a csendes telepítés (és persze nem csak operációs rendszereknél, alkalmazásoknál is van erre opció), és van rengeteg más megoldás is,

[18] Egyébiránt mind az ICT, mind a Server Manager indításkori megjelenését vagy tiltását a Csoportházirendből szabályozhatjuk.

amelyek lényegesen több lehetőséget rejtenek magukban, ám egyúttal sokkal bonyolultabbak is (lásd: tömeges telepítés, azaz „*mass deployment*”).

Visszatérve a csendes telepítés lebonyolításához is szükség lesz jó pár teendőre, de ezeket szerencsére csak egyszer kell megtenni, és aztán sokszor élvezni a hasznát. Szükségünk lesz a Windows Automated Installation Kit (WAIK) legfrissebb változatának letöltésére[19], ami egy ingyenes eszköz és a Microsoft Download Centerben[20] találjuk meg. A WAIK egyik alapkomponensével azaz a Windows System Image Manager-rel (WSIM) készíthetünk egy ún. distribution share-t (és így persze a hálózaton keresztüli telepítés lehetőségéhez is hozzájutunk), és a WSIM grafikus felületén, rengeteg opcióval egy unattend.xml fájlt, amellyel aztán az összes telepítés előtti, alatti és utáni műveletet nagyon granulárisan szabályozhatjuk, és ha ezt megtesszük akkor ezek után a telepítési folyamat is minimális beavatkozást igényel majd.

Persze ez a téma, mármint a tömeges telepítés, hiperbonyolult is tud lenni (pl. további 3 és 4 betűs rövidítésű eszközök garmadája áll a rendelkezésünkre, WDS, MDT, Lite/Zero Touch Install - talán ezek a legfontosabb kulcsszavak), így aztán meg sem próbálom ennél jobban ebben a fejezetben kifejteni.

3.3 Frissítés vagy migráció?

Általában a rendszergazda szakmai életének egyik komoly dilemmája ez a kérdés, ami ráadásul rendszeresen visszatér, hiszen 3-4 évente biztosan kapunk új operációs rendszereket és persze szerver alkalmazásokat (gondoljunk az Exchange vagy a TMG szerverre), és a cserét még egy jól működő rendszerben is meg szoktuk és meg is kell lépni az ideális rendszer[21] elérése apropóján (nyilván ez sosem fog sikerülni, de azért csak csináljuk és csináljuk és csináljuk ☺).

Történetesen az a helyzet, hogy mindkét megoldásnak számtalan előnye van, ám a hátrányokkal is hasonlóan állnak. Ha például frissítünk helyben (in-place upgrade), akkor:

- A feladat lényegesen egyszerűbb, mivel az alkalmazások, a beállítások, a környezet marad régi – csak éppen a rendszer komponensei frissülnek.

[19] Vagy inkább az MDT-re (Microsoft Deployment Toolkit). Az MDT desktop oldalról ismerős lehet, jó megjegyezni, hogy ugyanazok az eszközök működnek a szervereknél is. Az MDT-nek része a WAIK, továbbá az extra bonyolult WSIM helyett is egy barátságosabb task sequence állítható össze (a lektor megjegyzése).

[20] http://www.microsoft.com/download/en/default.aspx

[21] Az ideális rendszer - az ideális gázhoz hasonlóan - mindig kitölti a rendelkezésére álló teret (a lektor megjegyzése).

- A frissítés után - optimális esetben - egyből működik minden, nem változik a szerver neve, sem a TCP/IP beállítások, sem semmi más, a kliensek ugyanúgy látják, és ugyanazt biztosan meg is kapják ettől a szervertől, mint eddig.

Ha naiv rendszergazdák vagyunk, akkor már dörzsölhetjük is össze a kezeinket, nincs kérdés, ez lesz a nyerő! De nem biztos, mivel:

- A hardver egész egyszerűen nem bírja el az új OS-t, tehát ugyanerre a gépre nem lehetséges feltenni. Változnak az idők, a hardverspirál működik, az eszközök szempontjából halott ügy a frissítés, meg aztán egyébként is szeretnénk új hardvert, mert ki nem ebben a szakmában? ☺
- Az operációs rendszer nem frissíthető helyben, mert:
    - Eltérő a platform (32 bit > 64 bit vagy esetleg fordítva), erre jó példa 98%-ban a Windows Server 2003-ról Windows Server 2008 R2-re való átállás, hiszen az utóbbiból ugye nincs is 32 bites.
    - Eltérő a nyelv (eddig magyar volt, de okosabbak lettünk, ☺[22] és angolt szeretnénk használni).
    - Eltérő a kiadás, például eddig Small Business Server-t használtunk, de... kinőttük.
- A gép már túlélt pár évet, teli van szemetelve, már az előző váltásnál is helyben frissítettünk, ergo szoftveres szempontból is elavult, és nagyon szeretnénk tiszta lappal indulni.
- Az időzítés fontos, ha frissítünk, akkor azt egy adott időpontban tesszük meg, és egyből az 1-ről a 2-re jutunk. Visszavonni a változásokat általában problémás vagy inkább lehetetlen, és ha bármiért is belehal a rendszer, nincs vagy nagyon nehéz a visszaút. Szép kihívás.

Szóval mégis migráció lesz? Az jó, mert:

- Teljesen új hardver és szoftver környezetünk lesz, gyors, szép és használható lesz minden része a rendszernek.
- Megvan a remek alkalom arra, hogy kijavíthassuk az előző rendszer építése során elkövetett alapszintű hibákat (névkonvenció, komponensek újratervezése és elosztása a szerverek közt, stb.)
- Ráérünk. Párhuzamosan megy majd a két rendszer, és ha szépen nyugodtan átpakolgattunk mindent, és a bolygók is együttállnak és áldoztunk már egy kecskét is éjfélkor, akkor átbillentjük - de marad még a régi szerver is, azaz van visszaút, mert szépen, fokozatosan fogjuk kivezetni (és akár kicsit megújítva tartalékként újra is hasznosíthatjuk).

[22] Ez egy erősen szubjektív és politikailag teljesen inkorrekt megjegyzés, amely szellemétől az Olvasó bátran eltérhet, de a szerző határozottan hisz abban, hogy érdemes és fontos az angol nyelvű változatokat használni - legalábbis a szerver oldalon.

De azért ez sem fenékig tejfel, mivel:

- A migráció lényegesen bonyolultabb, a komponensek és a tartalom (AD, DHCP, tanúsítványok, fájlszerver, megosztások, nyomtatók, stb.) átvitele során lehetnek nehéz pillanatok és/vagy rengeteg munka.
- Tesztelni mindkét esetben kell, de itt talán sokkal többet, mivel rengeteg minden változni fog.
- A kliensek ekkor mindig kérdésesek, hogyan fognak reagálni a változásra, gondoskodtunk-e mindenről, a folyamat a kliens szempontjából teljesen transzparens-e, és csak az előnyöket érzi-e majd a felhasználó?

Még lehetne ragozni, de nem teszem. Ellenben a voksomat azért leteszem: én a migráció híve vagyok, igaz hogy melósabb, és sokkal több dolgot kell tudni, illetve sokkal több tényezőt figyelembe kell venni, de ez egy tiszta, száraz érzés a végén, és ráadásul ettől csak felkészültebbek leszünk, hiszen rengeteg újdonságot tanultunk közben (meglehet azt is, hogy ilyet soha többet nem csinálunk ☺).

De nézzünk egy konkrét és viszonylag egyszerű gyakorlati példát. Rengeteg ilyennel vagy hasonlóval szembesülök különböző levelezőlistákon kérdés formájában, és persze a hétköznapokban ezt nehéz aprólékosan megválaszolni, de most fussunk neki! Lesz benne pár téma, ami ebben a könyvben később jön majd logikailag, de nem baj.

> Sziasztok![23]
> Adott egy: régi hardver, Win 2k3 3 R2 32bit, Exchange 2003 és a célgép, ami a régit leváltja: új hardver, Win 2k8 R2 64bit, Exchange 2010.
> Kérdésem, hogyan oldhatom meg legegyszerűbben, az Active Directory felhasználói, jogok, beállítások átöröklődjenek rá, hogyan állítsam be az újat, h. ne kutyuljon be a rendszerbe, hogyan tudom, azt megtenni, h. teljesen átvegye a régi szerver szerepét?

A szerző receptje szerint a sorrend illetve a teendők nagyjából, de nem feltétlenül a teljesség igényével[24] a következőek:

1. Először tervezünk, papíron, vagy Excel-ben, összegyűjtjük az eddigi és a tervezett új szerverre kerülő adatokat (IP konfiguráció, szerepkörök, partíciók, megosztások, stb.)
2. Tovább gondolkodunk: a kliensek mi mindennel vannak a szerverhez kötve, pl. van-e login szkript/csoportházirend konfig a meghajtó felcsatolásokhoz, van-e Home meghajtó és/vagy vándorló profil a user profilokban, beleírtuk-e a proxy

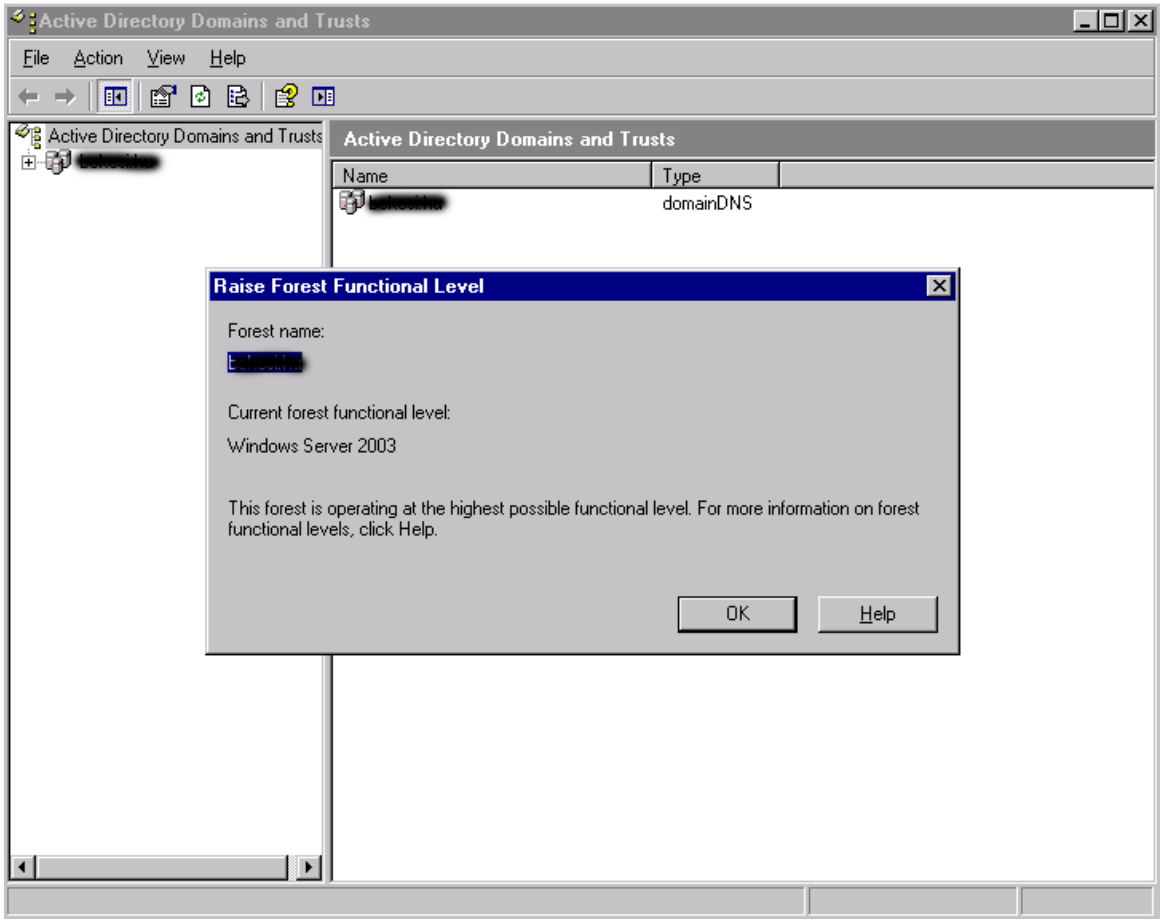
[23] A hardver eszközök jellemzőit és az IP, név adatokat kiszedtem, de mást nem, ez tényleg egy valódi, elhangzott kérdés.
[24] A teendők listája kicsit más és más lehet minden rendszerben, mert ugyebár két egyforma rendszer nincs.

címét a Csoportházirendbe, szóval mindent megtettünk, hogy ezeket egyszerűen átírva, gond nélkül menjen majd az új rendszer is?

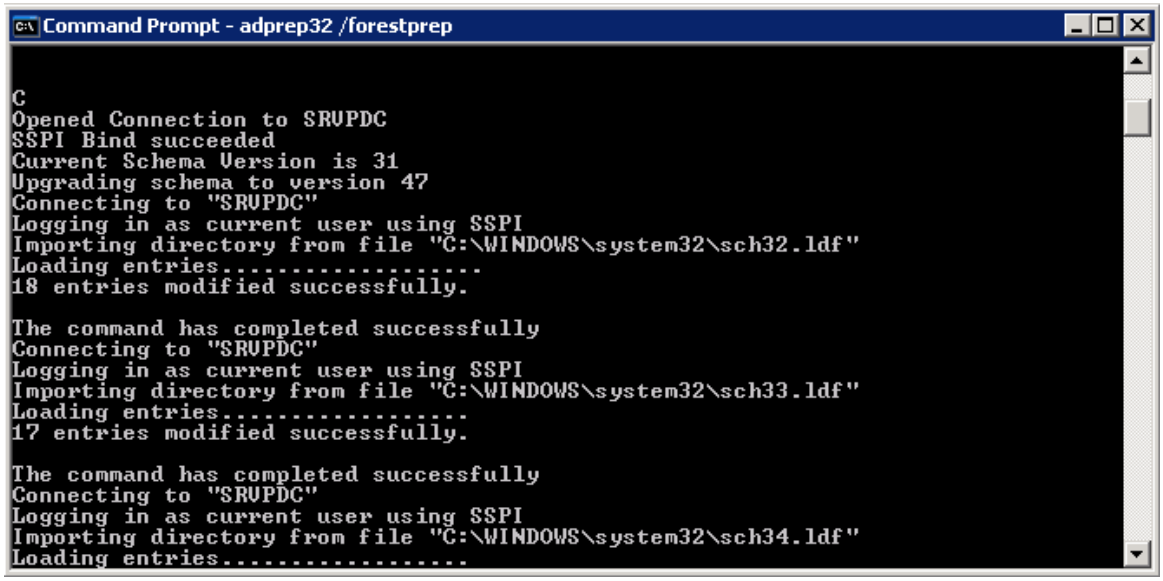
3. Biztos, hogy a legfrissebb SP-vel és javításokkal szerelt a Windows 2003-as szerver? Ha nem, korrigáljuk. Lehet, hogy időbe telik és ez egy újabb küzdelem lesz, de muszáj.
4. Az Eseménynaplót láttuk mostanában? Vannak benne új hibák és figyelmeztetések? Ha igen, először korrigáljuk ezeket, majd 1-2x indítsuk újra a kiszolgálót, és nézzük meg, hogy rendben, szabályosan működik-e minden, és az Eseménynapló is ezt tükrözi-e?
5. A régi szerver teljes és részletes mentése, mert az ördög nem alszik.
6. Ezután feltelepítjük az új hardverre az R2-t, új név, TCP/IP konfig (pl. az AD telepítés után már a DNS-nél a régi és az új gép IP címe is része a TCP/IP konfignak, de előtte még nem, és ugyanez a helyzet a WINS szervernél is), majd beléptetjük a tartományba.
7. Az AD előkészítéséhez ellenőrizzük le a tartomány és az erdő működési szintjét, és emeljük fel (ha még nincs) a „Windows 2003 natív" módba.[25]
8. Séma bővítés: mielőtt egy új Windows Server 2008 R2 tartományvezérlőt bele óhajtunk emelni a jelenleg még Windows 2003-s tartományba, AD séma bővítést kell végeznünk. Tudnunk kell azt, hogy a sémabővítés egy visszafordíthatatlan folyamat, ergo ha egyszer elvégeztük, nem térhetünk vissza egy korábbi változatra, ezért ezt tényleg óvatosan kell megtenni[26]. Viszont az adprep32 /forestprep parancsot (a mi esetünkben, mert ha lenne több domain, akkor a /domainprep jönne előbb, és egyesével) az új OS, az R2 telepítőjén kell keresni (\sources\adprep mappa), de itt is kettő van, egy 32 és egy 64 bites. Valószínű nekünk az előbbi kell majd, és persze - nyilvánvalóan az ekkor még egyetlen tartományvezérlőn - a régin.

> Igaz ami igaz, egy ideje már legalább deaktiválhatjuk az esetlegesen téves vagy hibás bejegyzéseket, de törlés az nincs. A helyzet az, hogy viszont az R2-ben már van visszaállítás is, de csak bizonyos feltételekkel illetve körülmények között, de erről tényleg csak majd később lesz szó.

[25] http://technet.microsoft.com/hu-hu/library/cc776703%28WS.10%29.aspx
[26] Óvatos meglépés: http://emaildetektiv.hu/2007/01/20/szabalyozott-megfertozes (a lektor megjegyzése)



3.13 ÁBRA EZ AZ ERDŐ FELKÉSZÜLT



3.14 ÁBRA TART A SÉMABŐVÍTÉS, R2-RŐL R2-RE (NÉZZÜK MEG A SÉMA VERZIÓKAT, 31 > 47)

9. A sikeres séma bővítés után (újraindítás nélkül) jöhet az AD telepítés, DNS és GC beállítás, TCP/IP változtatás mindkét gépen az új szerver adatainak a bevezetéséhez.

10. Ha felment és működik, akkor jöhet a spéci, és egyedi AD FSMO (Flexibile Single Master Operations) szerepek átadása[27] az új gépnek. A „netdom query fsmo" paranccsal ellenőrizhető.
11. DHCP költöztetés a netsh-val[28], egyszerű import és export, és mindent átvisz, a jelenleg kiosztott címektől kezdve a rezervációk minden adatáig. A teendő csak annyi, hogy a régi leállítása után az új szerver adatait (mint DHCP és WINS szerver) vigyük be majd az új szkópba!
12. A WINS szerver költöztetés tipikusan - egyszerűbb esetekben meg főképp - az egyik oldalon a komponens leszedését, míg a másik oldalon a telepítését jelenti, ugyanis az adatbázist majd szépen felépíti a háttérben újra a hálózati forgalom alapján, konfigurálnivaló meg szinte semmi sincs. Ellenben nagyon fontos, hogy a két szerverben már az új WINS szerver IP szerepeljen, és hogy a kliensek innentől már a DHCP-vel is ezt kapják.
13. Felhasználói adatok és környezet átvezetése, azaz a tartományi profil részleteinek (home mappa, vándorló profil, megosztások, stb.) átírása. Azért ez nem csak ennyi, előtte az új kiszolgálón ki kell alakítani ugyanazt a mappastruktúrát (a megfelelő megosztási és NTFS jogosultságokkal![29]), majd a megfelelő tartalmat át kell másolni, ráadásul úgy, hogy az eredeti jogosultságok megmaradjanak (az egyszerű Windows másolás ebben nem segít, ehhez többnyire külső eszköz kell). Itt nyilván gondolni kell arra is, hogy a másolás akkor történjen, amikor nem dolgozik senki a fájlokkal. Ha mindez kész, és rendben van, akkor jöhet a userek AD fiókjában a hivatkozások átírása, illetve a login szkriptekben a megosztások elérési útjának módosítása.
14. Az Exchange szerver költöztetése szép, nagy feladat, de jól dokumentált és nincs benne elvileg ördöngösség, főleg ha egy régi és egy új szerverről van szó.[30] A lényeg nem is a költöztetés lesz, hanem egyrészt az előkészítés, másrészt a folyamat végén az Exchange Server 2003 eltávolítása ☺
15. Ezután pár nap türelem, a kliensek és az új szerver folyamatos ellenőrzése után jöhet a régi tartományvezérlőn az AD eltávolítása, majd a kiléptetése a tartományból (van olyan eset is, amikor ez egyetlen fázis). Figyeljünk oda az eltávolításkor az admin jelszó megadására, mert még kellhet ez a gép! Ha viszont minden szépen megy ezek után is, akkor végleg törölhető az operációs

---

27 http://www.softwareonline.hu/art3066/fsmo+szerepkorok+athelyezese+masik+tartomanyvezerlore.html

28 http://blogs.technet.com/b/networking/archive/2008/06/27/steps-to-move-a-dhcp-database-from-a-windows-server-2003-or-2008-to-another-windows-server-2008-machine.aspx

29 http://blogs.technet.com/b/askds/archive/2008/06/30/automatic-creation-of-user-folders-for-home-roaming-profile-and-redirected-folders.aspx

30 http://technet.microsoft.com/en-us/library/aa998604%28EXCHG.140%29.aspx

rendszer is, és akár erre is kerülhet egy Windows Server 2008 R2, mivel „egy DC nem DC”.

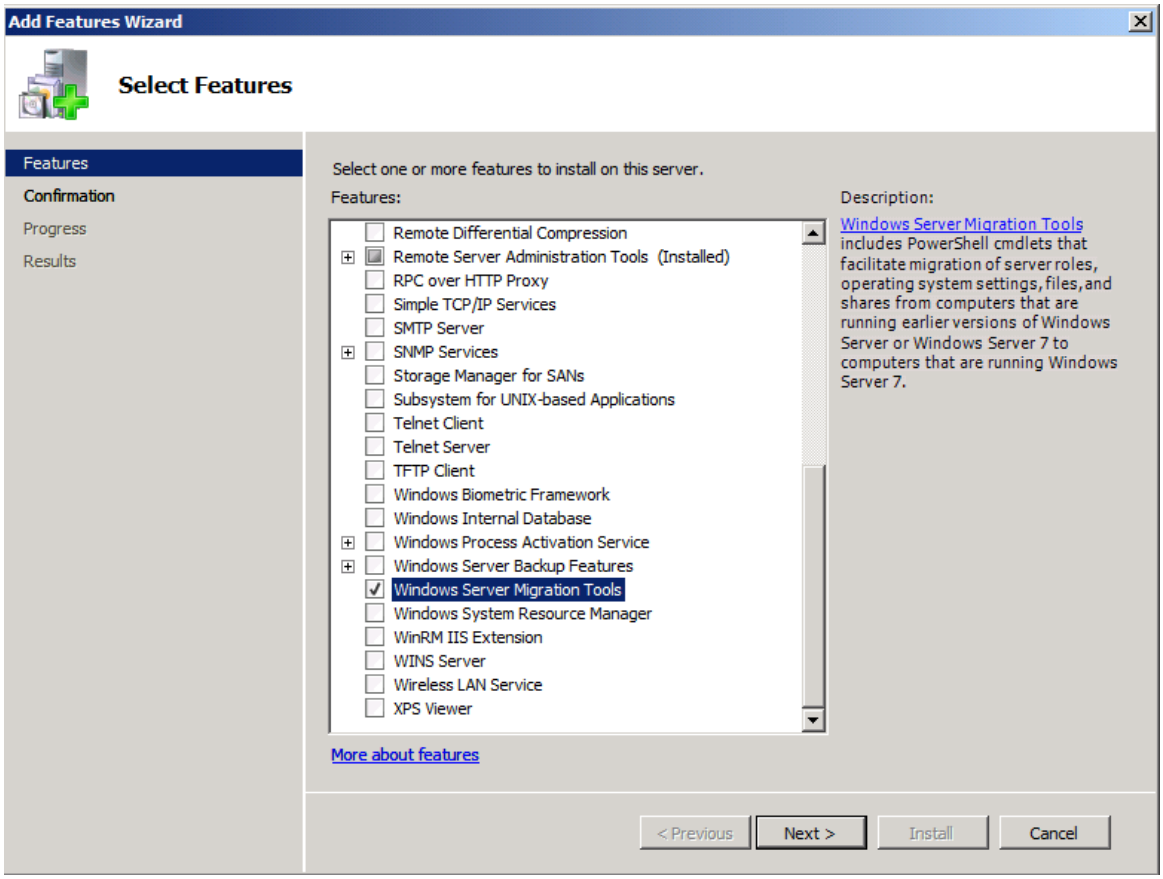
16. Ha már biztosak leszünk benne, hogy nem lesz többet Windows Server 2003-as tartományvezérlőnk (és jól eldugva a padláson sincs egy másik ☺), akkor az erdő és a tartomány működési szintjét tovább emelhetjük – hiszen csak ezután fogunk tudni bizonyos új szolgáltatásokat használni, a friss ropogós új szerverünkön és a tartományban, illetve az erdőben.

3.3.1 Egy új módszer: a Server Migraton Tool

Ahogy jeleztem korábban, szeretek migrálni. Szinte bármit. És sokszor kell. Van abban valami felemelő, amikor az új, erős és csilivili hardveren, és egy új, még szűzies erényeket felvonultató OS-en fut tovább minden, amit az elmúlt években összekalapáltál. Ráadásul az új hardverrel többnyire, új és okosabb feladat ki- és elosztás jön létre a szerverek között is (és itt gondoljunk bátran a fizikai és a virtuális gépek közötti migrációra is, oda és vissza is), azaz ilyenkor lehet korrigálni, az elmúlt évek tapasztalatai alapján kissé vagy akár gyökereiben is módosítani az infrastruktúrát. Sőt, ha már minden OK, és amikor már minden úgy működik, ahogyan eltervezted, akkor még az is lehet, hogy nem kell naponta piszkálni mint előtte, azaz jöhet a vállveregetés.

> Persze - mondhatni - nekem könnyű, hiszen maximum pár száz userig (na jó, van/volt ezres is) és általában 25 alatti szerverrel dolgozom, általában minimális számú telephellyel, és a nemzetközi kapcsolatok meg főleg az alá- és fölérendeltségi viszonyok (technikailag értem ezt) sem sűrűn hátráltatnak. A "*4 földrészen, 1200 szervered és 60.000 kliensed van*" viszonylatot csak az MCP vizsgákon tapasztaltam meg (na de ott aztán rendesen :D), az én körülményeim között nagyjából és általában maximum 1-2 fős a tervező-, kivitelező- és monitorozó/tesztelő csapat is, vagy csak jómagam.

Egy szó mint száz, viszonylag sok - ebbe a kategóriába tartozó - rendszerátalakítást végeztem már, ismerem a trükköket, van jó pár módszerem és jó pár eszközöm is. Azért kell a sok trükk és a jó módszer, mert a migráció általában bonyolult, és tegyük a szívünkre a kezünket, egyúttal kissé aluldokumentált illetve alultámogatott folyamatról van szó. Persze van ADMT, meg netsh, meg ntdsutil, meg export/import, mostanság már xml-be, de eddig ebben a könyvben is csak különálló, nem rendszerbe foglalt, nem azonos módszert követő megoldásokról volt szó. Most viszont a Windows Server 2008 R2-ben valami egészen újjal próbálkozik a Microsoft, és ez az ún. „Windows Server Migration Tool”, és a jelszava lehetne a „legyen a forrás és a cél is ugyanaz!”

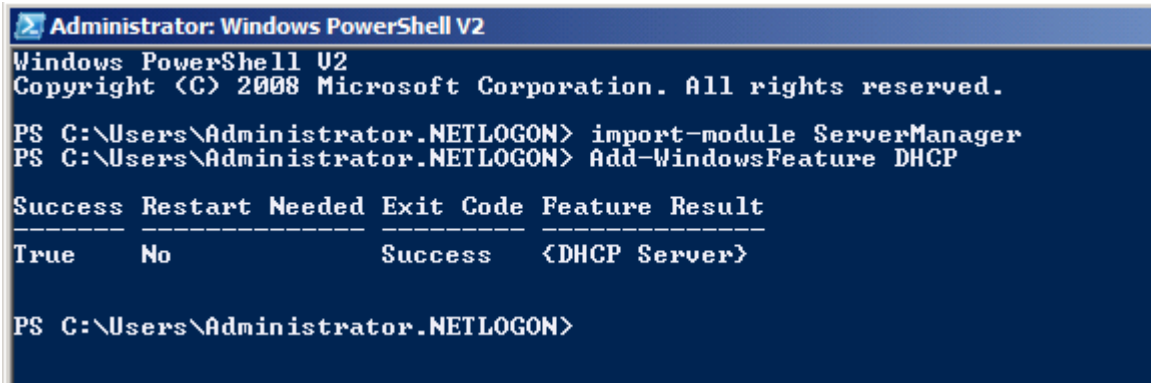


3.15 ÁBRA EGY PIPA MINDENEKFELETT - A WSMT EGY KÉPESSÉG, ELSŐ LÉPÉSKÉNT EZT KELL MAJD TELEPÍTENI

> Vagy kicsit szaladjunk előre: ha PowerShell rajongók vagyunk, akkor három lépés az eszköz telepítése: *1; Import-Module ServerManager, 2; Add-WindowsFeature Migration, 3; örül.*

Alapvetően mi kell ehhez az eszközhöz? Hát a jó öreg PowerShell-, a "régi" szerveroldalon az 1.0-ás, az R2-nél meg a 2.0-ás verzióval. Merthogy az egész migrációs eszköztár, tokkal-vonóval PS alapú. Nos, *hogyismondjam*, finoman szólva sem vagyok egy PowerShell zsonglőr, de a legelső Exchange 2007 migráció óta azért már nem kell a fokhagymafüzér, ha meglátom a PS előtagot a parancssorban, és eme migrációs kalandok közepette meg egészen megkedveltem. A legjobban a hibakezelés, illetve a beépített segítség mennyiségének mértéke az, ami feldob, persze, nyilván így kell elcsábítani a kezdőket, okos.

> Na és tényleg, tegyük a szívünkre a kezünket, mit nem lehet majd PowerShell-lel kezelni akár most vagy akár 5 év múlva? Már eddig is sok-sok mindent lehetett, de pl. az R2-ben már az AD-t is, a Csoportházirendet is (1. Import-Module grouppolicy, 2. New-GPO “Proba-GPO” és kész, és még az egeret se fogtam meg), sőt még egy kicsit az amúgy egészen konzervatív Forefront TMG is...



3.16 ÁBRA ENNYI ÉS NEM TÖBB

Visszatérve a fősodorba: az R2-es WSMT telepítés után a következő teendőnk a források felkészítése lesz. De mire is? A WSMT jelen pillanatban 7 különböző (néha azért összefüggő) konfigurációt, képességet, szerepkört támogat, konkrétan ezeket:

- TCP/IP konfig, DHCP szerver
- AD/DNS
- Fájlszerver (megosztások, VSS, VDS, FSRM is) és BranchCache
- Printszerver
- Lokális felhasználók és csoportok

És milyen szervereket támogat, azaz hogyan néz ki a verzió mátrix?

Forrás szerver CPU	Forrás szerver OS	Cél szerver OS	Cél szerver CPU
x86/x64	WS03	WS08 R2 teljes és Server Core is	x64
x86/x64	WS03 R2	WS08 R2 teljes és Server Core is	x64
x86/x64	WS08 teljes verzió	WS08 R2 teljes és Server Core is	x64
x64	WS08 R2	WS08 R2 teljes és Server Core is	x64
x64	Server Core WS08 R2	WS08 R2 teljes és Server Core is	x64

3.16 ÁBRA MÁTRIX EZ IS

És milyen kivételekkel, illetve aranyszabályokkal?

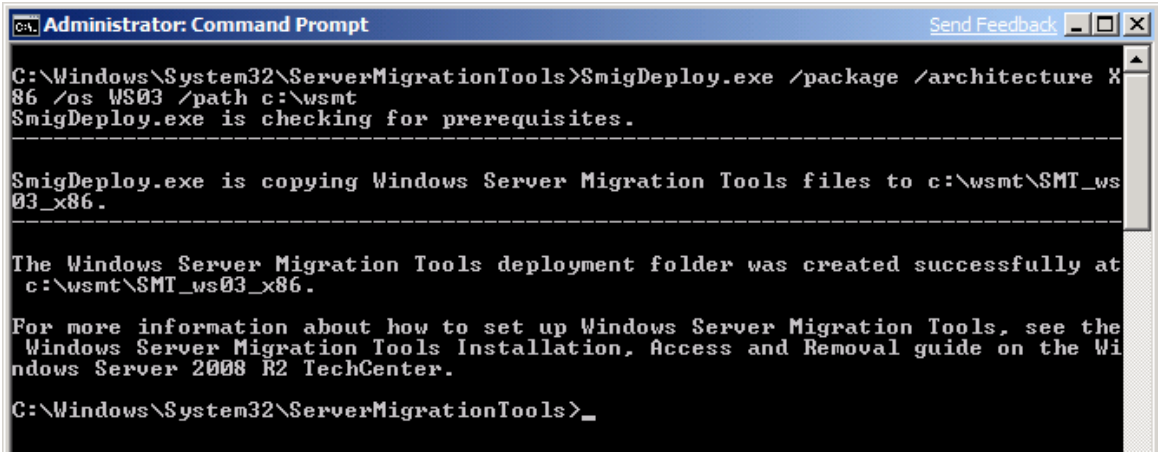
- Windows Server 2008 Server Core nem lehet forrása a Windows Server 2008 R2. Server Core-nak, ti. a .NET Framework csak az utóbbiban létezik.
- Eltérő nyelvi beállítású OS-ek között nem működik.

- Mindig legalább a (lokális) Administrators csoportban kell lennünk.
- Ahogy már elhangzott, PS1 kell a régi OS-eken, PS2 az R2-n.
- Minden szerveren kell a .NET Framework 2.0..
- Minden további nélkül variálhatunk a fizikai és a virtuális szerverek között, és persze fordítva is.

Most, hogy mindezt tudjuk (és jó rendszergazda szokás szerint szépen átsiklunk majd felette), kezdődhet az igazi munka, azaz a telepítés, majd a forrásgépek regisztrálása. Első teendőként a Windows Server 2008 R2-es szerveren csinálnunk kell egy mappát, és célszerűen egy megosztást a régi szervernek, majd indíthatjuk a parancssort, de szigorúan a "*Run As Administrator*" módszerrel.

Lépjünk be a %Windir%\System32\ServerMigrationTools mappába, és gépeljük a be a következő parancsok valamelyikét:

SmigDeploy.exe /package /architecture amd64 /os WS08 /path <az általunk legyártott deployment mappa>
SmigDeploy.exe /package /architecture amd64 /os WS03 /path <az általunk legyártott deployment mappa>
SmigDeploy.exe /package /architecture X86 /os WS08 /path <az általunk legyártott deployment mappa>
SmigDeploy.exe /package /architecture X86 /os WS03 /path <az általunk legyártott deployment mappa>



3.17 ÁBRA ÍGY KÉSZÜLT EL A WS03 SZERVER SZÁMÁRA A CSOMAG

Azt gondolom, nem kell túlmagyarázni, a készlet elemei CPU-nként és OS-enként eltérőek, így aztán csini kis nevekkel ellátott mappákat gyárt le az SmigDeploy.exe, ha jól csináljuk. Lépjünk át a forrás oldalra, és az adott szerverre másoljuk le a megfelelő mappát, majd egy szintén admin parancssorból (már ahol van ilyen), a helyi mappába belépve, adjuk ki a következő parancsot (nem elírás, valóban pont és per jel van az elején :D).

.\Smigdeploy.exe

Ezzel kész is van a telepítés, illetve a kliensek migrációs eszköztárral ellátása, most pedig jöjjön az export, azaz most már aztán nézzük a lényeget! A feladat szerint egy Windows Server 2003 DHCP szerverének összes létező adatát és beállításait akarjuk migrálni, de kombinálni akarjuk a migrációt a forrásgép komplett TCP/IP beállításainak átvitelével (tehát azonos lesz a két gép címzése, nyilván egyszerre nem fognak működni), sőt a helyi fiókok és csoportok (ergo nyilván ez nem egy DC) migrálásával is. Kicsit életszagú, kicsit nem (mivel a helyi user fiókok szinte elhanyagolhatóak egy tartományi gép esetén), de a próba kedvéért jó lesz. A Windows Server 2003-on[31] indítsuk el a Powershell-t, ha jót akarunk magunknak, akkor az Administrative Tools-ban keressük meg az új migrációs programcsoportot, és az itt lévő PS-t indítsuk, ha nem, akkor elsőként be kell töltenünk a következő paranccsal a migrációs eszköztárt:

Add-PSSnapin Microsoft.Windows.ServerManager.Migration

A teljesség kedvéért leírom azt is, hogy mely utasításra van szükség akkor, ha egy szimpla parancssorból óhajtjuk a PS-t betölteni, viszont együtt a migrációs holmikkal:

Powershell.exe –PSConsoleFile ServerMigration.psc1

No és itt álljunk csak meg egy kicsit és számoljunk. Hálókártyát. Tudniillik ha történetesen a forrásoldalon több van, akkor a céloldalon is többnek kell lennie. Merthogy elképzelhető, hogy azért van több, mert a jó öreg DHCP szerverünk több kártyához is "hozzá volt kötve" (Bindings), azaz több alhálózat számára is tolta az TCP/IP konfigokat. De most már nézzük a konkrét export parancsot:

Export-SmigServerSetting –featureID DHCP –User All –Group –IPConfig –path <storepath> –Verbose

Úgy gondolom, hogy némi magyarázat szükséges, nézzük tagonként.

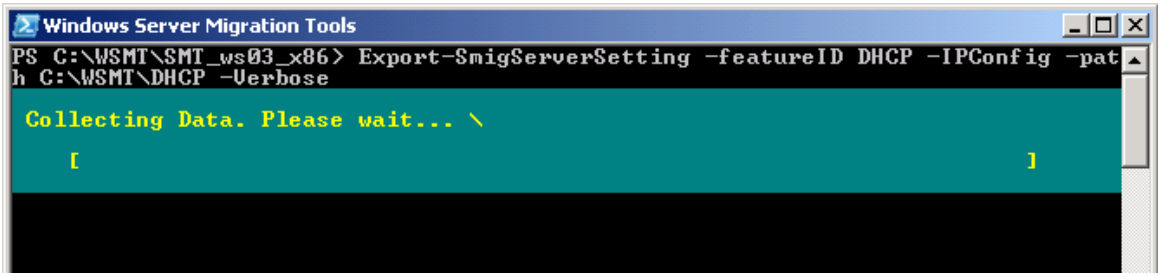
1. Export-SmigServerSetting: ez maga a cmdlet, a get-help-pel kombinálva borzasztó részletes példákat is kapunk a szintaxisra.
2. -featureID DHCP: itt adjuk meg, hogy melyik legyen a hat típus közül, ha nem vagyunk tisztában az elnevezésekkel, akkor használjuk a Get-SmigServerFeature parancsot a részletek kiderítésére.

[31] E felett is ugyanez, csak akkor van eltérés, ha Windows Server 2008 R2-ről Windows Server 2008 R2-re migrálunk, de úgy gondolom, hogy ez nem ennek a könyvnek a témája

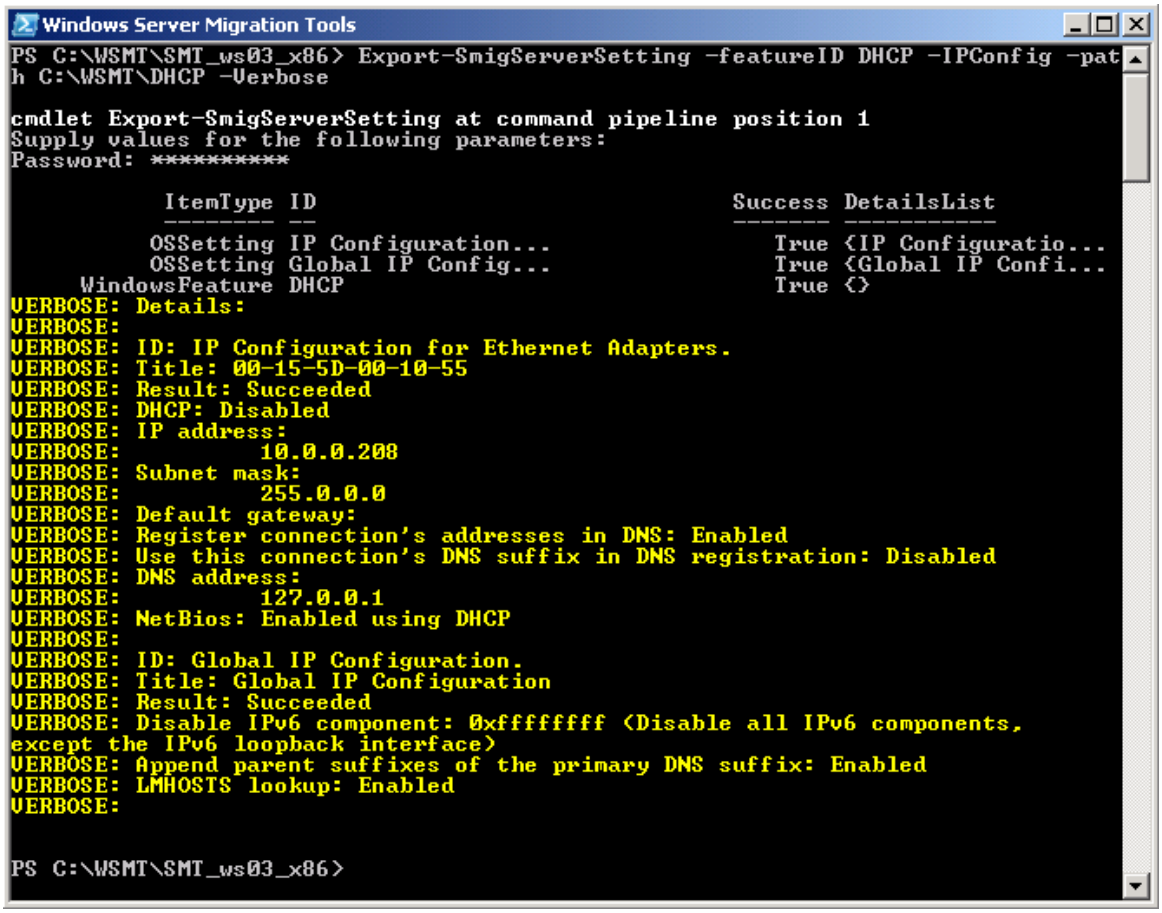
3. -Users All; -Group: ahogy mondtam, nem muszáj, de mondjuk akkor igen, ha pl. valamelyik lokális user a DHCP Administrators csoport tagja.
4. -IPConfig: ez az amitől a teljes TCP/IP konfig átcsúszik majd ha ez a szándékunk (de nem lesz muszáj mindent beimportálni, lásd később).
5. -path: lehet egy üres, vagy nem üres mappa is, a lényeg, hogy külön mappába kerüljön, és a másik lényeges dolog, hogy CSAK a mappanevet kell szerepeltetni a parancsban.
6. -Verbose: részletes infókat kapunk a művelet eredményéről, szép sárga színnel

+ Infó: menet közben kérni fog egy jelszót is, amely minimum 6, maximum 256 karakter lehet.

Ha minden jól megy, az eredmény részleteit megkapjuk egyrészt a képernyőre (ezért jó a -Verbose), másrészt célmappánkba egy pár tíz kbyte-os srvmig.mig fájl formájában. Félig hátradőlhetünk, és közben lőjük le a forrásszervert (ugye az IP és DHCP konfliktus miatt).



3.18 MÁR GYŰJT...



3.19 ...ÉS MÁR KÉSZ IS.

Ezek után viszont nyargaljunk át a cél oldalra, azaz a Windows Server 2008 R2-höz! Ha még az import előtt elgondolkozunk azon, hogy vajon be kell-e léptetni a tartományba, akkor ne gondolkodjunk tovább, nem muszáj, sőt gyakorlatilag nem oszt és nem szoroz, később is beléptethetjük. A TCP/IP beállítása sem érdekes, úgyis felülírjuk. Viszont az imént készített srvmig.mig fájlt egy fájlmásolással el kell majd juttatnunk az új gépre, ezzel számoljunk. Nos igen, még egy dolog: feltehetjük előre a DHCP szervert is, például a Server Managerből.

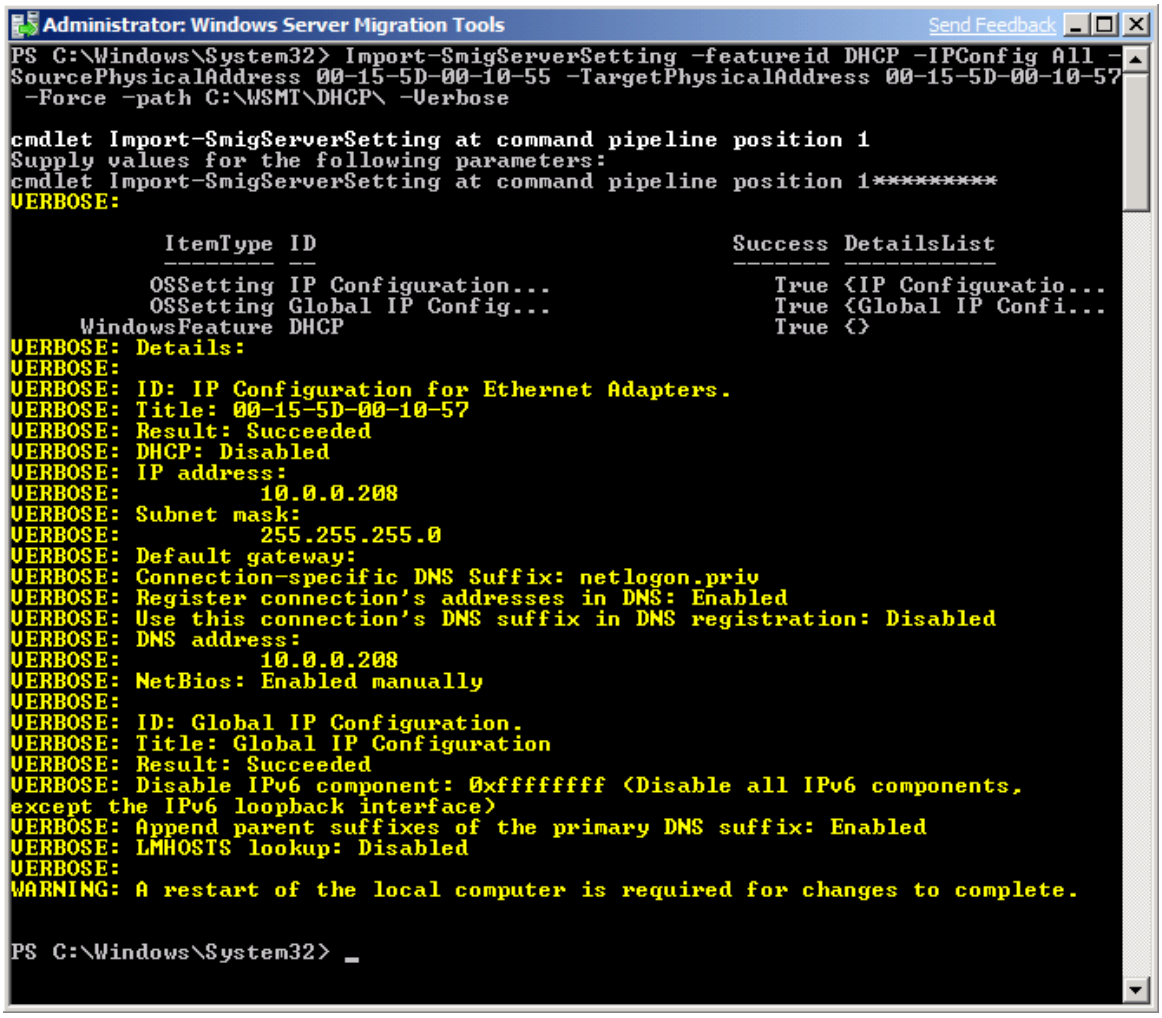
> De mondok jobbat: PS> Add-Windowsfeature DHCP. Ilyenkor nem kérdez semmit (ellentétben a Server Managerrel), ami azért is jó, mert úgysincs mit beállítani, hiszen minden szükséges adatot importálunk. De mondok még jobbat: az „Import-SmigServerSetting" cmdlet a featureID DHCP paraméter apropóján érzékeli, hogy nincs DHCP Server és felrakja. Persze ez egy újraindítással jár, meg azzal, hogy újra be kell ütni a parancsot, de azért cool, nem? :)

Ha viszont már felraktuk, akkor állítsuk le, ha esetleg elindult a szerviz (ha a PS-ből tesszük fel, nem fog). Nos, nézzük meg a parancsot:

Import-SmigServerSetting -featureid DHCP –User All –Group –IPConfig <All | Global | NIC> –SourcePhysicalAddress <SourcePhysicalAddress-1>,<SourcePhysicalAddress-2> –TargetPhysicalAddress <DestinationPhysicalAddress-1>,<DestinationPhysicalAddress-2> –Force -path <storepath> –Verbose

1) Import-SmigServerSetting; featureid: ua. mint az előbb, és a help is
2) -User All; Group: ua., de gondolkozzunk, ha csak domain tag usereink vannak a helyi csoportokban, pl. az említett DHCP Admin csoportban, akkor elég a -Group is
3) -IPConfig, na itt kezd el bonyolódni, mert ahogy említettem, szabályozhatjuk a TCP/IP konfig "ráhúzás" mértékét, ugyanis három kapcsoló is van:
   a) NIC: csak némi NIC specifikus infó (a kapcsolat-specifikus suffix, IPv4 beállítások), de ekkor kell még két paraméter illetve némi adat is, konkrétan a "-SourcePhysicalAddress" és a "-TargetPhysicalAddress"**, amelyek mögé a forrás és cél hálókártyák MAC címeit adjuk meg - lehet többet is, vesszővel elválasztva
   b) Global: a globális TCP/IP paraméterek
   c) All: az előző kettő együtt, de ilyenkor is kellenek a forrás, illetve cél MAC címek
4) -force: agresszív kismalac üzemmód, akárhogy is, de csinálja meg, ha ez nincs, akkor egy menet közbeni elakadás esetén marad a régi érték
5) -path: ahol az srvmig.mig fájl van, nyilván legyen jogosultságunk, és itt is CSAK a mappanév kell (ez nekem egy kb. 24 órás gondolkodásba illetve külső segítség igénylésébe került, de ez volt az a szakasz, amikor legalább belekóstoltam a PowerShell alapokba ☺)
6) -Verbose: ua.

+infó: csak szeretném jelezni, hogy van még jó pár paraméter mind az export, mind az import tekintetében, mint pl. a -whatif, a -confirm, -passsword, stb..



3.20 ÁBRA A MAGYARÁZAT LENTEBB

Némi kép specifikus infó:

- A felhasználókat nem migráltam (az azonos nevűeket, azaz a gyáriakat amúgy sem pakolja át).
- A "path" végére mindig kell a per jel.
- Az IPv6-ot letiltotta, mivel a WS03-on nem volt.
- Illetve még az is kiolvasható az utolsó sorból, hogy az újraindítás kötelező.

Ha minden OK (elsőre úgy sem lesz az[32]), akkor ez kiderül a sárga színű szövegből, ezek után mehet a PS-ből a "*Set-Service DHCPserver –startupType automatic*" plusz a "*Start-Service DHCPServer*", és tekintsük meg a TCP/IP konfigot, meg a DHCP szervert, nahát, működik.

> Amit még jóleső dolog átgondolni, az az hogy igazából nem bántottuk meg a forrásszervert mélyen, úgyhogy ha valami balul sült el, és ez kiderül már rögtön az utólagos teszteléskor, akkor az instant rollback nem okozhat gondot

[32] Nem nézek senkit sem bénának, csak éppen figyeljük meg pl. a Hyper-V „Type clipboard text” parancsának működését, előszeretettel hagyja le a kötőjeleket és egyéb extra karaktereket, amit persze csak később szúr ki az ember fia.

- ellentétben pl. egy helyben frissítéssel, ami... ...de ezt nem ragozom tovább, mert ebbe belegondolni is fájdalmas.[33]

Nos, közben azért füllentettem egyet, amikor azt mondtam, hogy *"...az imént készített srvmig.mig fájlt egy fájlmásolással el kell majd juttatnunk az új gépre..."*, mert ez mégsem kizárólagosan a fájl másolását jelenti. Ugyanis ez a csodakészlet rendelkezik egy "*Send-SmigServerData*" paranccsal is, amely kimenete a TCP 7000-es port. És nyilván van egy "*Receive-SmigServerData*" is, amely bemenete ugyanitt figyel. Azonos alhálón és egyidejűleg indítva a forrás és a céloldalon is a megfelelőt, nem lesz szükség a régimódi másolásra. Alapértelmezés szerint 5 percig figyel, de még ezt is módosíthatjuk a registryben, sőt alapértelmezés szerint titkosított is, a jelszóval titkosítja a forgalmat. Nincs több kérdésem...

A WSMT naplófájlja a %windir%\Logs\SmigDeploy.log, de egy további naplófájlt ugyanitt találhatunk ServerMigration.log néven is. De cifrázzuk kicsit, ha a forrás egy Windows Server 2008 vagy Windows Server R2, akkor a %localappdata%\SvrMig\Log mappa lesz a számunkra kedves, ha viszont egy WS03, akkor a %userprofile%\Local Settings\Application Data\SvrMig\Log tölti be ugyanezt a szerepet. Ha viszont valamilyen rejtélyes okból nem ezeken a lelőhelyeken lesz szerencsénk, akkor a ServerMigration.log és a SmigDeploy.log a %temp% mappába kerül. Senki ne kérdezze meg, hogy mi a kiváltó ok, tudjuk és kész. Szerintem ezen a területen még kicsit koncentrálnia kell a fejlesztőknek.

Nos, végül a konklúzió jön. Ugyan ez a szösszenet még csak a TCP/IP és a DHCP migrálást részletezte (és ezeket sem mindenre kiterjedően, hiszen sem a TCP/IP-s rész mélységéiről, sem pl. Server Core-os implementációról nem esett szó), a dolog az életben SOKKAL egyszerűbb, mint leírva. Főleg az első procedúra után. Főleg az első 30 önerőből elkövetett hiba és ezek korrekciója után, amikor már érted is, hogy mit, miért és milyen sorrendben. Nagyjából ezért is írtam le mindezt. Uff.

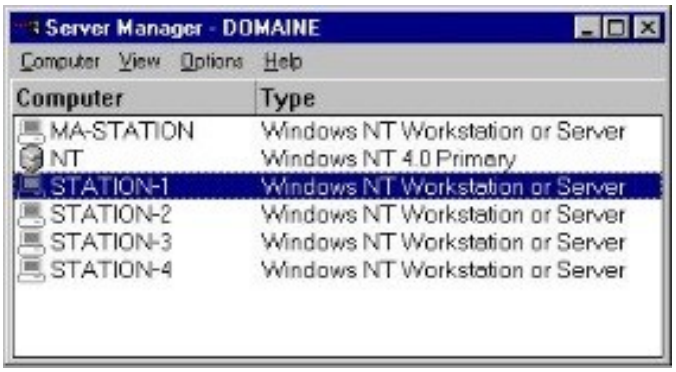
További számos eszköz és leírás a migrációs témakörben.
http://www.microsoft.com/migration

[33] Időre nem érzékeny szolgáltatások esetén, virtuális gépnél nagyobb jelentősége lehet a frissítési opciónak, mivel ekkor használható a pillanatfelvétel (snapshot) technológia (a lektor megjegyzése).

4 FELÜGYELET, KEZELÉS, ELLENŐRZÉS

4.1 A SERVER MANAGER

Mivel mással is kezdhetnénk ezt a fejezetet, mint a rendszergazdák számára abszolúte mindennapos használatú Server Manager-rel, ami gyakorlatilag tényleg egy svájci bicska, és valóban minden hétköznapi feladatunkhoz szervesen hozzátartozik. De nem volt ez mindig így, nézzünk meg egy képet egy igen korai Server Manager-ből, mégpedig egy Windows NT 4.0-ás példányból.



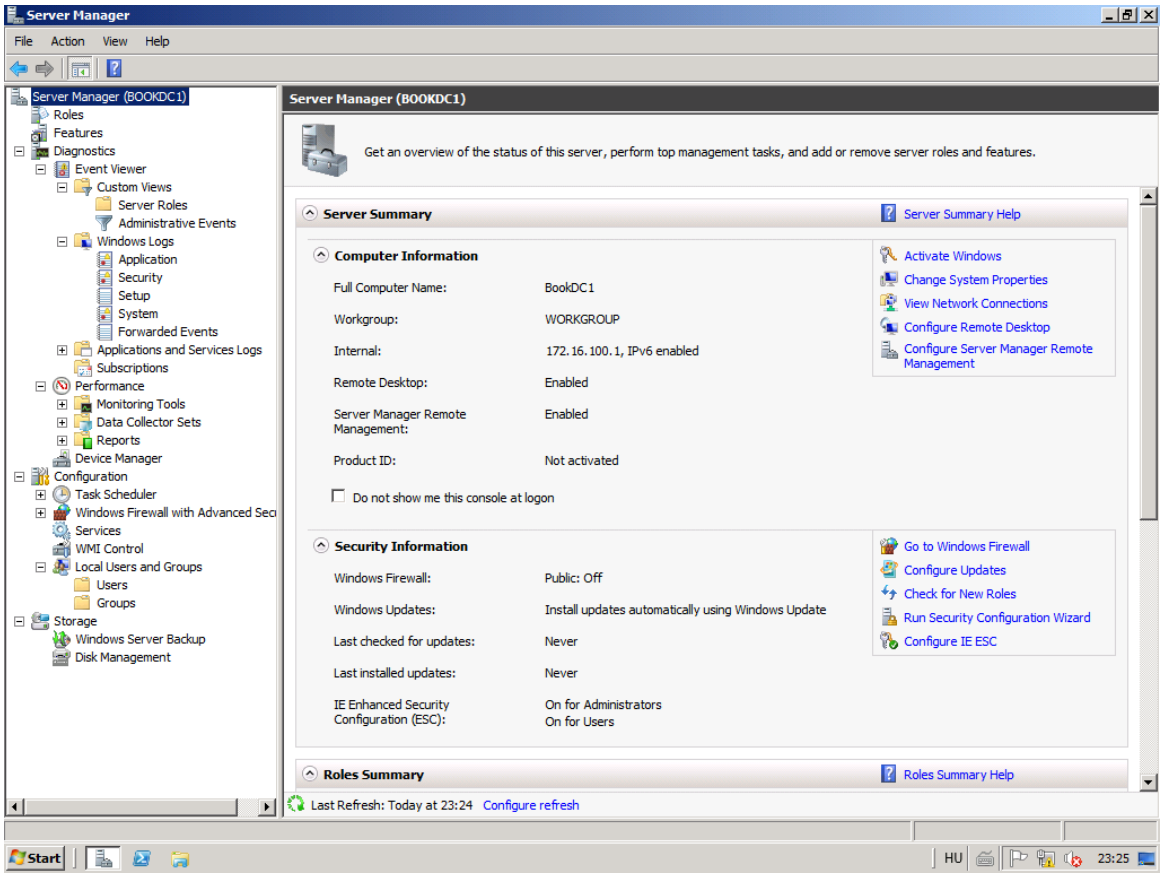
4.1 ÁBRA EGYKOR ILYEN VOLT

Majd ezután, a Windows 2000 Server-től kezdve érkeztek a különböző felügyeleti eszközök és varázslók, úgymint a *„Manage Your Server”*, a *„Configure Your Server”*, illetve az *„Add or Remove Windows Components”* és persze a *„Computer Management”* MMC. Őszintén szólva, hmmm... mindig is kissé szkeptikus voltam ezekkel a "...Your Server" varázslókkal, szerintem nagyjából csak kozmetika volt, és nem több. Ennek megfelelően az "*Igazi rendszergazda ilyet nem használ!*" - felkiáltással általában a bal alsó sarokban lévő (a végleges bezárását kiváltó) négyzetre kattintottam egy-egy új szerver telepítése után. Az „Add or Remove Windows Components” pedig igencsak gyengélkedett akkor, ha komplex módon szerettük volna használni, azaz nekünk kellett mindig, minden esetben kitalálni, hogy mi mindent kell még feltelepíteni egy szolgáltatás használatához, nem beszélve a „leszedésről”, amikor aztán tényleg csak a saját intelligenciánkban bízhattunk, ergo biztonsági és teljesítményproblémák sorozatát is hozhatta egy gondatlan, csak félig-meddig elvégzett eltávolítás.

De ez a helyzet - szerencsére - drasztikusan megváltozott a Server Manager-rel, ami a Windows Server 2008-ban debütált, és tényleg teljes szemléletváltozást hozott. Pár szóban arról, hogy elsősorban, akár rögtön a telepítés után mi mindenre alkalmas:

1) Az aktuális szerver szerepkörök (roles) megtekintése illetve telepítése/eltávolítása
2) Az aktuális szerver képességek (features) megtekintése illetve telepítése/eltávolítása

3) Szerverállapot felmérés (már a kezdőlapon is), kritikus hibák beazonosítása, eseménynapló, device manager, diagnosztika, és persze a "troubleshooting" szakasz
4) Mindennapos üzemeltetési feladatok (szervizek, helyi tűzfal, lokális felhasználók, stb. kezelése)
5) A Disk Management MMC + a Windows Server Backup elérése



4.2 ÁBRA JÓ SOK MINDEN, EGY HELYEN

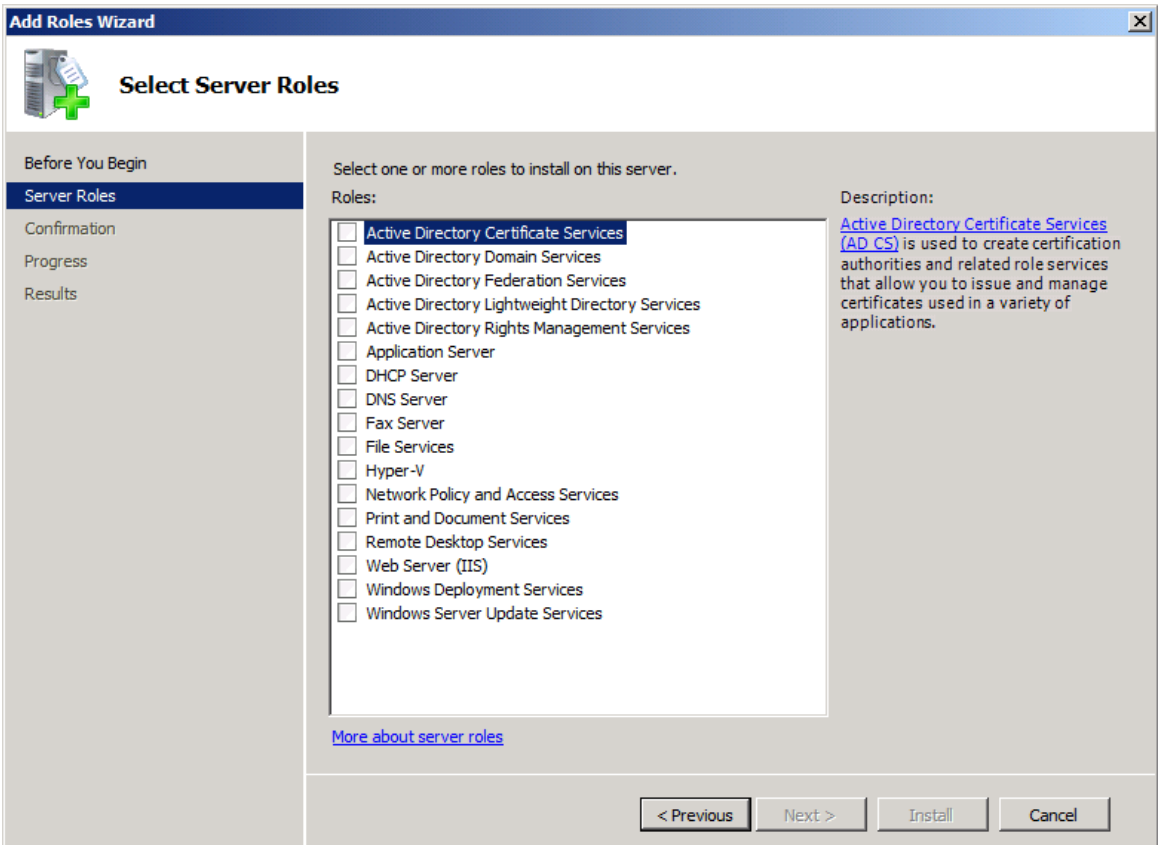
Az előző listából igazából az 1. és 2. pont az, ami rögtön és mellbevágóan újdonság lesz egy Windows 2003-as rendszergazdának, úgyhogy kezdjük a szerepkörökkel és a képességekkel! A szerepkör (Role) tehát egy olyan jól definiált feladat együttes, amit a szerverünk elláthat a rendszerünkben. De ennél lényegesen élvezetesebb egy mélyen tisztelt kollégám, *Petrényi József* definíciója:

> A server role az tulajdonképpen egy alap szerverfunkció. Egy építőkocka. Például role a File Server funkció, a Print szolgáltatás vagy a Terminal Service (Távoli hozzáférés). Ezeket a szerepköröket lehet aztán felcicomázni matyó szalagokkal, csíkos napernyőkkel... szerepkör szolgáltatásokkal. Nézzünk is rögtön néhány példát: a File Server szerepet felturbózó szerepkör szolgáltatás lehet mondjuk a Distributed File System szolgáltatás vagy a File Service Resource Manager, vagy a Single Instance Service. Az első az elosztott fájltárolás képességével javítja a File Server szerepkört, a második kvótát,

monitorozási lehetőséget és menedzsment felületet biztosít, a harmadik pedig egy helyspórolós tárolási forma.
Kicsit olyan ez, mint a régi népi gyógyszer, a vasalma. Ahhoz, hogy kellő vastartalma legyen, beleszúrtunk egy rozsdás szöget. Aztán beleszúrtunk még néhányat. Ha elfogytak a szögek, szúrhattunk bele ácskapcsot is. A végén már úgy nézett ki az alma, mint egy sündisznó: de ekkor már elég magas lett a vastartalma, a szögek kihúzkodása után el lehetett fogyasztani. (Ma persze már vastablettát eszünk helyette.)

http://technetklub.hu/blogs/winserver2008r2/archive/2010/08/12/Windows Server 2008-10-sz-237-nh-225-z-az-eg-233-sz-vil-225-g.aspx

Valamennyi szerepkör-szolgáltatás tételes felsorolása nagyon hosszú volna, de azt azért érdemes (képes formában) áttekintenünk, hogy milyen szerepkörök állnak rendelkezésünkre, immár az R2-ben, ismerős lesz azért bőven.

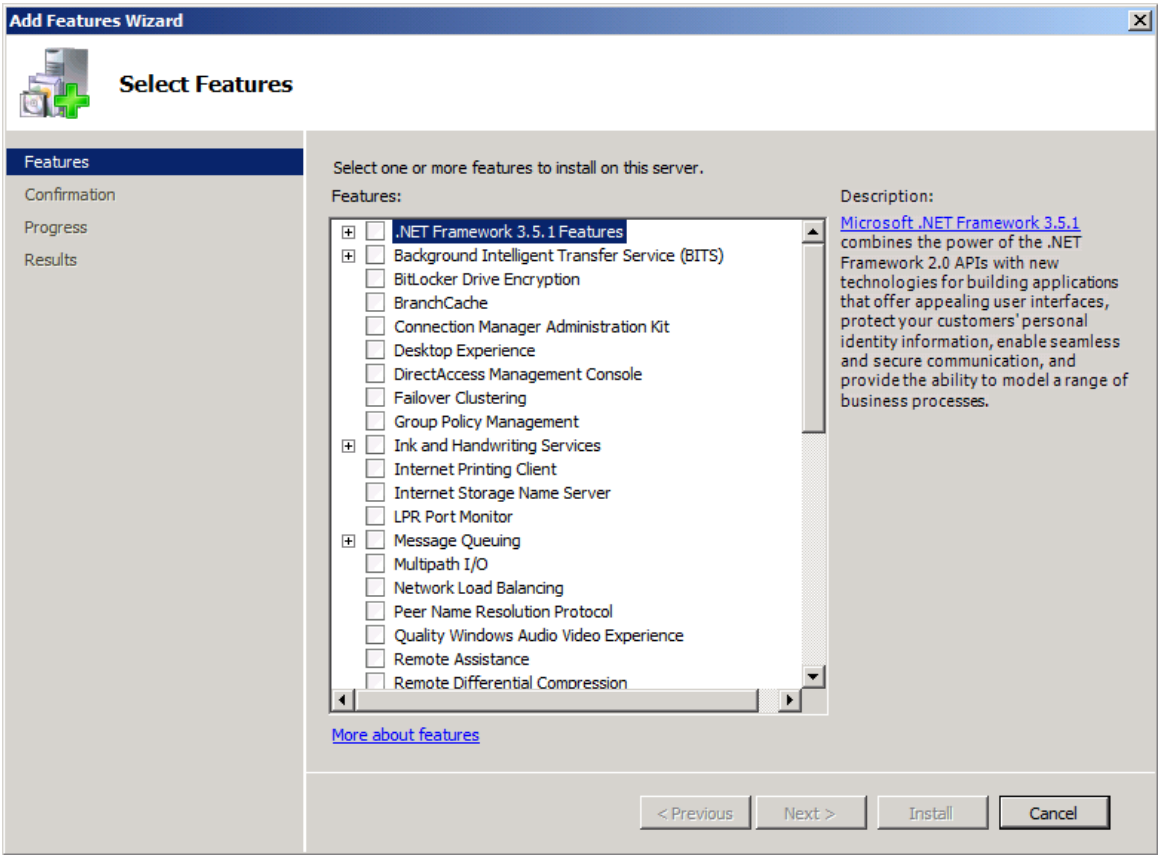


4.3 ÁBRA TIZENHÉT DARAB

Van persze egy másik halmazunk is (és ez a nagyobb számú, bár a „role service”-ekkel együtt nyilván nem), ez pedig a képességeké. Ezek olyan rendszerkomponensek, amelyek önmagukban általában nem meghatározó módon

befolyásolják a szerverünknek a rendszerben betöltött szerepét, tevékenységét. Újabb idézet jön, ugyanattól a szerzőtől:

> Végül nézzük, mit értünk feature alatt? Hát az extra mutatványokat. Ezek olyan szolgáltatások, esetleg szolgáltatáscsoportok, melyek extra funkcionalitást biztosítanak a szerverünknek. Ilyen lehet például a Bitlocker partíciótitkosítás, a .NET3.0 keretrendszer, a Netbios telefonkönyv, azaz WINS névfeloldó szolgáltatás, vagy a Failover Cluster, mely különböző erőforrások magas rendelkezésre állását biztosítja.
> http://technetklub.hu/blogs/winserver2008r2/archive/2010/08/12/Windows Server 2008-10-sz-237-nh-225-z-az-eg-233-sz-vil-225-g.aspx



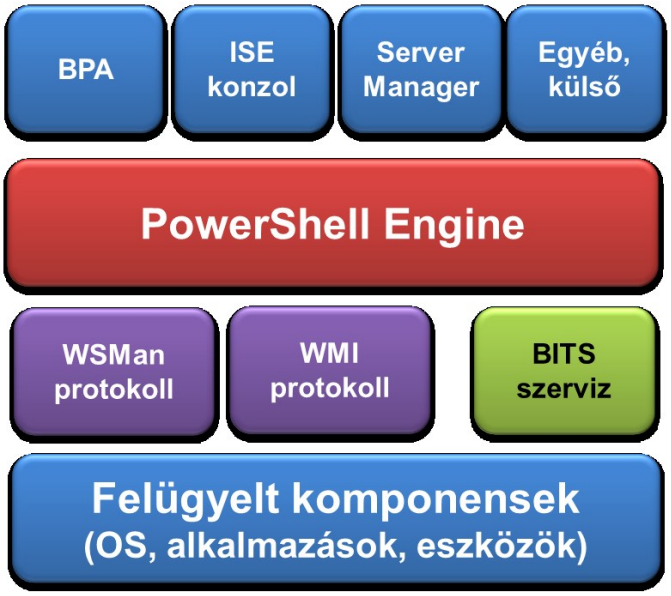
4.4 ÁBRA 42 VAN, DE CSAK A FELE FÉRT IDE

És akkor foglaljuk össze, egy kicsit ismét más tollával ékeskedve:

> Még egyszer: mi is az a role? Alapszolgáltatás. Mi a role service? Kiegészítő szolgáltatás. És a feature? Extra szolgáltatás.
> Szolgáltatás szolgáltatás hátán. De nem ez volt a kiindulási alapunk is: szolgáltatások összelapátolva?
> A különbség a rendezettség. A funkcionális csoportosítások. A fenti kategóriák ugyanis nem csak a fejünkben léteznek, hanem valóságosan is: a Windows

Server 2008-ban nem szolgáltatásokat telepítünk a jó öreg Add/Remove Windows Component módszerrel, hanem szerepeket, szerepkör szolgáltatásokat, kunsztokat teszünk fel a Server Manager-ből vagy a parancssorból. Az absztrakció egy magasabb szintjén gondolkozunk a szolgáltatásainkról.
A vége felé nézzünk bele egy kicsit a motortérbe. Vajon mennyire lettek szétszedve a régi, ismerős szolgáltatások... és mi alapján lett eldöntve, hogy meddig szeletelnek? (Szereposztó dívány, hehe.) A válasz: CBS, azaz Component Based Services. Ez egy új architektúra, mely a Vistában jelent meg - és természetesen a Windows Server 2008-ban. Egészen a binárisokig leásva térképezték fel az egyes szolgáltatások alkotóelemeit, a köztük lévő függőségeket - és ezekből alakították ki azokat a lego kockákat - komponenseket - melyek meghatározták, hogy mi lesz role, mi lesz role service és mi lesz feature - illetve mik lesznek már ezen a magasabb szinten a szolgáltatási függőségek.

De azért még mindig nem hagyom abba ezt a részt, ugyanis továbblépünk az általánosságtól az R2 felügyeleti keretrendszerét alkotó elemek konkrét megvalósítási formájáig.



4.5 ÁBRA A SZÍNES-SZAGOS FELÜGYELETI KERETRENDSZER

Látható, hogy a Server Manager igazából csak egy, a tetőn lévő komponens, a háttérben és a mélyben számos egyéb alkotóelem működik azért, hogy tényleg multifunkciós jellegű legyen a rendszergazdák kelléktára. Így aztán a következő részekben kicsit megnézzük a felépítmény részeit, meg persze a többi szerszámot is – de csak néhány kiemelkedőt.

4.2 A POWERSHELL 2.0 ÁLDÁSAI

> "Ha egyetlen mondatban kellene megfogalmaznunk, hogy mi is a PowerShell - amiről ez a könyv szól -, akkor azt mondhatnánk, hogy a PowerShell egy teljesen objektumorientált, a .NET keretrendszerre épülő parancsfeldolgozó- és szkript környezet, ami gyökeresen új alapokra helyezi (és fogja helyezni) a Windows operációs rendszerekkel és kiszolgáló-oldali alkalmazásokkal kapcsolatos felügyeleti feladataink elvégzését. [...]
>
> Ha egy műveletsort egyetlen gépen csak egyetlen egyszer kell végrehajtanunk, akkor a grafikus felület a logikus választás, ebben az esetben a parancssor használata, vagy a megfelelő szkript megírása csupán időigényes (bár szórakoztató) hobbinak tekinthető. Egészen más a helyzet azonban, ha az adott műveleteket minden nap el kellene végeznünk (vagy esetleg 300 gépen kell minden nap elvégeznünk). [...]
>
> Aki látja a jövőt, az tudhatja, hogy a PowerShell mindent visz. Előbb-utóbb mindenkinek ugyanúgy meg kell tanulnia, mint annak idején a DOS-t - egyszerűen nincs nélküle élet a Windows-világban."

A bevezető rész *Soós Tibor* MVP kollégám első Powershell (PS) könyvének [34] beharangozójából származik, és nehéz vele vitatkozni. A PS (kódnevén Monad) sok-sok év fejlesztés után eleinte még csak az Exchange 2007 kiszolgálóban köszönt vissza, azóta viszont feltartózhatatlanul halad, és mára gyakorlatilag szinte az összes kiszolgáló szoftver mellett, az operációs rendszereknél is teljes mértékben jelen van. Az utóbbiak esetén a totális debütálás az R2-vel következett el (PowerShell 2.0), amikor is az újabb modulok a felügyeleti eszközök, a Server Manager és pl. a címtárszolgáltatások területén is teret nyert (jó példa erre a 2.4 ábra), méghozzá többnyire teljes eszköztárral.

Nézzünk egy egyszerű gyakorlati példát, a Server Managerhez kapcsolódva, és feltételezve, hogy már elindítottuk a PS-t:

Az összes képesség listázása, x-szel jelölve, hogy valójában mi is van fent a rendszeren:

```
import-module servermanager
Get-WindowsFeature
```

Csak azon képességek listázása, amelyek fent vannak a rendszeren:

[34] Erről a hivatkozásról minden anyag letölthető, többek között az azóta megjelent 2.0-ás könyv is: http://technetklub.hu/TechCenters/TechCenterPage.aspx?id=18

Get-WindowsFeature|where {$_.Installed -eq "true"} |fl

Kérdezzük meg, hogy a .Net-framework fent van-e?

Get-WindowsFeature net-framework

Ha nincs, rakjuk fel:

Add-WindowsFeature net-framework

No és van más is, PS2-ben immár van távvezérlés is, azaz a „Remoting”, amivel szenzációs dolgokat is művelhetünk, kétfajta modell szerint is:

- Egy gépről soknak: parancsok, szkriptek küldése egy gépről több gép felé, akár a háttérben is (a kapcsolatok limitálása lehetséges)
- Sok gépről egynek: „Hosting” modell, pl. egy kiszolgáló vs. több üzemeltető, akár eltérő jogosultság szerint is

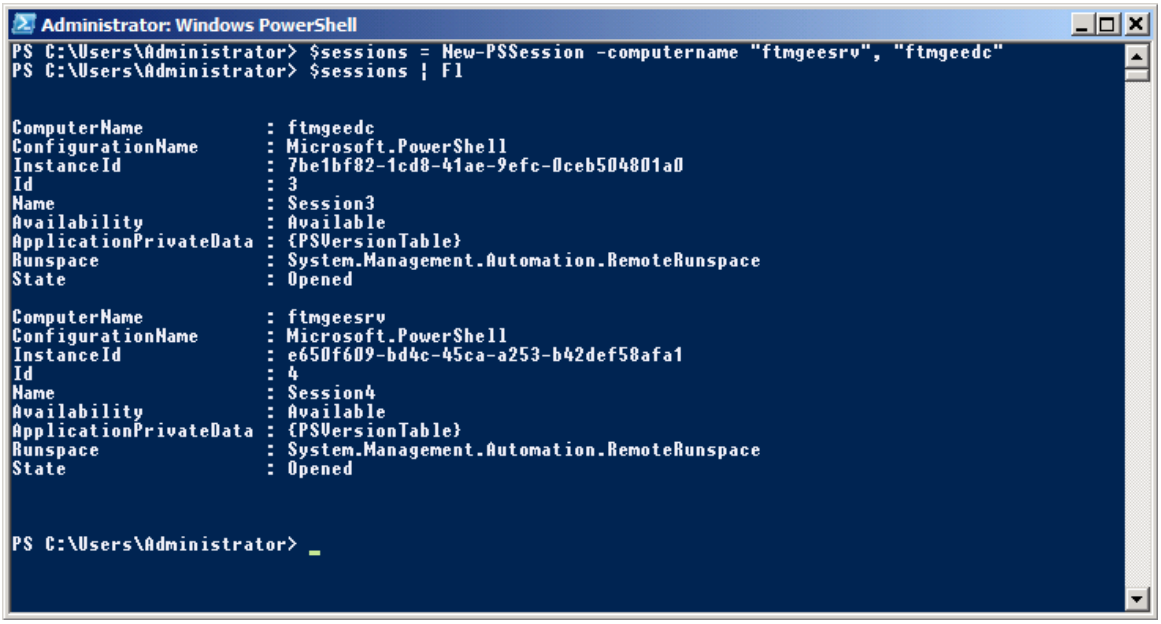
Nos, akkor nézzünk néhány egyszerű példát:

A távoli R2 gépről kérdezzük le a processzeket:

Invoke-Command –Computername srv1 –Command {get-process}

Két session kialakítása, majd jellemzőik listázása:

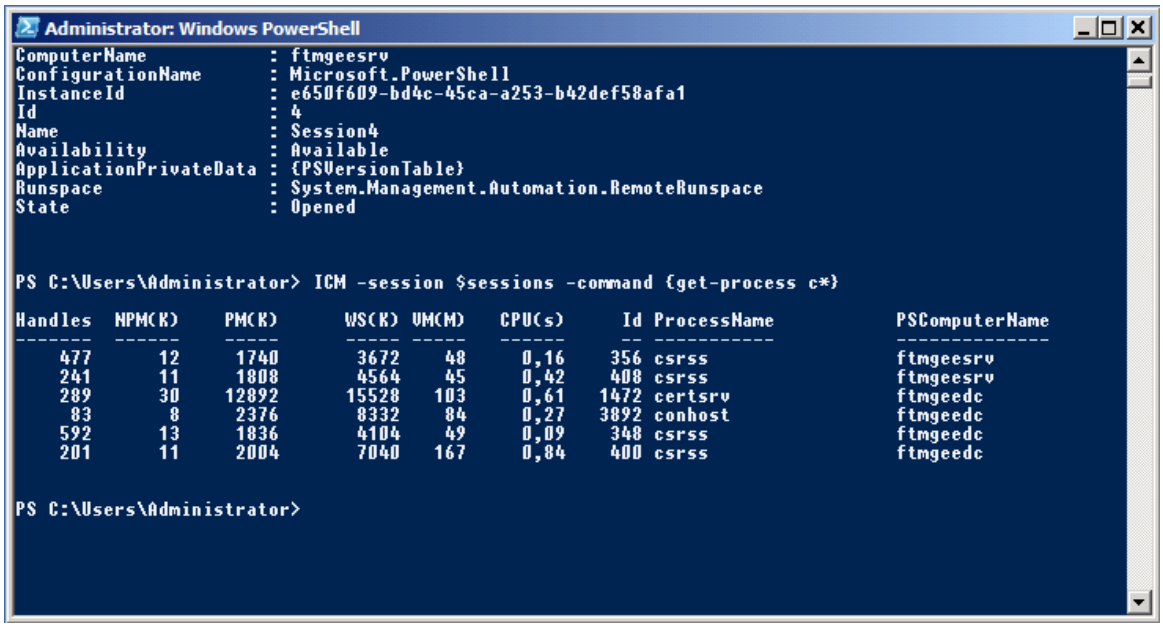
$sessions = New-PSSession -computername “srv1”, “srv2”
$sessions | Fl



4.6 ÁBRA EGY GÉPRŐL, KETTŐRE

De ne álljunk meg itt, kérdezzük le a „c” betűvel kezdődő processzeket a két gépről!

ICM -session $sessions -command {get-process c}*



4.7 ÁBRA 6 PROCESSZ, 2 AZ EGYIK, 4 A MÁSIK GÉPRŐL

És végül telepítsük fel párhuzamosan a Windows Backup-ot mindkét gépre, majd nézzük meg, hogy sikerült-e!

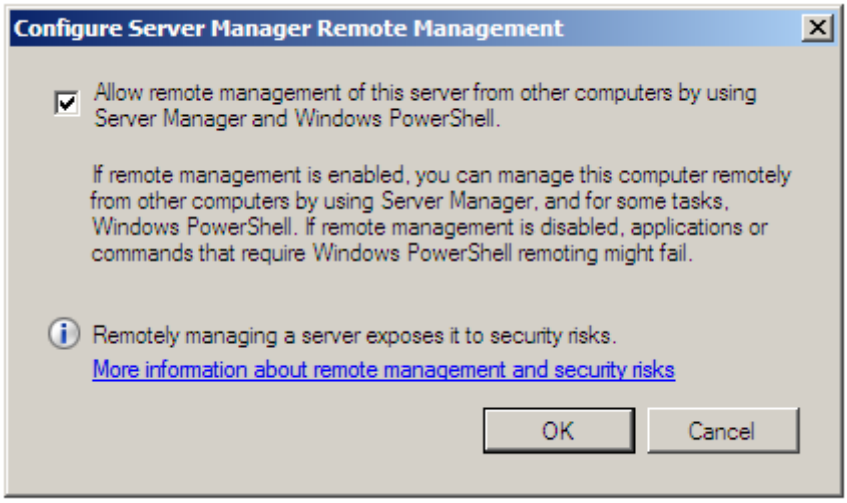
Enter-PSSession -Id 2
import-module servermanager
add-windowsfeature dhcp
get-windowsfeature backup
Get-PSSession | Remove-PSSession

Nem semmi.

A PS viszont láthatóan egy programozási nyelv, ebből következően nem mindig és nem mindenki számára egyszerű használni - előképzettség nélkül. Ezért a Microsoft az R2-be több könnyítést is tett a PS előnyeit kihasználni szándékozó rendszergazdák számára, ezek közül az egyik a Server Manager Remoting (az előbb tárgyalt PS Remoting segítségével), ami az RSAT hiányosságait igyekszik kiküszöbölni, míg egy másik segítség az Integrated Scripting Environment (ISE), ami egy grafikus felületű segédeszköz (telepíthető képesség) a PS teljes körű kihasználásához.

A felmérések szerint a Windows Server 2008 megismerése után, a felügyelet témakörben az 1. számú kérés a rendszergazdák részéről a távoli Server Manager

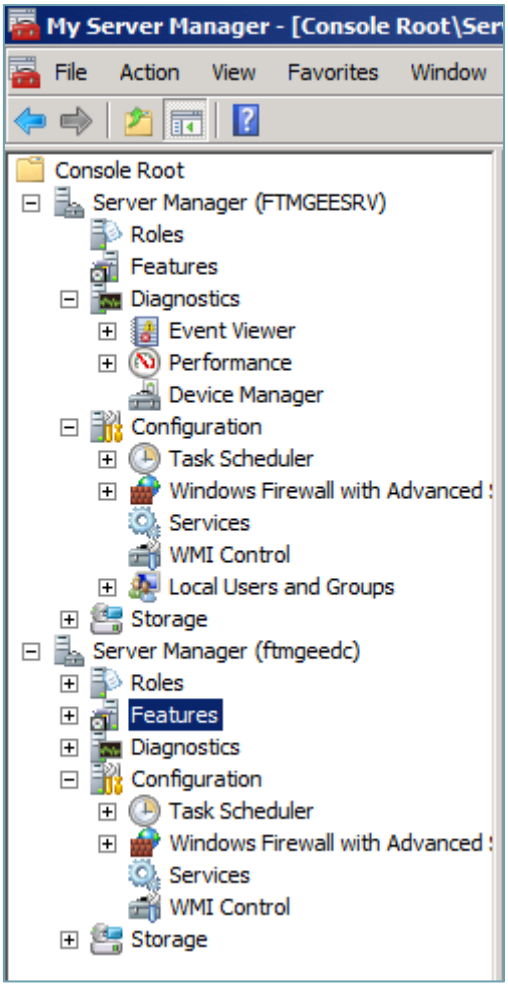
kezelés volt. Teljesült is, az R2-ben. Tudniillik, a két fejezettel előrébb lévő RSAT-tal csak a komponensek felügyeletét tudtuk ellátni pl. egy Windows 7-ről, magát a Server Manager-t nem tudtuk betölteni. Ennek szerencsére vége, az új RSAT része a Server Manager konzol is (látható is kakukktojásként a 4.10-es ábrán). És csak egyetlen dolog kell az engedélyezéshez: a Server Manager nyitólapján a „*Configure Server Manager Remote Management*" pontra kattintva az előző ábra jön fel, amiben egyetlen pipával ki is adhatjuk ezt az engedélyt.



4.6 ÁBRA CSAK EGYETLEN PIPA

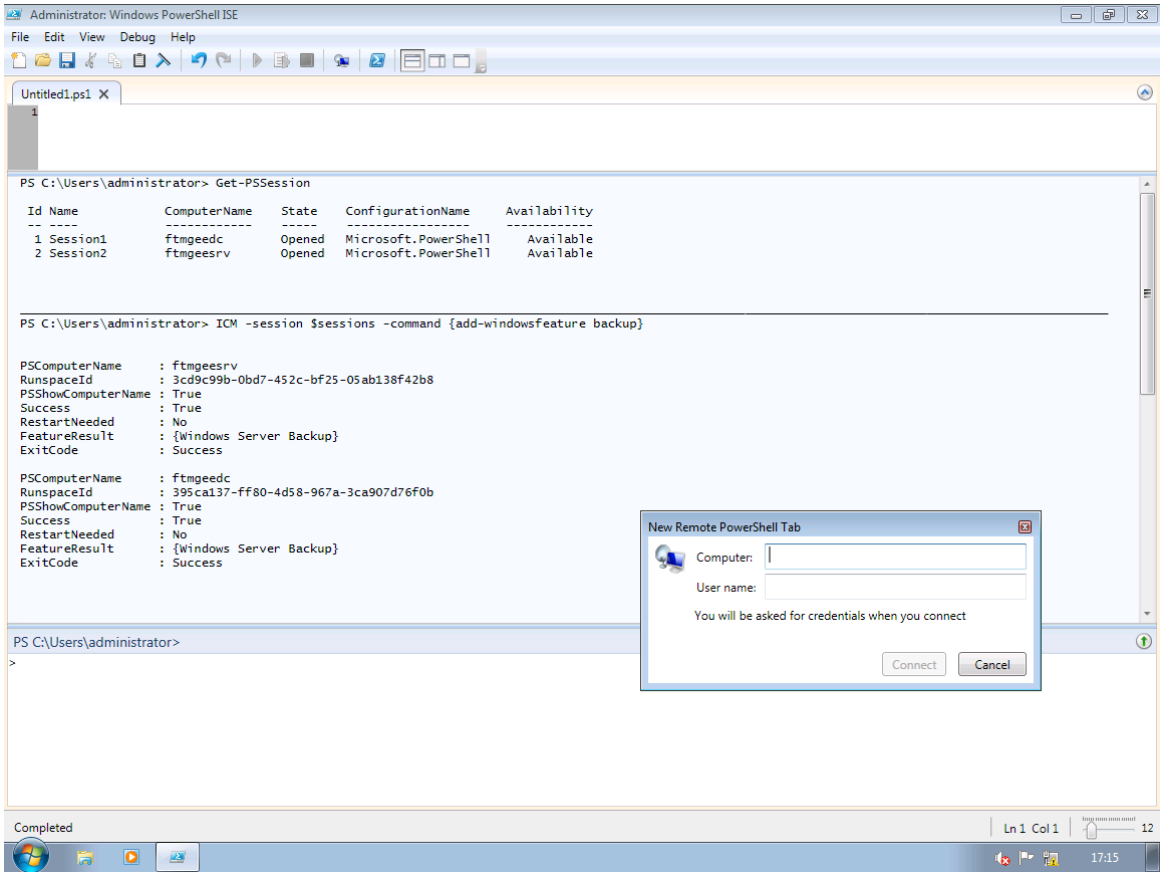
> A ráadás az, hogy ez a PS funkció bővülés kihasználható lett a Windows Server Core verzióján is, hiszen az R2-től kezdve a Core alatt is van PS támogatás és .NET Framework (lásd később).

Sőt, igazából egy rendes MMC konzol módjára, több kiszolgáló Server Manager-ét is beletölthetjük egyetlen konzolba, de csak úgy, ha elindítunk egy üres MMC-t, és külön-külön betöltjük, majd elmentjük, mivel a „gyári" Server Manager-ből párhuzamosan nem megy.



4.7 ÁBRA MULTISERVER MANAGER

Ahogy korábban említettem, a másik példa, az ISE egy tényleges mankó az amatőr PS használóknak egy GUI, azaz egy grafikus felület formájában. Így néz ki:



4.8 ÁBRA TETSZETŐS MANKÓ, ÉN SZERETEM IS HASZNÁLNI

Természetesen itt is működik a Remoting, azaz távoli használatra is alkalmas, látszik is a képen, hogy éppen túl vagyok az előző két szerverre egyszerre történő Windows Server Backup képesség telepítésén, és már nyitottam is egyszerűbben egy új Remote Shell panelt. Pont ez a lényeg az ISE használatnál, az egyszerűség és a grafikus felület lehetőségeinek a kihasználása. Ismerkedjünk meg vele, próbálgassuk, megéri.

4.3 BPA

A BPA jelentése a „Best Practice Analyzer”, és szerencsére jó régóta létezik ez az ingyenesen letölthető eszköz a Microsoft szervereihez, eleinte csak Sharepoint-hoz és Exchange-hez, de aztán pl. az ISA, SQL, stb. kiszolgálókhoz is megjelentek sorra a megfelelő verziók. És most már az operációs rendszerekhez is, hiszen az R2 óta immár nem egy külön letölthető változatban, hanem a Server Manager-be beépítve is találkozhatunk a BPA tudásával.

Személy szerint nagyon szeretem ezeket a segédeszközöket, mert egyrészt sokszor tudom ajánlani, ha kérdeznek, mivel ha kezdők vagyunk (mindenki így indul), akkor a tippek, illetve a konfigban per pillanat lévő hibák vagy hiányosságok listázása remek terep a tanuláshoz (arról nem is beszélve, hogy *problémákat* oldunk meg ☺).

Másrészt sokat segítenek az olyan borzasztóan elbizakodott szakembereknek is, mint például én. Miért is? Egyszerű: ki emlékszik arra, hogy pl. az évekkel ezelőtt beállított rendszerben beállítottam-e[35] a hálózati kártyák kötését a DNS-ben? A BPA majd megmondja. Ki emlékszik arra, hogy vajon minden ISA Server alatti WS03 SP2-ben lelőttem a Scalable Networking Pack-et a megfelelő registry variálással? Az ISA BPA majd megmondja. Honnan tudom meg, hogy bizonyos Public Foldereken nincs öröklődő NTFS jogosultság (mert 342 éve egyszer átállítottam, egy őrült problémamegoldó éjszaka során), és ezért mondjuk az E2K10 migrációval baj lesz? Az Exchange BPA megmondja. Ésatöbbi, ésatöbbi, ésatöbbi. Szóval, ha bővül a BPA köre, én örülök. Márpedig bővül az R2 RTM kiadásban, nem is kicsit, nézzük csak meg konkrétan, melyekkel is?

- Active Directory Certificate Services
- Active Directory Domain Services
- DNS Server
- Web Server (IIS)
- Remote Desktop Services

De később is érkeztek frissítések a következő szerepkörökhöz[36]:

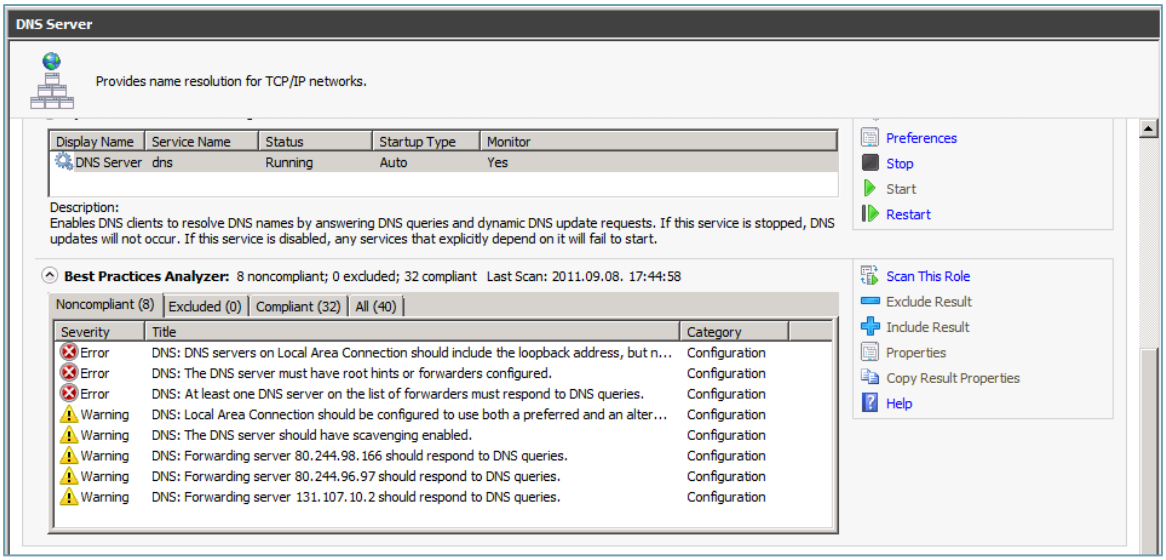
- Hyper-V
- NPAS
- AD RMS
- Application Server
- File Services (DFS/DFS-R is)
- DHCP
- WSUS

De mit is csinál a BPA? Összehasonlít. Egy ideális, optimális konfigurációt ahhoz, amit mi kalapáltunk össze. Ezenkívül felismer még jó pár jelenséget a termék működésével kapcsolatban, és a közölnivalóját három kategóriába osztva hibák, figyelmeztetések, vagy egyszerűen csak információs csomagok formájában és összesítve meg is jeleníti.

A használata pofonegyszerű, megkeressük a Server Managerben az adott szerepkör, pl. a DNS szerver nyitólapját, majd elindítjuk a BPA-t a jobb oldali panelen található „Scan this Role" paranccsal. A vizsgálat után jobb esetben örülünk, rosszabb esetben piros keresztes hibákat és sárga háromszöges figyelmeztetéseket kapunk egy listában, magyarázattal, tippekkel, amelyek alapján indulhat a probléma megoldása.

[35] Valószínű azért, hogy igen, mert ez már kiderült volna ☺, de példának jó lesz.

[36] http://blogs.technet.com/b/askds/archive/2010/04/28/win2008-r2-bpa-updates-released-for-april-2010-wave.aspx



4.9 ÁBRA VAN MIT JAVÍTANI[37]

Nem árt, ha megengedjük a Windows Update-en keresztüli frissítést, ugyanis ez olyan eszköz, amely tudásanyagát a Microsoft ígérete alapján rendszeresen frissítik (ahogy láthatjuk is az előző oldalon) a beérkező problémák és hibajelenségek, leírások apropóján.

És azért ne feledjük: a BPA csak megmutatja, meg nem oldja a problémát! ☺

4.4 Az RSAT

Remote Server Administration Tool a becsületes neve ennek az eszköznek, ami a Windows Server 2008-cal együtt született, és a korábbi Windows Server 2003 Administrative Tools Pack (Adminpak.msi) csomagot volt hivatott leváltani (a Vista megjelenésekor sajnos még nem is volt kész, ergo az Adminpak.msi-vel kellett trükköznünk, sokat), no és persze megújítani. A cél az volt, hogy a rendszergazdák ne csak a szerver konzolon vagy RDP-vel legyenek képesek elérni a szerveren futó szerepkörök és képességek konfigurációs lehetőségét, hanem a saját munkaállomásukról is, ahol valószínűleg mostanság egy Windows 7 fut.[38] [39]

Ha az utóbbihoz tartozó RSAT verziót[40] használjuk és egy R2-es kiszolgálót óhajtunk felügyelni, akkor a következő szerepköröket (és a részeiket is) leszünk képesek a

[37] Mielőtt szó érné a ház elejét, jelzem, hogy direkt kreáltam problémákat a DNS-ben ☺

[38] Persze az egyik szerverről a másikat az RSAT-tal elérni könnyebb, hiszen be van építve a képességek közé, de nyilván nem ez a tipikus használati mód.

[39] De nem is atipikus. Az Exchange szerver telepítésének például erősen javasolt előfeltétele az RSAT, ugyanis ezen kereszül lehet az AD-t is matyizni. (A lektor megjegyzése).

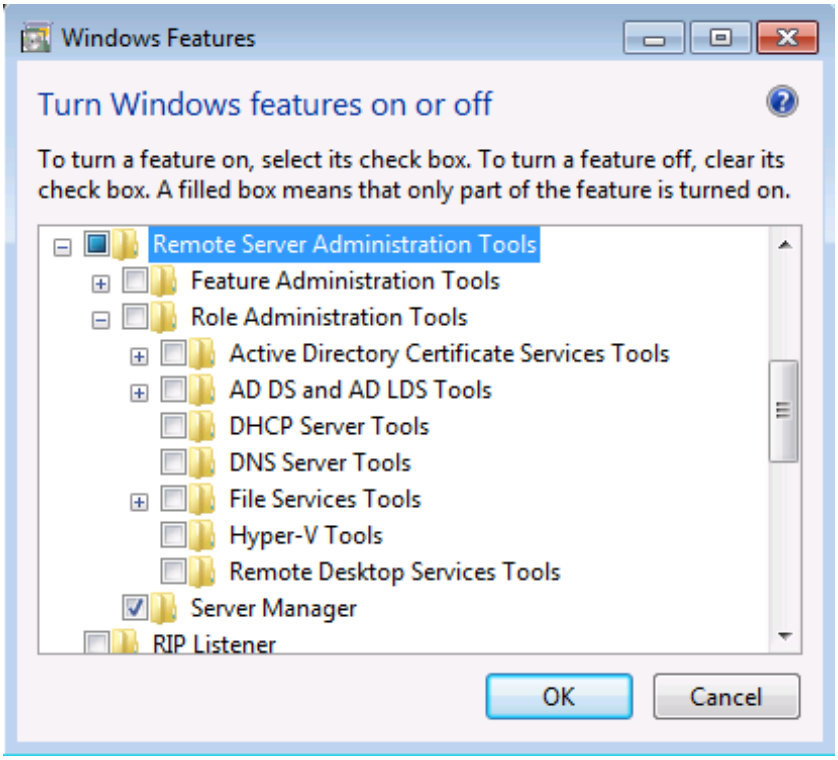
[40] Remote Server Administration Tools for Windows 7 with Service Pack 1 (SP1): http://www.microsoft.com/download/en/details.aspx?id=7887

munkaállomásról felügyelni (a Server Manager-t már említettem, ezért nincs is a listában):

- Active Directory Certificate Services (AD CS) Tools
- Active Directory Domain Services (AD DS) Tools
- Active Directory Lightweight Directory Services (AD LDS) Tools
- DHCP Server Tools
- DNS Server Tools
- File Services Tools
- Hyper-V Tools
- Remote Desktop Services Tools

Képességek esetén pedig a következő lehetőségeink vannak:

- Bitlocker AD Password Recovery Viewer
- Failover Clustering Tools
- Group Policy Management Tools
- Network Load Balancing Tools
- SMTP Server Tools
- Storage Explorer Tools
- Storage Manager for SANs Tools
- Windows System Resource Manager Tools



4.10 ÁBRA AZ RSAT CSOMAG RÉSZEI, A PIPA KAKUKKTOJÁS

A letöltés után (figyeljünk oda, mert külön változatok vannak a Vistához és a Windows 7-hez, sőt utóbbi esetén az SP1-hez is, plusz x86/x64 megkülönböztetés is van) egy

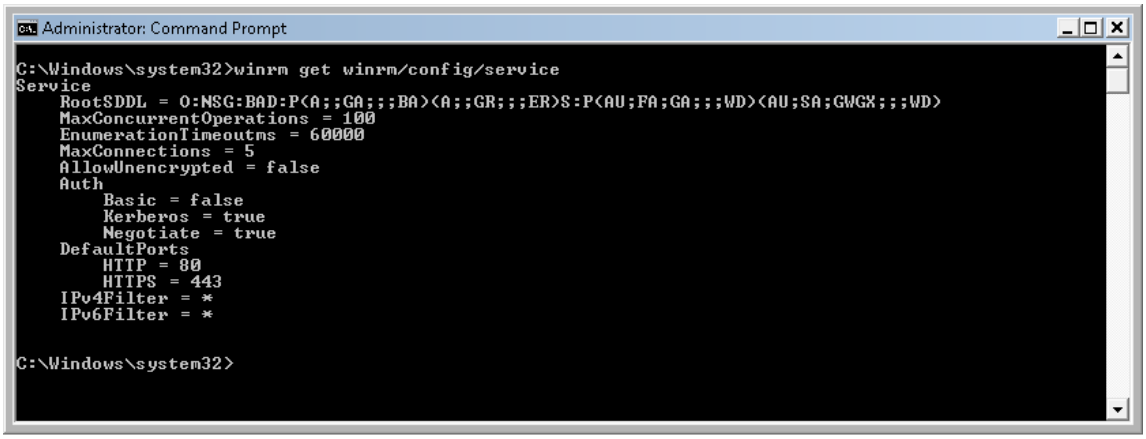
„next-next finish” módszerrel feltelepíthetjük a gépünkre az RSAT-ot. De ettől használni még nem fogjuk tudni, egy második körben külön kell bejelölni a különböző felügyeleti komponenseket. Ehhez keressük meg a „Programs and features” elemet a Vezérlőpulton, majd jöhet a „Turn Windows features on or off”., és innentől már csak választanunk kell.

4.5 WS-MANAGEMENT

A WS-Management a Microsoft és számos más IT-nagyvállalat (pl. IBM, Sun, Intel, AMD, Dell stb.) által közösen kifejlesztett, SOAP szabványra épülő rendszerfelügyeleti technológia, mely lehetővé teszi, hogy a felügyelt eszközök (legyenek azok szoftverek, vagy hardverek) egységes protokollon keresztül egyaránt elérhetők és kezelhetők legyenek. A Windows Remote Management (WinRM) pedig a WS-Management szabvány Microsoft által megvalósított implementációja, mely távoli számítógépek felügyeletét és menedzselését szolgálja – az ismert webprotokollokon (HTTP/S), többféle hitelesítési módszerrel (Basic, Digest, Kerberos) és „tűzfalbarát” módon.

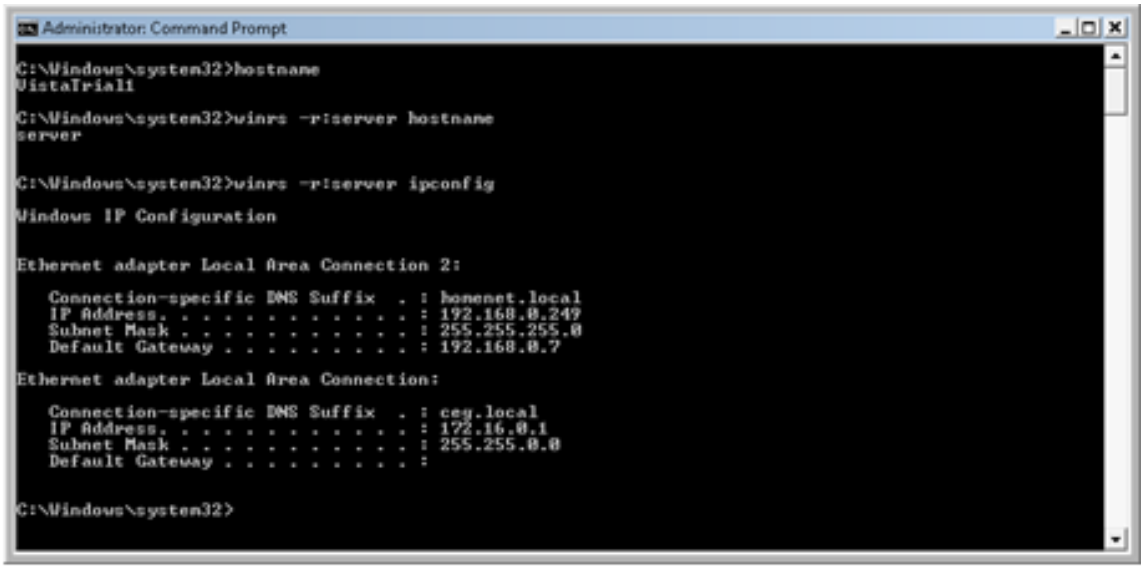
> Mivel az adatgyűjtés az imént említett webprotokollokon keresztül zajlik, az egész művelet egyszerű webszolgáltatásként kezelhető, valamint zökkenőmentesen együttműködik a már meglévő webes szolgáltatásokkal, például az IIS-sel. Bár a WinRM nem függ az IIS-től, ha mindkét szolgáltatás aktív, közös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

A WinRM konfigurálásához használjuk a „winrm quickconfig” parancsot, amely elindítja és automatikus indításúra teszi a WinRM-szolgáltatást, létrehozza a tűzfal kivételszabályát, valamint egy HTTP/S listener-t, amelyen figyeli a beérkező kéréseket. Az operációs rendszeren mindezt a rendszergazdai parancssorból (jobb gomb a parancssor ikonon és „Run as administrator”) indíthatjuk el. A WinRM alapértelmezés szerint a Kerberos hitelesítést használja a 80-as HTTP-porton, erről – és több egyéb, a szolgáltatást érintő paraméterről – meggyőződhetünk a „winrm get winrm/config/service” paranccsal.

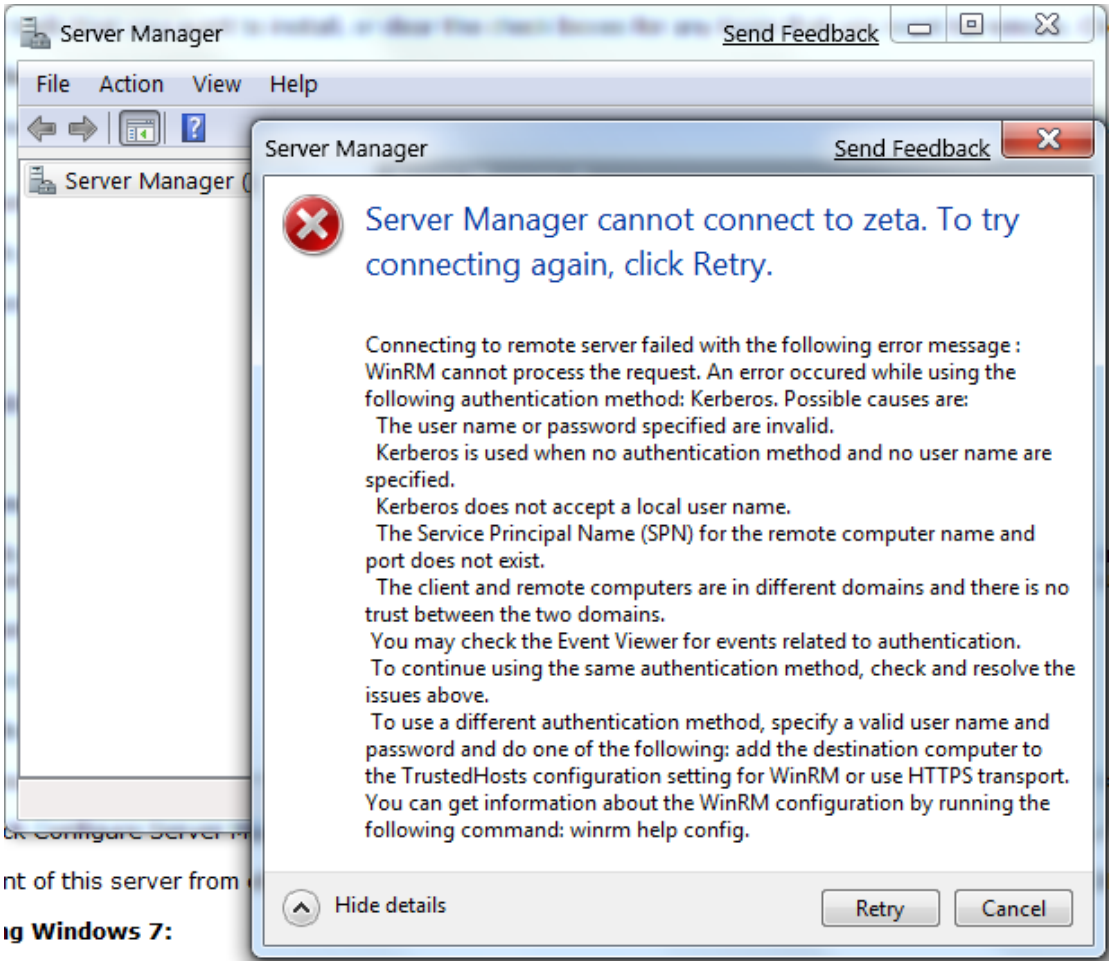


4.11 ÁBRA A WINRM SZOLGÁLTATÁS ÁLLAPOTÁNAK LEKÉRDEZÉSE

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



4.12 ÁBRA A WINRS-SEL KÉPESEK LESZÜNK A TÁVOLI GÉPEN PARANCSOKAT FUTTATNI



4.13 ÁBRA A SERVER MANAGER REMOTING IS WINRM-MEL MEGY, DE PERSZE WINDOWS SERVER 2003-RA NEM FOG SIKERÜLNI

E fejezet lezárásaképp jelezném, hogy a felügyeleti eszközök körébe természetesen beletartoznak olyan komponensek is, mint a Feladatkezelő, az Eseménynapló, a Feladatütemező vagy éppen a Teljesítmény figyelő és még sokan mások. Mivel ezekben az eszközökben minimális vagy éppen zéró változás van, és mivel ezeket a már emlegetett előzmény könyvben részletesen kitárgyaltuk a Windows Vista kapcsán, ezért a felesleges oldalszaporítás helyett, elég lesz a linket megosztani a kedves Olvasóval:

> „Rendszerfelügyelet rendszergazdáknak”
> http://www.microsoft.com/hun/technet/article/?id=f0c8cf69-ae4c-4b1b-b333-9feeda419509

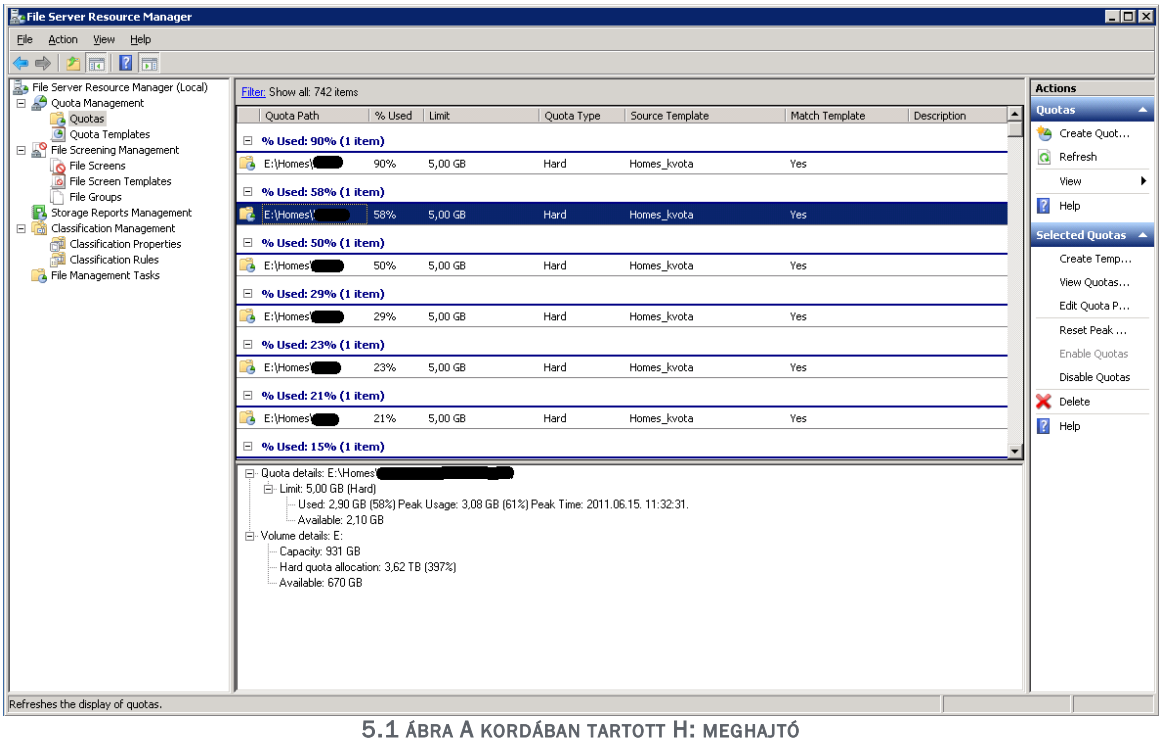
5 KISZOLGÁLÓ ALAPSZOLGÁLTATÁSOK

5.1 FÁJL- ÉS NYOMTATÓSZOLGÁLTATÁSOK

5.1.1 FSRM

A File Server Resource Manager (FSRM) MMC nem 100%-osan újdonság, sőt még a Windows Server 2008-ban sem az (a Windows Server 2003 R2-ből való), de sokszor érzem úgy, mintha nem is létezne, mintha nem is tudnának róla az üzemeltetők. Pedig figyelemre méltó, ráadásul van R2-es újdonságunk is, úgyhogy 1-2 oldalt megér most nekünk is. Négy fő része van:

- Storage reports management: Jelentéseket generál az általunk kiválasztott állományok illetve mappák használatáról. Rengeteg mintát adhatunk meg a jelentés kritériumaként, pl. lehetséges állománytípusok vagy felhasználók vagy állománycsoportok alapján szűrni vagy éppen a két vagy több példányban létező állományokat is kiszűrhetjük, de létezik minta a nagyméretű vagy a legtöbbet/legkevesebbet használt állományok listázására, illetve akár a kvóta használat nyomon követésére is. Nagyon részletes, további finomítási lehetőségeink is vannak egy-egy kategórián belül. A jelentést kérhetjük e-mailben - természetesen időzíthetjük is -, de van lehetőségünk - alapértelmezésben DHTML, vagy HTML, XML, DSV illetve sima szöveg formában - menteni is.
- Quota management: A már a Windows 2000 Server óta használható (?) kvóta menedzser drasztikus változásokon ment keresztül. Nincs többé a csak lemezre vonatkozó korlát, akár mappánként különböző korlátokat adhatunk meg. Nincs többé a logika méret alapján történő számolás, hanem a lemezhasználat számít, és nem kell többé kizárólagosan az Eseménynaplót figyelgetnünk, az FSRM pl. e-mailben is értesíthet, és képes adott szkriptet vagy parancsokat futtatni illetve jelentéseket gyártani, ha "esemény" van. Kétfajta kvótát gyárthatunk, az ún. "hard" kvótát, amely megtiltja a felhasználóknak és az alkalmazásoknak a limiten felüli lemezhasználatot, illetve a "soft" kvótát is, amely nem ilyen "kőkemény", viszont értesítést ekkor is kaphatunk a túllépésről. Kellemes lehetőség a kvóta sablonok használata, melyeket egyszer kell alaposan megtervezni, és mindenre kiterjedően elkészíteni, és aztán ad hoc alapon alkalmazni.
- File screening management: A harmadik elem ebben a csoportban a "File screening", azaz egyfajta szűrési lehetőség, ti. megtiltja bizonyos állománytípusok (pl. .mp3, .avi, stb.) mentését az adott lemezre/mappába. Részletesen konfigurálható, léteznek hasznos sablonok és előre gyártott állománytípus csoportok, de tetszőlegesen bővíthető is. A kvóta menedzserhez hasonlóan itt is megkülönböztetünk kétfajta akciótípust: az "Active" tilt, a "Passive" csak értesít és van kivétel beállítási lehetőség.



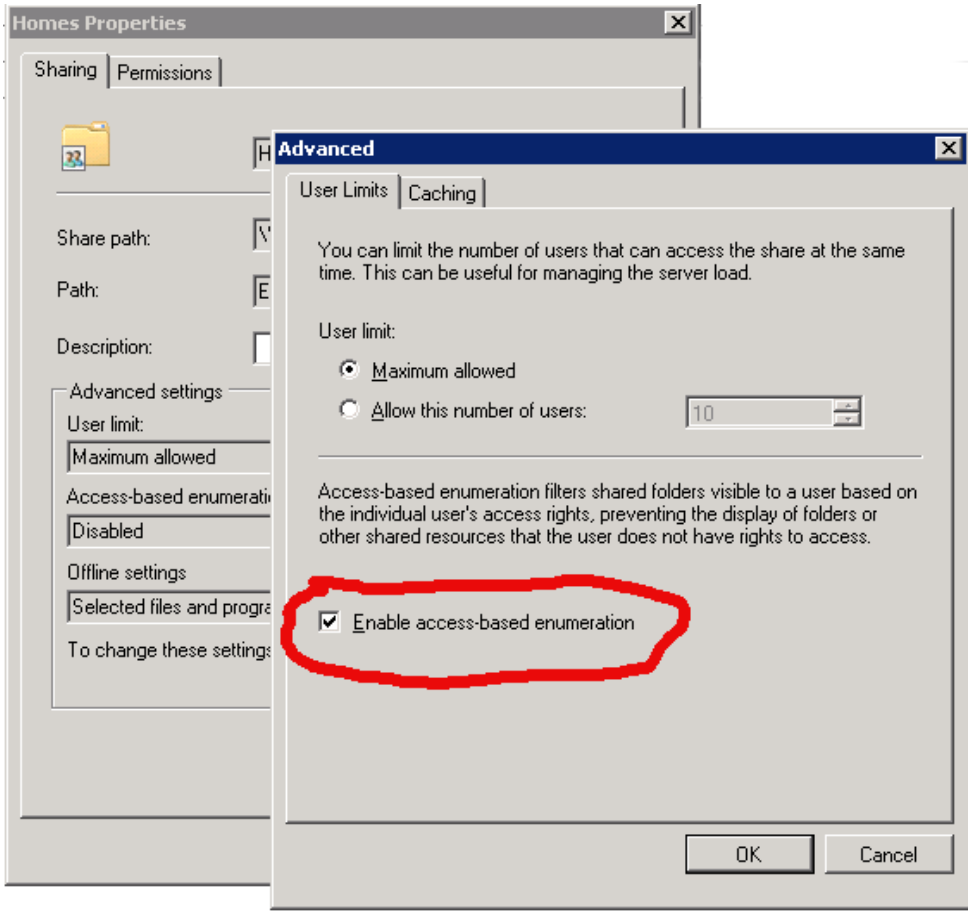
5.1 ÁBRA A KORDÁBAN TARTOTT H: MEGHAJTÓ

- Classification management: Csak az R2-ben létezik (ellenben minden kiadásban), és részben egyfajta „megjelölő” vagy inkább „besoroló” (classification) eszközről van, amellyel a fájlokat különböző tulajdonságaik alapján képesek leszünk logikailag csoportosítani, majd műveleteket végezni velük (File Management Tasks). Például egy nagy-nagy hálózati megosztásról a rendkívül ritkán használt fájljainkat elkülöníthetjük egy másik, lassú elérésű tárolási helyre, vagy az érzékeny fájlokat (mi mondjuk meg pl. kulcsszavakkal, hogy mi számít szenzitívnek) eltávolítjuk a megosztásból, vagy akár vízjelessé is tehetünk automatikusan dokumentumokat. Ha pedig az AD Rights Management Server-rel (RMS) kombináljuk, akkor az automatikusan azonosított és osztályozott érzékeny adataink úgy is biztonságban lesznek, ha különböző formákban (másolás, e-mail csatolás) elhagyják a szervezetünk informatikai rendszerét.

5.1.2 ABE

A Windows Server 2008-ban végre a grafikus felületen is megjelent *Access Based Enumeration*. Ismerős? Lehet, mivel volt már ilyen a Windows 2003-ban is, anno az SP1-gyel érkezett, de csak parancssorból érhettük el, és kissé fárasztó módon. Szóval eme durva nevű, de finom módszert takaró megoldás célja az, hogy akinek nincs joga egy hálózati megosztáshoz, az ne is *lássa* a tartalmát.

Ez régóta elvárt opció, sőt mondhatnánk teljesen természetes igény. Persze lehetett trükközni a mappa$-al és a testre (userre) szabott felcsatolással, de ez fárasztó és követhetetlen megoldásnak bizonyult már a múlt században is.



5.3 ÁBRA AZ ABE LEGYEN VELÜNK

De ennek vége, indítsuk el a sok más szempontból is érdekes "*Share and Storage Management*" MMC-t az Administrative Tools-ból, és ha varázslunk egy megosztást akkor egy adott lépésben az "Advanced" gomb alatt megtaláljuk a GUI-n is ezt a lehetőséget. Persze nemcsak a varázslóban állíthatjuk ezt be, hanem utólag is, sőt alapértelmezés szerint nem is minden esetben érvényes, azaz ha a lenti listában szereplő módszerekkel kreáltunk egy megosztást, akkor kézzel kell utólag beállítani:

- Az „Advanced Sharing” a Windows Explorer-ben
- Ha a „net share” parancsot használjuk
- Ha kötetek megosztásáról van szó
- Az admin megosztások esetén (kötetek vagy mappák, úgymint C$ vagy ADMIN$)

5.1.3 DFS ÉS DFS-R ÚJDONSÁGOK

A DFS és a DFS-R témakör szintén nem teljesen új, azaz a Windows Server 2003 R2-ben történtek az elsőkörös és igazán nagy változások (pl. az MMC bővítmények

változásai, vagy eleve a teljesen új replikációs megoldás, az új tömörítési algoritmussal[41]). De azért az újabb operációs rendszereknek sem kell szégyenkezni, vannak újdonságok szép számmal. Ezek közül kiemelnék most egy párat, először olyanokat, amelyek a Windows Server 2008-cal érkeztek.

Content Freshness

A DFS-R tartalmaz egy új, tartalom frissítő megoldást, ami megtiltja a kiszolgálónak, hogy bizonyos - offline állapotban töltött - idő után, vadul elkezdje szinkronizálni automatikusan - ha majd online állapotba kerül. Ez azért fontos, mert a DFS-R nagyjából ugyanúgy működik, ahogy az AD replikáció, azaz ez is JET adatbázis, és multimaster replikációt használ, és a törlés itt sem fizikai először, hanem logikai, azaz a jól ismert sírköves módszer, ami 60 nap után töröl csak - fizikailag is.

És itt jön a probléma: ha a DFS-R szerver több mint 60 napig nem tud replikálni, viszont utána majd egyszer csak igen, akkor a fájlok rég törölt példányainak a sírköve újra feltűnik, és persze replikálódik is, adott esetben konfliktusba kerülve a meglévőekkel[42].

A Content Freshness védelem nem alapértelmezett, hanem beállítható, méghozzá egyesével, minden DFS-R szerveren az alábbi paranccsal.

wmic.exe /namespace:\\root\microsoftdfs path DfsrMachineConfig set MaxOfflineTimeInDays=60

És amikor majd a CF él, akkor a régi-új szerveren letilthatjuk vagy törölhetjük a kapcsolatokat, leállíthatjuk a DSF-R szervizt, az időzítést rövidre zárhatjuk vagy akár kikapcsolva is tarthatjuk a gépet - ergo lesz időnk korrigálni.

A váratlan leállások kezelése

Az NTFS fájlrendszerben bekövetkező változások az esetek többségében először memóriában helyezkednek el, és csak egy kis idő után íródnak ki a merevlemezre. A DFS-R replikáció adatbázisa szempontjából viszont a változás már a diszkre írás előtt bekövetkezik. A köztes időben bekövetkező bármilyen katasztrófa, legyen az váratlan szerverleállás vagy szabálytalan volume-dismount, a DFS-R adatbázis inkonzisztenciájához vezethet. Míg a Windows Server 2003 R2 esetén ez a komplett DFS-R adatbázis újraépítésével és így rengeteg idővel járt, az új változat ezt az adatbázis újraépítése nélkül, azaz sokkal gyorsabban intézi el.

Propagation report

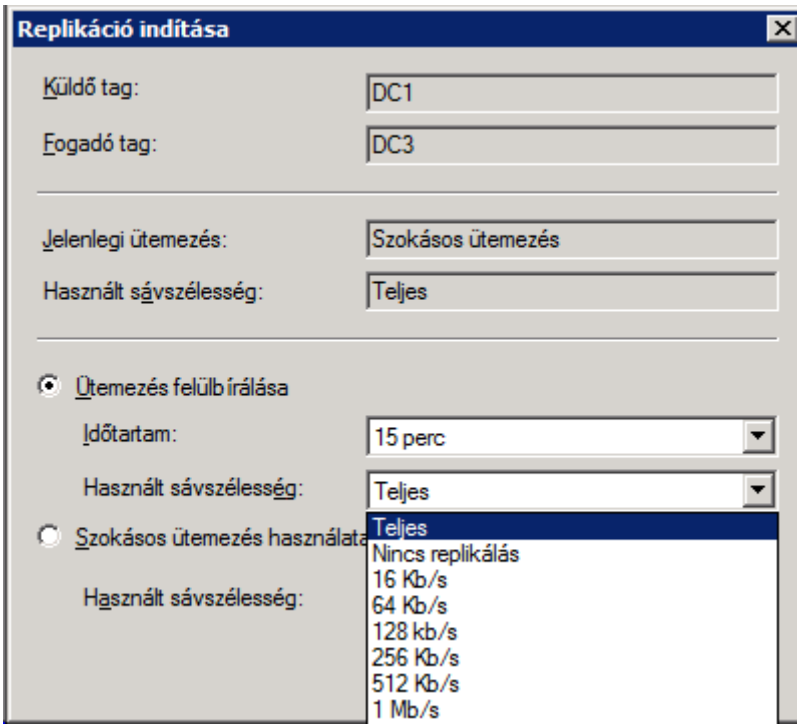
---

[41] Remote Differential Compression (RDC): http://technet.microsoft.com/en-us/library/cc781091%28WS.10%29.aspx

[42] Ez az AD-nál az ún. „lingering object” szituáció.

A DFS Management MMC tartalmazza egy új típusú diagnosztikai jelentés kérését ezzel a névvel. Ha ezt választjuk, akkor egy olyan jelentést hozhatunk létre, ami egy terjesztési teszt (ami igen fontos dolog, főképp az elején) replikáció állapotát követi.

Replicate now
Az azonnali, azaz a kijelölt célterületek között[43] felülbírálható időzítésű replikálást végezhetjük el ezzel a paranccsal, úgy, hogy egyben a kívánt sávszélességet is variálhatjuk. Kedvelem ezt az opciót, a gyakorlatban igen hasznos.



5.4 ÁBRA CSAK MOST, CSAK ITT

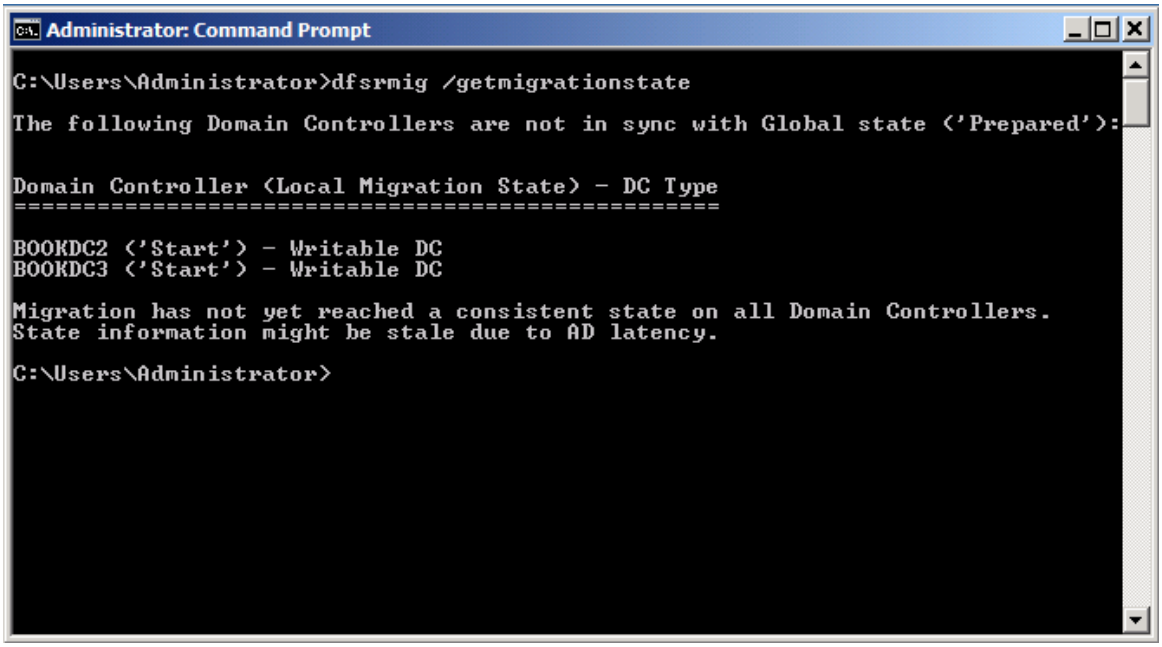
SYSVOL replikáció a DFS-R segítségével
Amikor a DFS-R megjelent a Windows Server 2003 R2-ben, akkor már csak egyetlen kérdés maradt. Kidobjuk-e az FRS-t? Nos, sajnos nem dobhattuk ki ezt a kövületet, mert egy fontos dolga megmaradt, ez pedig a tartományvezérlők "SYSVOL" megosztásainak replikációja.

De most már, a Windows Server 2008-ban akár ezt a feladatot is átruházhatjuk a DFS-R-re, bár nem kötelező. Egy biztos, az áttérést igen körülményesen és lépésről-lépésre kell megtennünk, mert bár lehet, hogy nagyon óhajtjuk és tényleg remek lenne az előnyeit kihasználni, de azért pl. a régi tartományvezérlőket (Windows 2000/2003) egész jól ki tudnánk akasztani az új replikáció módszerrel.

[43] A SYSVOL replikációnál - lásd következő bekezdés - nem működik.

Ergo az első lépés a tartományi működési szintjének emelése, ez úgyis csak akkor megy, ha már régi DC-ink nem lesznek. Ezután jöhet a DFS-R install minden DC-re, majd egy parancssori segédeszközre lesz szükség, a dfsrmig.exe-re, amivel a 4 különböző státuszt fogjuk átugorni, pontosabban hármat, mert alapból a 0. szinten vagyunk[44]. A migrációs állapotok a következőek:

0 START
1 PREPARED
2 REDIRECTED
3 ELIMINATED



5.5 ÁBRA A ELSŐ SZINTRE PRÓBÁLUNK FELKAPASZKODNI, DE 3 DC-BŐL 2 MÉG NEM OK

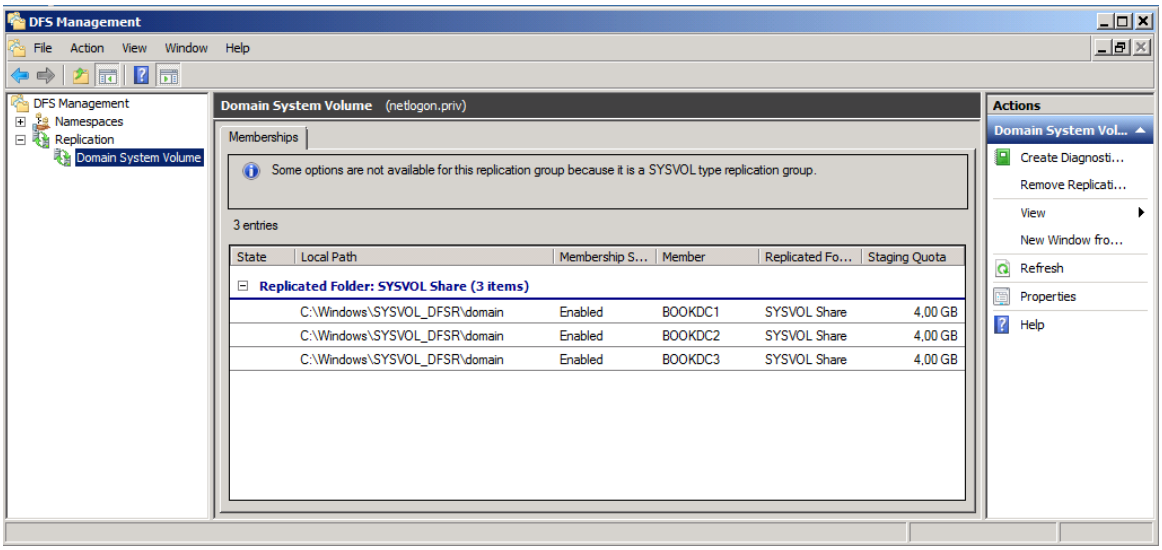
A további szükséges lépések:

- A *„dfsrmig /setglobalstate 1”* utasítás, minek hatására egyet ugrunk, és eközben a DFS-R készít magának egy másolatot a SYSVOL mappáról, majd egy másik DC DFS-R szervizével megpróbál egy kezdő replikációt végrehajtani. Ha ez sikerült az összes tartományvezérlőn, akkor mehetünk tovább. Ellenőrizni a "dfsrmig /getmigrationstate" paranccsal tudjuk ezt.
- Most jön a „dfsrmig /setglobalstate 2", ha OK, akkor erre válaszul párhuzamosan elkezd majd működni a replikáció, ami szintén lekérdezhető, ugyanúgy mint az előbb. Ami fontos, innen még mindig visszatérhetünk az FRS-re, de ez az utolsó esély.
- Az utolsó - értelemszerűen - a „dfsrmig /setglobalstate 3” parancs lesz, ennek hatására a DFS-R törli az eredeti SYSVOL-t, és az újjal megy tovább. Ellenőrizzük, és ha minden klappol, akkor majdnem készen is vagyunk, egy

[44] Csak óvatosan, mert a használata minden tekintetben globális, azaz bármelyik DC-n alkalmazzuk, az az egész tartományt egyformán érintő változtatást jelent.

dolgunk van még: az FRS-sel tudatni kell, hogy ennyi volt, nyugdíj. Ez például megoldható a szerviz leállításával, és kézi vagy letiltott indításúra történő beállításával[45].

Ha viszont teljes megoldást akarunk, akkor a stoppolt FRS mellett kitörölhetjük a JET adatbázist a %systemroot%ntfrsjet alól, így az újrainduló FRS létrehoz magának egy teljesen új adatbázist, amibe már nem is akarja majd a SYSVOL-t belereplikálni.



5.6 ÁBRA EZ MÁR EGY MODERN TARTOMÁNY

Természetesen a Server Core-ral is működik mindez, a képen látható BookDC2 pl. ilyen. No és még annyit szeretnék hozzáfűzni mindehhez, hogy a DFS-R SYSVOL replikációt nem tudjuk olyan részletesen konfigurálni a DFS Management MMC-ben, mint a többi replikációs csoportot, de ez valahol logikus is, örüljünk inkább szépen csendben a lehetőségnek ☺!

RODC támogatás (lásd 6. fejezet)
Miután a DFS replikációba a tartományvezérlők SYSVOL megosztása is belevehető, ebből az RODC sem maradhat ki. Egy RODC esetén viszont meg kell felelni az Active Directory-ban erre vonatkozó szabályának, miszerint az RODC-ről nem származhat semmiféle változás vissza a többi, írható-olvasható adatbázisú DC-re, de ez nem is gond, működik.

Az R2 fájlszerver szerepkörének is fontos és megbecsült része a DFS/R, ezért aztán ebbe a verzióba is került néhány újdonság.

ABE támogatás

[45] Bár úgy vettem észre, hogy az R2-ben ezt megoldja automatikusan.

Az ABE-t az előző fejezetben már részleteztem, így most elég csak annyit megjegyezni,hogy a DFS névtereknél az R2-ben szintén engedélyezhetjük a DFS Management konzollal vagy akár a Dfsutil.exe-vel, a parancssorból. De, mindez csak akkor működik majd, ha az összes DFS szerverünk Windows Server 2008 vagy R2.

Csak olvasható replikált mappák
Van olyan lehetőségünk is az R2 DFS-R alatt, hogy egy replikációs csoporttagot csak olvashatónak jelölünk meg, azaz így megtilthatjuk a felhasználóknak, hogy az adott mappa tartalmát módosíthassák. Persze ezt eddig is megtehettük, de csak manuálisan, az NTFS jogok konfigurálásával, de így még egyszerűbb, igaz kicsit nagyobb terhelést kap emiatt a DFS szerver.

A RODC-nek csak egy read-only SYSVOL jár
RODC támogatás már eggyel korábban is volt, ám az R2-ben ez tovább bővült, mivel innentől a RODC SYSVOL mappája egy csak olvasható replikált mappává alakult át. Ez az igazi megoldás, mert így nem lehet ebben a mappában sem változás, csak felülről indítva.

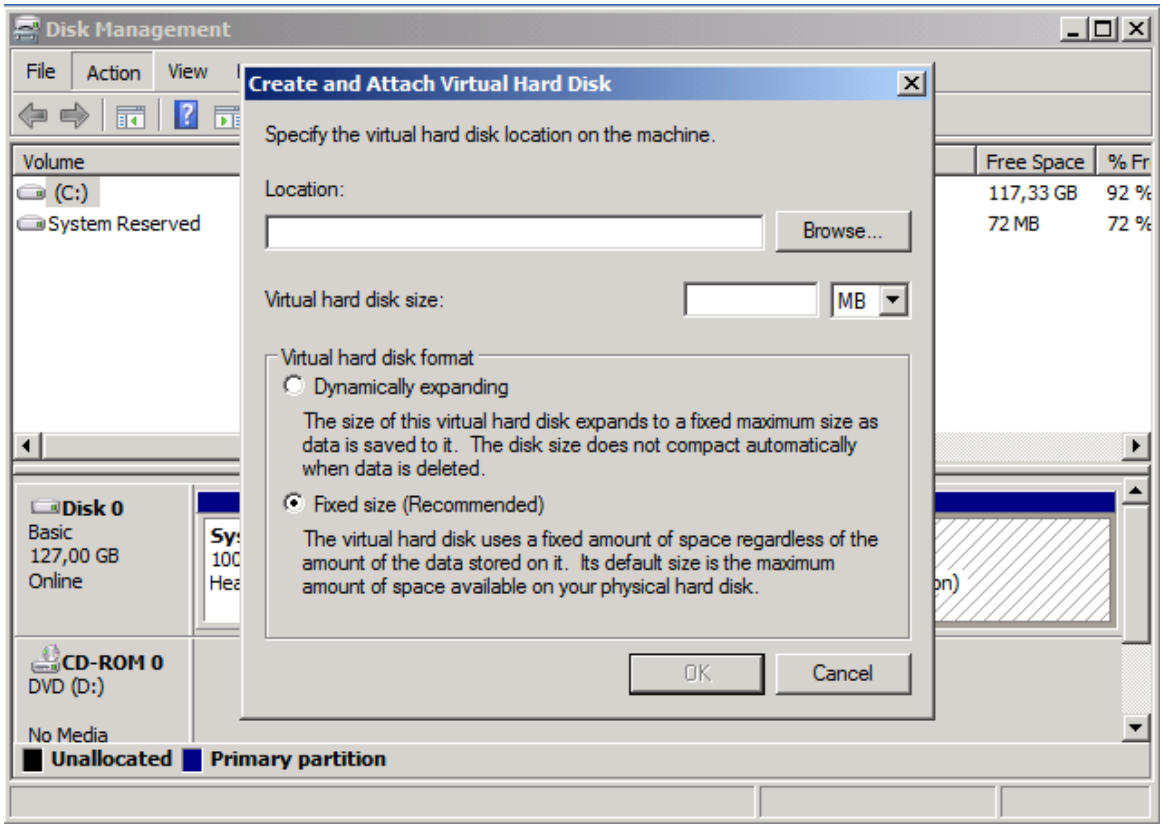
Failover cluster támogatás
Az R2-es DFS-R megteremti a lehetőséget arra, hogy egy failover cluster is tagja legyen egy replikációs csoportnak, azaz pl. a clusterezett fájl megosztások ezután replikálhatóak lesznek. A korábbi verzióknál ez az együttműködés nem volt lehetséges, azaz a szolgáltatás nem költözött át egy másik node-ra, ha az adott tagon futott.

5.1.4 VHD KEZELÉS, VHD BOOT

Ez a szakasz viszont teljesen új megoldásokat takar, és a második rész például elég megdöbbentő újdonság is egyben.

Az első nem annyira, ugyanis a VHD kezelés a Disk Management MMC-ben kezdődik, ahol (most csak az R2-ről van szó[46]) innentől kapunk egy .vhd készítési illetve felcsatolási lehetőséget.

[46] De mindez a Windows 7-re is igaz azért.

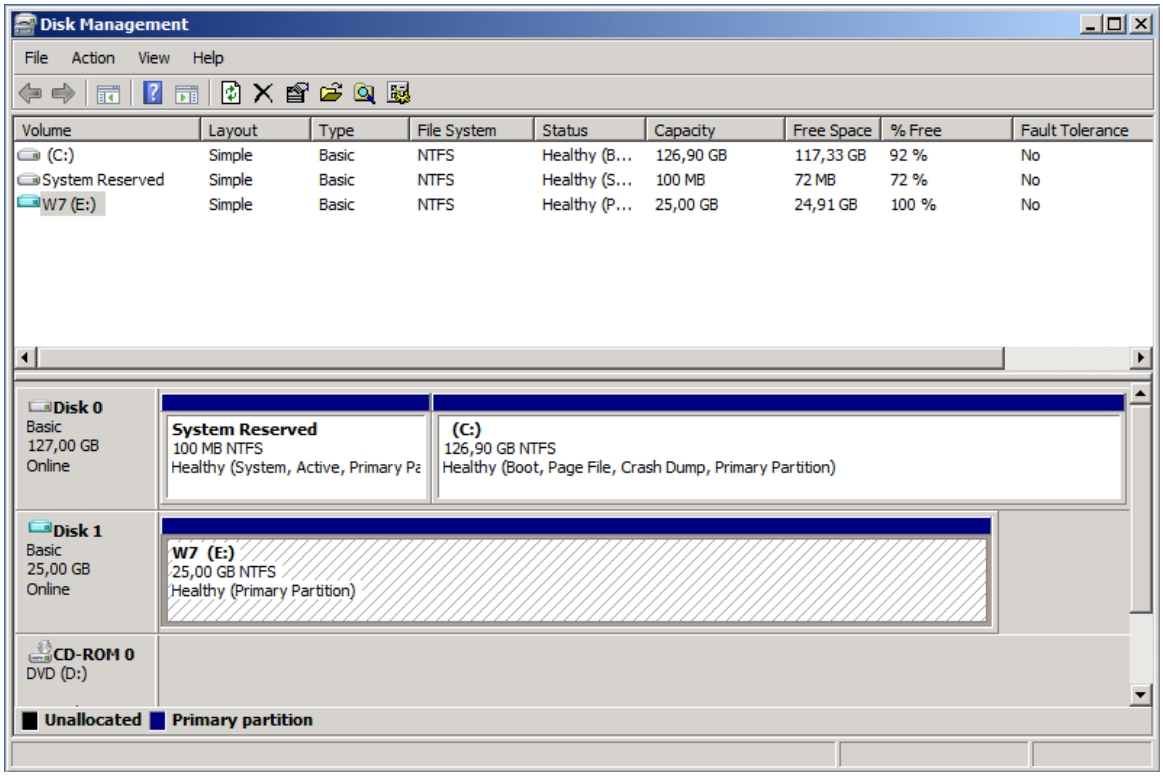


5.7 ÁBRA VAN „CREATE ÉS ATTACH", ÉS PERSZE „CREATE AND ATTACH" IS

Az .vhd készítésnél választhatunk, hogy mekkora és hogy milyen típusú legyen, ha pedig van már egy vhd. fájlunk (mert pl. egy Hyper-V alól kiszedtünk egyet), akkor csak be kell tallóznunk, máris egy új kötetként látjuk majd.

A második dolog viszont ennél lényegesen bonyolultabb. Tömören: létrehozhatunk egy multi-boot-os rendszert úgy, hogy a második, harmadik, stb. operációs rendszer a fizikai gépünkön egy .vhd fájl formájában létezik majd mindösszesen. Elképesztő, nem? Nos, a következő folyamat lépéseiben azt mutatom meg, hogy pl. egy R2 alá hogyan teszünk be egy Windows 7 OS-t. Nem annyira életszerű példa, de most nem is ez a lényeg, hanem a lehetőség.

Nos, a konfigurálás lépései is úgy kezdődnek, mint ahogy az előző képen látszik ti. először le kell gyártanunk egy .vhd fájlt (ez lesz az új OS diszkje, úgyhogy csak okosan a méretét) valahová a gépünkre helyben, azaz a HDD-nk valamelyik partíciójára. Majd ezek után csatoljuk fel, és formázzuk meg NTFS-re, és adjunk neki egy betűjelet, mondjuk a példa kedvéért a V:-t!



5.8 ÁBRA CSAK EGY KÜLÖNBSÉG VAN, A DISK1 IKONJA ZÖLDESKÉK SZÍNŰ

A második lépéscsokor arról szól, hogy a Windows 7-es telepítő image-et rá kell gyógyítani erre a .vhd fájlra, azaz ez olyan lesz, mintha egy fizikai gépnél betoltuk volna a DVD-t, és a másolás fázist is megtettük volna.

- Az ImageX.exe-re van szükségünk (ez a WAIK része, ami látszik is az elérési útból) illetve az install.wim-re (ez a W7 DVD-n lesz) és a következő parancsra:

  cd /d "c:\program files\Windows AIK\tools\amd64\" imagex /apply <full path to install.wim> 1 V:

- Ez beletelik egy kis időbe, de ha kész, akkor bootolhatóvá kell tennünk az új kötetünket a BCDBoot paranccsal::

  cd c:\windows\system32 bcdboot v:\windows

- Ezután válasszuk le a diszket a Disk Management MMC-ben, vagy egyébként a DiskPart-ot is használhatjuk erre, hiszen fel van rá készítve:

  diskpart
  select vdisk file=c:\temp\w7.vhd
  detach vdisk
  exit

Ezután egy újraindítás jön, és aztán meg fogunk döbbenni, megjelenik a boot menü, és ha a Windows 7-es részt indítjuk, akkor egy Windows 7 telepítés kezdődik, pontosabban folytatódik. Ha viszont kész lesz, akkor egy teljes értékű új operációs rendszerünk lesz, ami viszont csak egyetlen .vhd fájl – egy másik operációs rendszerben ☺.

5.1.5 Nyomtatószolgáltatások

A hálózati nyomtatók kezelése fontos és alapvetően szükséges gyakorlatilag minden hálózatban, épp ezért muszáj, hogy jól megismerjük és jól ki is használjuk a nyomtatókezelést támogató szolgáltatásokat. Nyomtatók biztonságos és praktikus használata, valamint migrációja, a printszerverek és a felügyeleti feladatok központosítása, a nyomtatási sorok korrekt kezelése, illetve a hálózati nyomtatók automatikus telepítése a Csoportházirend segítségével - mind-mind megoldható, és a már ismert megoldásoknál szinte minden területen vannak újdonságok is.

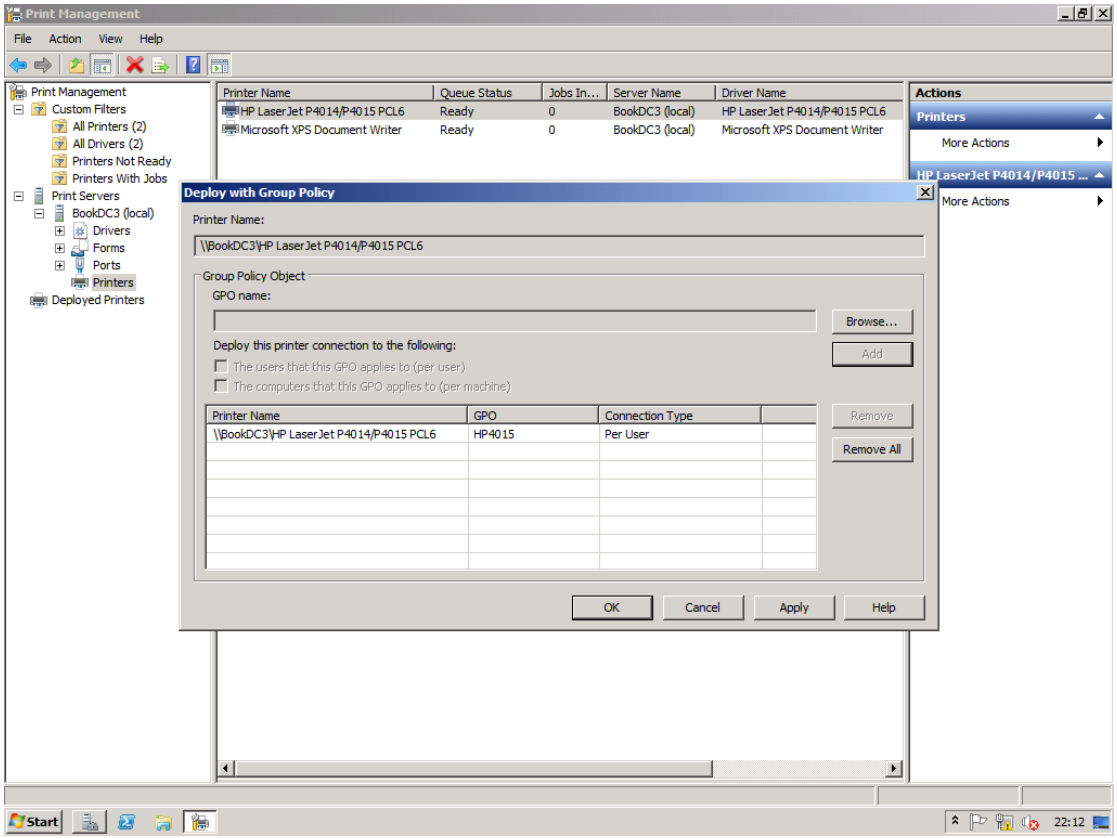
Nyomtatótelepítés a Csoportházirendből

A Print Manager Console (PMC) telepítése (Server Manager > Print Services[47] > Print Server) nélkül is installálhatunk és használhatunk hálózati nyomtatókat, de amit ezzel leszünk képesek művelni, az egy másik kategória. Ha PMC-ben már bepakoltunk egy hálózati nyomtatót (pl. SNMP-vel automatikusan megtalálva), akkor a helyi menüjében a „Deploy with Group Policy” pontot kiválasztva egy GPO-hoz rendelhetjük hozzá, kétféle módon:

- User: ekkor azok a felhasználók, akikre vonatkozik majd a GPO, mindig megkapják a printert, akármelyik tartományi gépen lépnek be, gyakorlatilag „követi” őket az adott printer minden gépre.
- Computer: az adott számítógépeken mindig elérhető lesz a printer, bármelyik felhasználó számára, aki belép.

Aki sok printert felügyel, ezért hálás lesz, bár aki sok printert felügyel most is, az tudja, hogy ez sem teljesen újdonság, hiszen a Windows Server 2003 R2-ben ez a módszer már működött. Igaz, sokkal körülményesebben, meg kellett keresnünk egy PushPrinterConnections.exe nevű apró segédprogramot a PMC telepítése után, majd az adott GPO-ba (ha a felhasználóról volt szó, akkor a logon szkriptbe, ha a számítógépekről, akkor a startup szkriptbe) bele kellett tenni egy hivatkozást, illetve az adott GPO-ba ezt a fájlt bele is kellett másolni.

[47] Csak jelzem, hogy a Windows Server 2008-ban hívják így.



5.9 ÁBRA A PMC EGYÜTTMŰKÖDIK AZ AD-VAL - A LEGNAGYOBB ÖRÖMÜNKRE

Macerás volt, de működött igen szépen, viszont erre az egész kínlódásra ma már nincs szükség, ha minimum egy Vista vagy Windows Server 2008 gépről van szó, ergo elég csak a hozzárendelést legyártani, és az ezek után a GPMC-ben megjelenő printer GPO-kat a kívánt felhasználókra/számítógépekre ráirányítani.

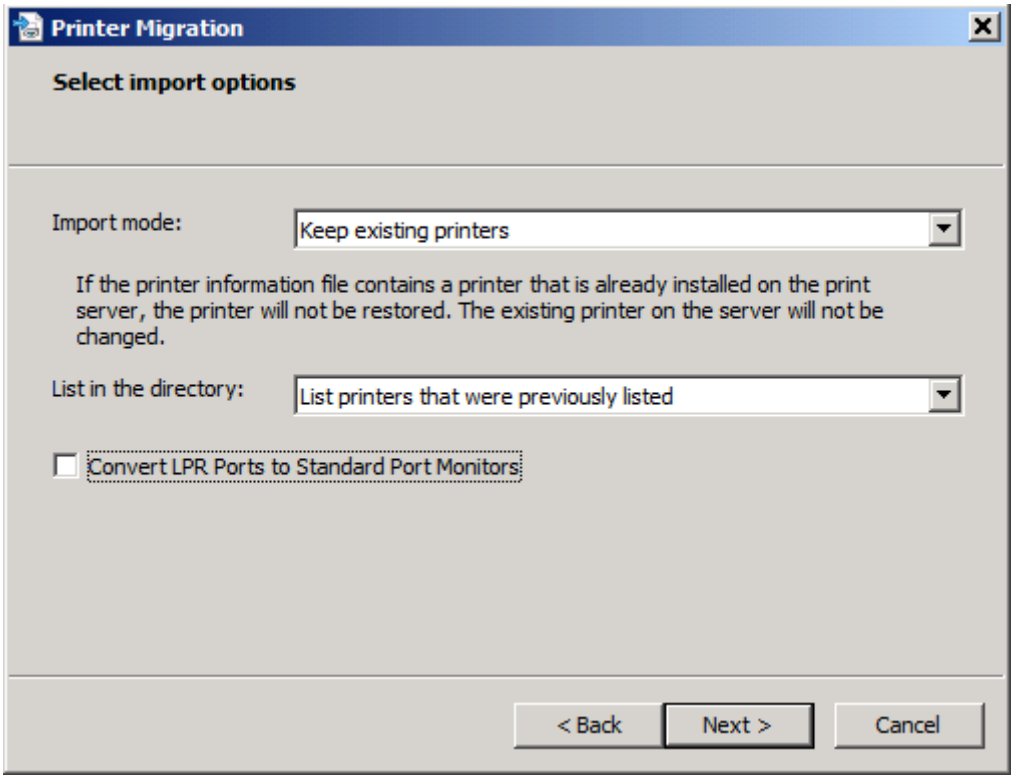
> Fontos az, hogy ehhez a módszerhez az AD sémájának minimum Windows Server 2003 R2-es vagy Windows Server 2008-asnak kell lennie, de ez már nem is annyira fájó dolog, igazából én is csak kötelességből említettem meg.

A Windows Server 2008 R2-ben ez a szerepkör új nevet kapott (Print and Document Services) és többek között kibővült olyan nagyobb mutatványokkal, mint a hálózati szkennerek használata (Distributed Scan Server service role, amelyhez van egy dedikált MMC is) illetve 1-2 további extrával is.

A printer migrációs lehetőségek bővülése

Ha sok hálózati printerünk van, és így sok-sok nyomtatási sor és sok-sok meghajtó program és esetleg költözik a szerver, akkor a migráció valamilyen automata eszköz nélkül borzalmas rémálommá válik. Szerencsére ehhez azért mindig is volt valamilyen eszköz, pl. a Windows Server 2003-nál ez volt a Print Migrator 3.1-es verziója, de továbbléptünk és a Windows Server 2008-ban egy új eszközünk lett erre a feladatra, sőt kettő is. Az egyik a PMC-ből indítható varázsló, a másik pedig egy parancssori eszköz, a Printbrm.exe.

Ezekkel minden gond nélkül lehetséges akár több száz, több ezer printer adatainak mentése és visszaállítása (csak R2), exportja és importja, beleértve a nyomtatási sorokat, a beállításokat, a print processzorokat és a portokat is, sőt egyéb a printer driver izolációs beállításokat is migrálhatjuk, vagy pl. mentésből vissza is tölthetjük a nyomtatási sorok biztonsági beállításait (az utóbbi két dolog szintén csak az R2-re vonatkozik).



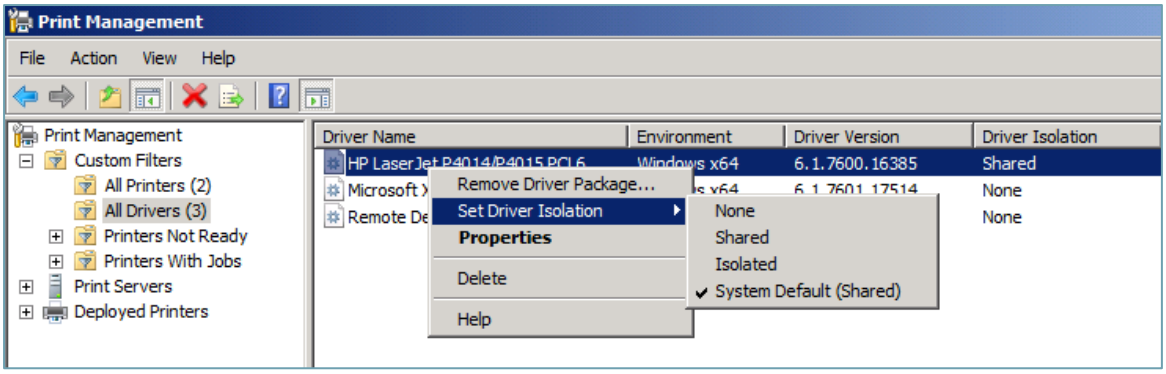
5.10 ÁBRA A MIGRÁCIÓ VÉGÉN MÉG EXTRA DOLGOKAT IS BEÁLLÍTHATUNK

Printer driver isolation

Ha sosem volt még printer driver fagyás a nyomtatószervereden, akkor ugord át ezt a részt! De inkább mégse ☺!

Az R2 előtt ha egy bármilyen okból problémás nyomtató meghajtó szoftver[48] esetleg szétfagyott, akkor minden valószínűség szerint kiakasztotta az egész printer spooler processzt, és így az egész nyomtatási alrendszert, tehát a *„mindenki egyért”* elv szépen működött. Az R2-ben viszont a drivereket akár egyesével is elválaszthatjuk a spooler processztől, így csökkentve a globális problémákat. A kivitelezés rém egyszerű, a képen látható módon a PMC-ben elérhető. Figyelem, az alapértelmezés nem az izolált mód!

[48] Szerintem mindenki tudja, hogy – többek között - mely nyomtatókat gyártó cég készít fantasztikus printereket - borzalmas driverekkel ☺



5.10 ÁBRA AKÁR IZOLÁLHATUNK IS

Location-aware printing

Talán „helyzetérzékeny nyomtatás”-nak fordítható a legjobban ez a szolgáltatás, amit a lehet hogy ismerünk is Windows 7-ből. De az R2-ben az alapértelmezett beállítás is ez, szóval a laptop felhasználók akár minden hálózaton, amelyhez csatlakoznak, más és más printert kaphatnak meg a telepítettekből alapértelmezettnek - és persze teljesen automatikusan.

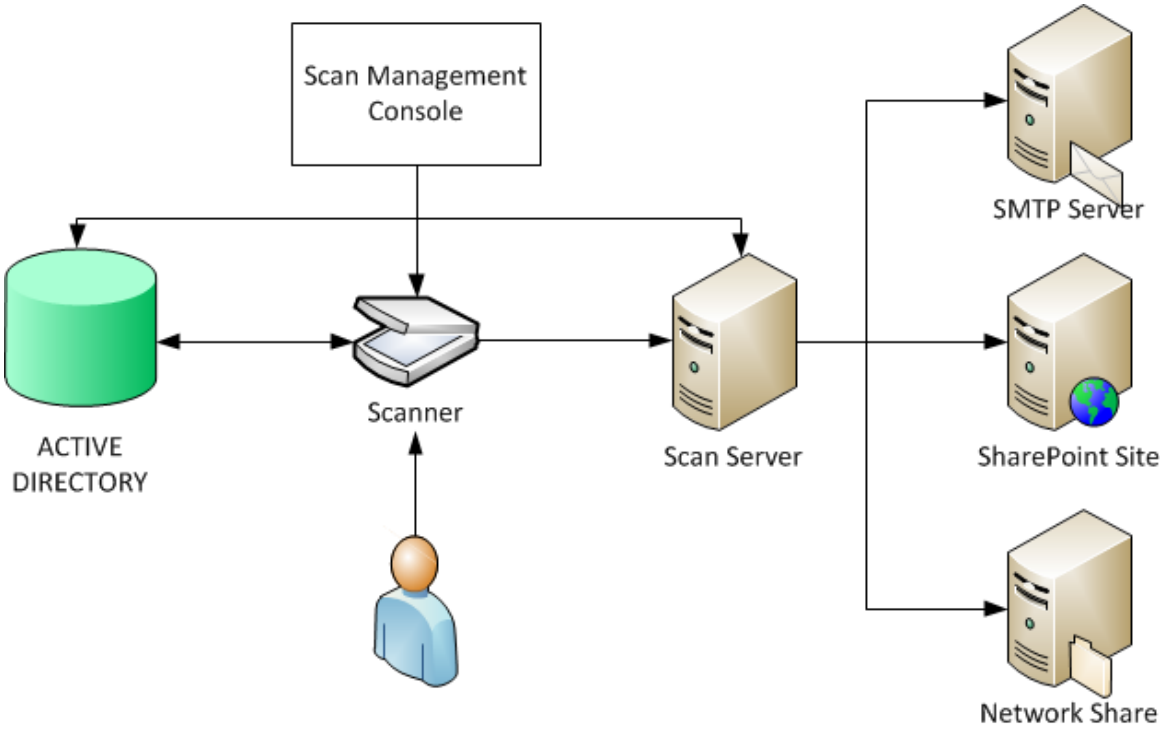
Distributed Scan Server

A végére maradt egy igen érdekes dolog, amelyet őszintén szólva még sohasem próbáltam ki vagy láttam élesben, de biztos nem marad ez így örökre. Azt viszont tudom, hogy a hálózati szkennelés mindig komoly probléma, ha a szkenner (mondjuk egy multifunkciós készülék részeként) nem rendelkezik egy webszerverrel, amelyhez csatlakozva egy böngészőből képesek szkennelni a felhasználók, akkor minden gépre mindenképpen telepíteni kell a gyári szoftvert, ha egyáltalán van (és ha ez a) megoldás a problémára.

A Distributed Scan Server-rel begyűjthetjük a WSD[49] (Web Services on Devices) kompatibilis hálózati szkennereket, így aztán monitorozhatjuk ezen eszközök állapotát, illetve kreálhatunk és felügyelhetünk szkennelési műveleteket is.

A lenti ábrából kiderül, hogy egy szkennelési művelet gyakorlatilag egy szabálycsokor[50], amiből kiderül, hogy hogyan, milyen jellemzőkkel (felbontás, színmélység, fájltípus) történik meg majd a művelet, hova kézbesíti a szerver a végeredményt (hálózati megosztás, e-mail vagy akár egy Sharepoint site, vagy ezek kombinációja), és azt is, hogy kinek vagy milyen csoportnak lesz műveletek végrehajtásához jogosultsága. A felhasználó csak odafárad a kompatibilis szkennerhez, hitelesíti magát pl. egy smartcard-dal, vagy egyszerűbb módon az AD-ba, kiválasztja a megfelelő műveletet és ennyi, persze ha akarja, akár felül is bírálhatja a betáplált műveletek jellemzőit.

[49] Az ilyen eszközök hálózaton keresztül SOAP üzenetekkel operálnak, UDP-t használva, és gyakorlatilag a plug and play élmény olyan, mintha USB-sek lennének.
[50] Post-scan processes (PSP) és az AD tárolja ezeket.



5.11 A NARANCSSÁRGA FEJ LÁTHATÓAN ÉLVEZI AZ ÚJ SZOLGÁLTATÁST

De azért itt is szükségesek bizonyos feltételek:

- A szervernek tartományi tagnak kell lennie
- Erdő szinten is követelmény az R2-es állapot (!)
- Nyilván kell bőven hely a szkennelt anyagok feldolgozásához (ez sok esetben csak átmeneti lesz a feldolgozás idejére, de akkor is)
- Szükség van egy tanúsítványra is a szkenner szerver számára, ami két folyamathoz is kell: egyrészt a szkennertől a szerverig, másrészt a kliensektől a szerverig, merthogy a Windows 7-ből is használható szoftveres eléréssel ez a komponens (a *Scan Management* alkalmazás ugyanis telepíthető a Turn Windows Features On or Off segítségével).

5.2 DHCP ÉS DNS

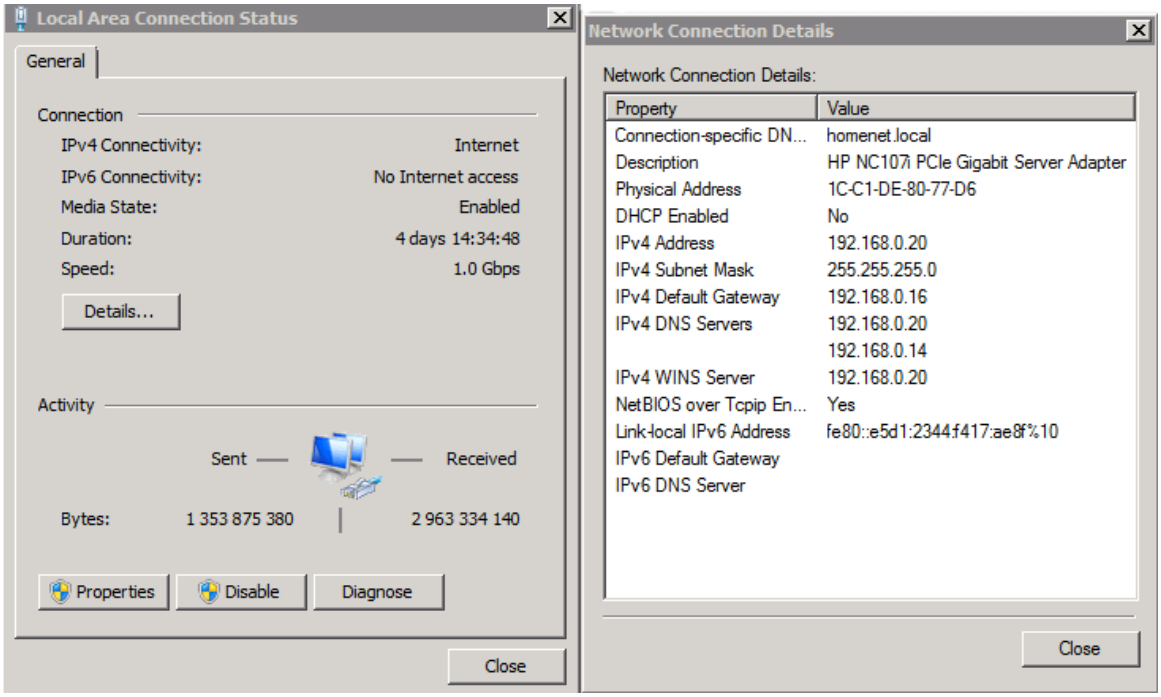
Mindkettő alapszolgáltatás, így mindkettő hétköznapi használatú, de persze méretes környezetben azért rendesen el is lehet merülni mindkettőben, így aztán mondjuk inkább azt, hogy hétköznapi *is*.

> Ide tartozhatna még a WINS is, de igazából ezzel kapcsolatban annyira nincs újdonság, hogy bele sem került a címbe. Illetve az az újdonság, hogy ha még mindig vannak (lesznek) régi OS-eink és alkalmazásaink[51], akkor még mindig

[51] Illetve vegyes hálózatban Samba klienseink, szervereink. Ilyenkor külön élvezhetjük az időnként felbukkanó WINS inkonzisztenciákat, illetve az idegölő törlési algoritmusokat (a lektor megjegyzése).

nem radírozhatjuk ki a WINS-t, de nem is kell, alig eszik valamit, és dolgozik rendesen.

Kezdésként beszéljünk e fejezet kapcsán egy mélyebben történt változásról is, az új TCP/IP stack-ről (*Next Generation TCP/IP stack*), amely egy alapos bővítésen esett át architekturális, biztonsági és hardver támogatási szempontból is. A Windows Server 2008 teljesen újraírt hálózati verme a jelenleg elterjedt IPv4-en kívül már natívan támogatta a TCP/IP6-os verzióját (IPv6) is. A 128-bites (16-bájtos) címekkel operáló IPv6 protokoll bevezetésére főként azért volt szükség, mert a világszerte működő gépek számának izmos növekedése miatt napjainkban egész egyszerűen elkezdtünk kifogyni, sőt gyakorlatilag kifogytunk a kiosztható IP-címekből. Emellett az IPv6 lehetőséget adott a TCP/IP-protokollal kapcsolatos néhány technológiai alapelv újragondolására is.



5.12 A DUAL STACK

Az IPv6 jóval tágabb címtartományok létrehozását teszi lehetővé, valamint a jelenlegi megoldásoknál könnyebben konfigurálható, gyorsabb és biztonságosabb adatátvitelt tesz lehetővé. A Vistától és a Windows Server 2008-tól kezdve a korábbi két egymástól teljesen független protokoll-vermet (tcpip.sys és tcpip6.sys) egy úgynevezett Dual IP architektúra váltja fel, így a rendszer az IPv4 és IPv6-os hálózatokat külön-külön, de mégis egyszerre tudja kezelni. Ennek köszönhetően a Windows egy időben kétfajta IP-címmel is rendelkezhet, egy 4-es, illetve egy 6-os verziójúval. A Vista Dual IP architektúrája egy hálózati vermen belül kezel mindent, így továbbra is egy szállítási rétegre (TCP, UDP) és egy adatkapcsolati rétegre van szükség.

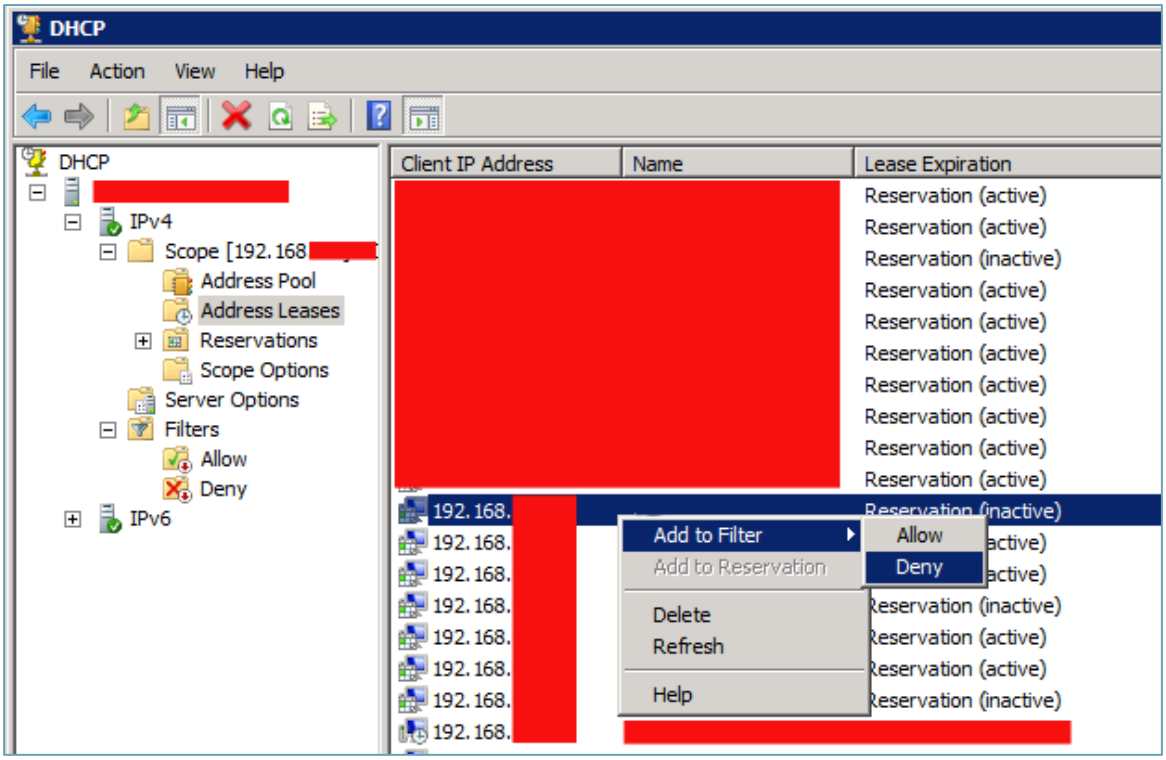
Az IPv6 kezelése teljes IPSec támogatást is nyújt, így az új formátumú címekkel is használhatjuk a nyílt szabványokból álló kriptográfiai keretrendszert. Az IPv6 mindezeken kívül elérhető PPP (Point-to-Point Protocol) kapcsolatok esetén is (kivéve PPTP VPN használatakor), és az IPv6 természetesen támogatja az automatikus címkiosztást is, mind dedikált DHCP-kiszolgálóval, mind anélkül. Alapértelmezés szerint mind az IPv4, mind az IPv6 protokoll települ, valamint mindkettő beállításai elérhetők a grafikus felületről is. Ha esetleg szkriptekkel automatizált konfigurációra van szükségünk, természetesen a parancssoron keresztül is megváltoztathatjuk a protokollok összes paraméterét – erre kiválóan alkalmas az egyébként is svájci bicska „netsh" parancs[52].

Az új stack rengeteg egyéb képességet ad a kezünkbe, például olyan új megoldásokat, mint a „Receive Window Auto-Tuning", a „Compound TCP" vagy az ECN (Explicit Congestion Notification) támogatás. De fontos a hálózati beállítások újraindítási kényszerének eltörlése, a számos diagnosztikai és nyomkövetési lehetőség, illetve az új (és főként szerveroldali) hálózati interfészekkel kompatibilis szolgáltatások alkalmazása (RSS, NetDMA, TCP Chimney Offload, stb.). Illetve emlékezzünk meg a szintén a Vista/Windows Server 2008 párosban debütáló Windows Filtering Platform-ról, ami gyakorlatilag egy új architektúra az új generációs TCP/IP veremben, és amely egy API gyűjtemény fejlesztők számára, így programozók a saját alkalmazásaikban (pl. tűzfalak, AV és diagnosztikai szoftverek) is használhatnak, de a Windows Server 2008 tűzfala és az IPSec is ezt használja.

Visszatérve a címben említett komponensekre és így a lényegre, a DHCP és a DNS egy közös új tulajdonsága az előzőek fényében teljesen logikus IPv6 támogatás, ami teljesen egyenértékű (pl. a parancssori eszközöknél is) az IPv4 támogatás szintjével. Ezek után először essünk át a DHCP újdonságain, és igazából a Windows Server 2008-at kihagyva, egyből az R2-re[53] ugorva:

- DHCP Name Protection (a DNS-sel együttműködve az ún. "name squatting" (azaz egy vegyes hálózatban egy nem Windows-os gép regisztrálása egy létező azonos nevű Windows-os gép nevére) probléma kiküszöbölése
- Delay configuration (a másodlagos DHCP szerverek reagálási intervallumának késleltetése)
- Deny, Allow filterek használata (a kliensek DHCP szolgáltatásból kizárása, illetve engedélyezése, a MAC cím alapján, a címre kattintva, a helyi menüből)

[52] Az IPv6-os konfigurációs lehetőségek bővebb ismertetéséhez használjuk a „netsh interface ipv6 /?" parancsot.
[53] Persze, a kliens oldalon a Windows 7 is tartalmazza ezen újdonságok támogatását.



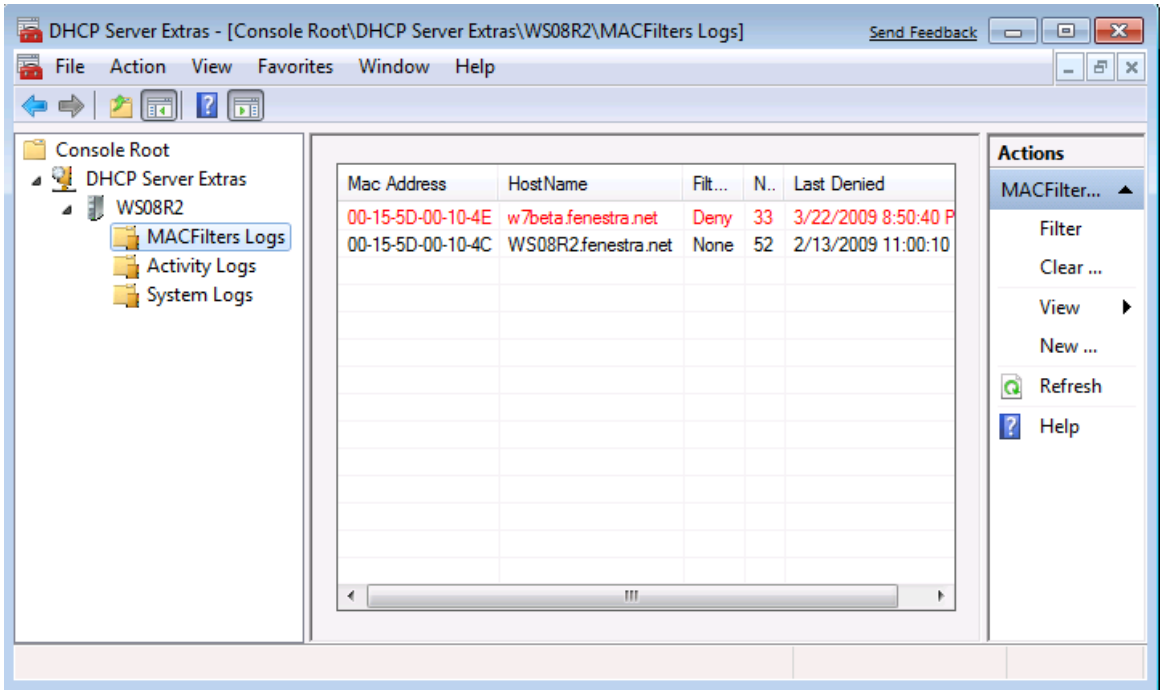
5.13 A PACÁK KÖZÖTT AZÉRT LÁTSZIK A LÉNYEG: A TILTÁS EGYSZERŰ

- Egyszerű rezerváció konfigurálás - két egérkattintással
- Egy speciális eszköz[54], a DHCP Server Events Tool, amely a DHCP adminoknak segít, elsősorban azoknak az eseményeknek a nyomon követése válik lehetővé ezzel az MMC-vel, amelyek egyébként is újdonságok az R2-ben. Lényeges az is, hogy ez az eszköz - egy rendes MMC bővítményhez hasonlóan - képes távoli DHCP szerverekhez is kapcsolódni[55], illetve többhöz is, plusz a képen is látható bal oldali keretben lévő kategóriák egy-egy bejegyzése másolható és szűrhető.
- Néhány új DHCP opció támogatása, főképp IPv6-osok, pl. az Option 15 (User Class), vagy az Option 32 (Information Refresh Time)

A DHCP Server szolgáltatásfiókja is változott a LocalService-ről a Network Service-re, így a veszélyes privilégiumok száma is csökkent. További részleteket rengeteg helyen találunk a „hardening services" kulcsszavakra, ami a Vistában kezdődő drasztikus rendszerszolgáltatás változásokra utal.

[54] Letöltés és telepítési információ: http://blogs.technet.com/b/teamdhcp/archive/2009/03/20/tool-to-read-dhcp-server-events-for-windows-server-2008-r2.aspx

[55] Feltéve ha adminok, vagy legalább a Event Log Readers csoport tagjai vagyunk.



5.14 EGY EXTRA MMC

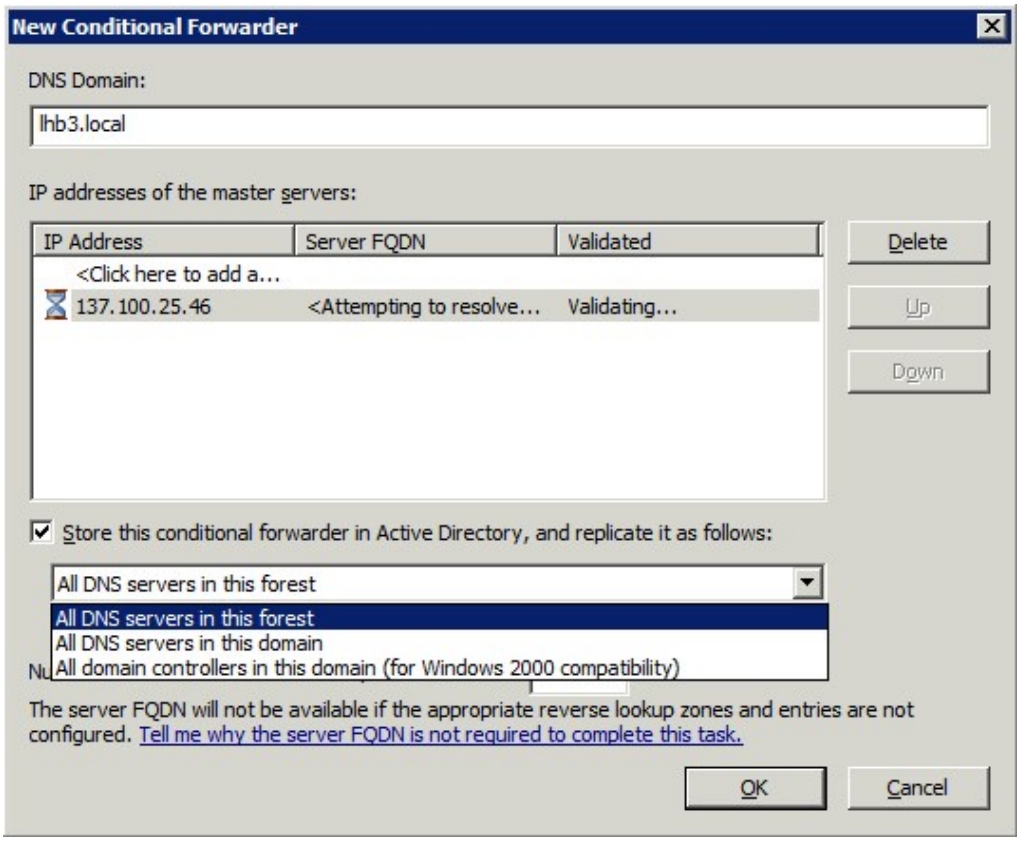
Két szerver oldali változást említenék meg a DNS témakörben. Elsőként a zónák háttérben történő betöltése fontos előrelépés, ami talán eldönti „...a fájlban vagy az AD-ban tartsuk a DNS zónákat" című vitát is, ti. az előbbi esetében ez az új lehetőség nem áll rendelkezésre. Ha viszont a címtárban tartjuk a zónáinkat, akkor a Windows 2008 és az R2 képes lesz ezeket egy DNS restart után a háttérben, szeparált szakaszokban, aszinkron módban betölteni, és így az eddigiekkel szemben képes lesz a folyamat közben is válaszolni a beérkező névfeloldási kérésekre, azaz nem bicsaklik bele egy esetlegesen nagyméretű zóna egyszerre - ezért aztán lassan történő - betöltésébe se. Sőt, ha olyan kérés/regisztráció érkezik, amely egy olyan zónára vonatkozik, ami még nincs a memóriában, akkor a kliens óhaja magasabb prioritást kap, és a DNS szerver kiszolgálja a kérést. De jelzem újra: ez csak a címtárban tartott DNS zónákra igaz, a fájlban tartott zónáknál marad a szekvenciális feldolgozás.

Egy másik szerveroldali újdonság a feltételes továbbítók újszerű használata. A DNS MMC-ben, a faszerkezetben a zónatípusok között egy új mappát láthatunk, „Conditional Forwarders" néven. Itt kell felvennünk a különböző továbbítókat (a megszokott helyen is lehet persze), és a felvétel után ezeket a jobb oldali keretben látható listában rögtön láthatjuk is.

Ennél talán fontosabb viszont az, hogy AD integrált zóna esetén lehetőségünk van a címtárban tárolni, és ebből következően replikálni is a továbbítókkal kapcsolatos adatokat [56] . A replikáció többféle szcenárióban is működhet, azaz minden

[56] Ránézésre nem tűnik nagy kalandnak, de huszonsok tartományvezérlő - és DNS szerver - esetén kifejezetten áldás (a lektor megjegyzése).

tartományvezérlő DNS szerverre (amely legalább Windows Server 2003), vagy például minden DC-re a tartományban.



5.15 FELTÉTELES TOVÁBBÍTÓ

Fontos még a RODC-k apropóján a read-only DNS opció is, ami gyakorlatilag egy elsődleges típusú zóna, névfeloldásra tökéletesen alkalmas, és rekordszinten frissít, ha szükséges, de csak „fentről". Mindent replikál (alkalmazáspartíciók, domainDNSZones, ForestDNSZones, stb.), de a telephelyről semmiképpen nem írható példány.

Még egy érdekes újdonságról számolnék be, ez pedig a WINS-hez hasonló (de azt azért nem teljesen helyettesítő) megoldás, a speciális „*GlobalNames*" zóna, ami egy AD integrált zóna lesz. Ha egy zónát ezzel a névvel hozunk létre a DNS-ben, akkor úgy lehetnek a statikus, globális rekordoknak NetBIOS nevei, hogy a WINS-t nem is telepítjük. De vegyük figyelembe, hogy ezzel csak azokat a tipikusan fontos gépeinket (a szervereket) jelöljük, amelyek már rendelkeznek fix IP-címekkel, tehát szó sincs dinamikus regisztrációról, és szó sincs méretezésről, főleg egy nagyobb, összetett hálózatban. [57]
Fontos tudni azt is, hogy amíg nem engedélyezzük az összes mérvadó DNS szerveren, addig nem használható ez a zóna. Az engedélyezés parancsa:

[57] Ezt jól jegyezzék meg a vizsgákra készülők (a lektor megjegyzése)!

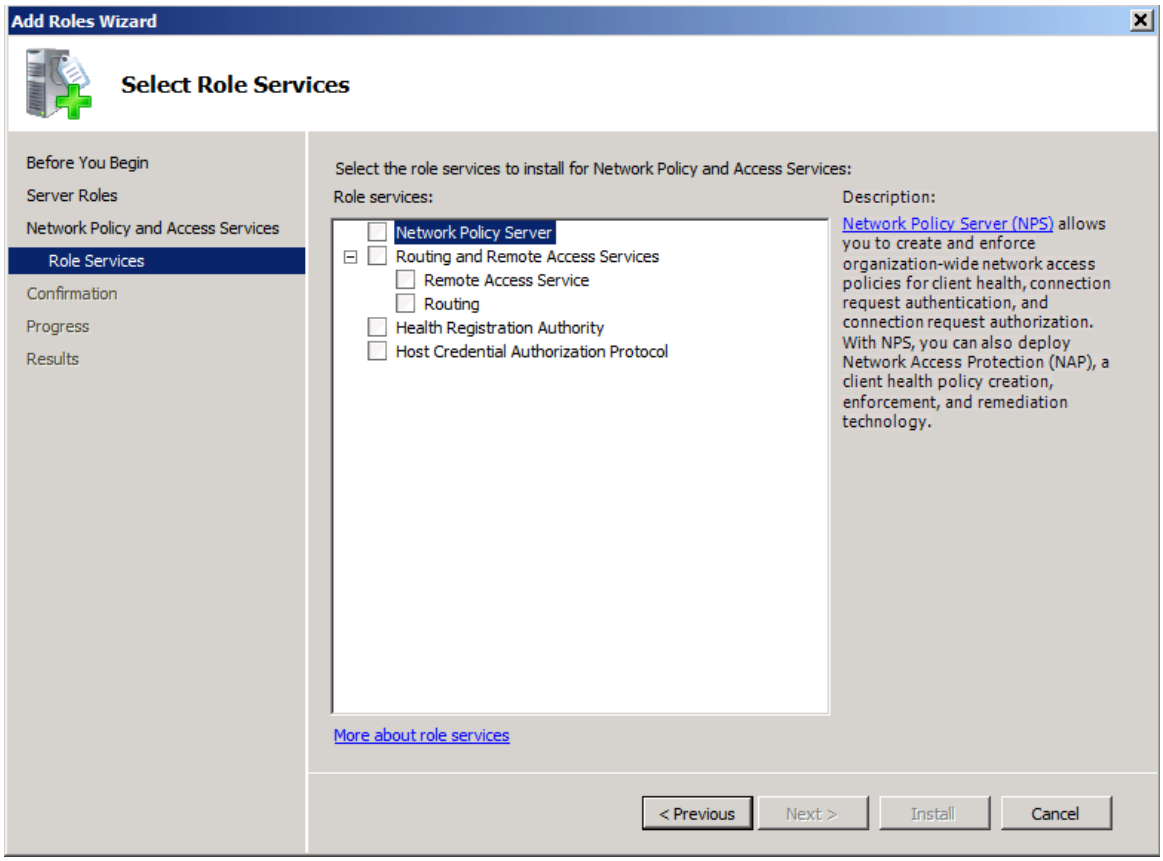
dnscmd <ServerName> /config /enableglobalnamessupport 1

Ezek után ahhoz, hogy az erdőben lévő összes DNS-kiszolgáló és ügyfél számára elérhető legyen ez a zóna, replikáljuk le az erdő minden tartományvezérlőjére, vagyis adjuk hozzá a GlobalNames zónát az erdőszintű DNS-alkalmazáspartícióhoz.

5.3 NPAS

Nagy bátorságnak tűnhet egy alfejezetben beszélni a Windows Server 2008-ban megjelent Network and Access Policy Server-ről, de már most jelzem, hogy a legnagyobb és *legrobusztusabb* rész, a Network Access Protection (NAP) szerkezetileg ebben a fércműben kissé később jön, ezért ide, az alapszolgáltatásokhoz csak a „maradék” kerül.

Ez se kevés azért, mivel az NPAS igen komoly méretű gyűjtő lett, méghozzá a NAP és a NAP-hoz szükséges részszolgáltatások mellett a komplett RRAS (Routing and Remote Access Services, azaz pl. a VPN és a DUN szerverek + a route-olás), pl. a Network Policy Server (az elérési és hozzáférési házirendek) és a korábbi IAS (Internet Authentication Services, azaz a Microsoft RADIUS teljesen RFC kompatibilis kiszolgálója) is ide került.

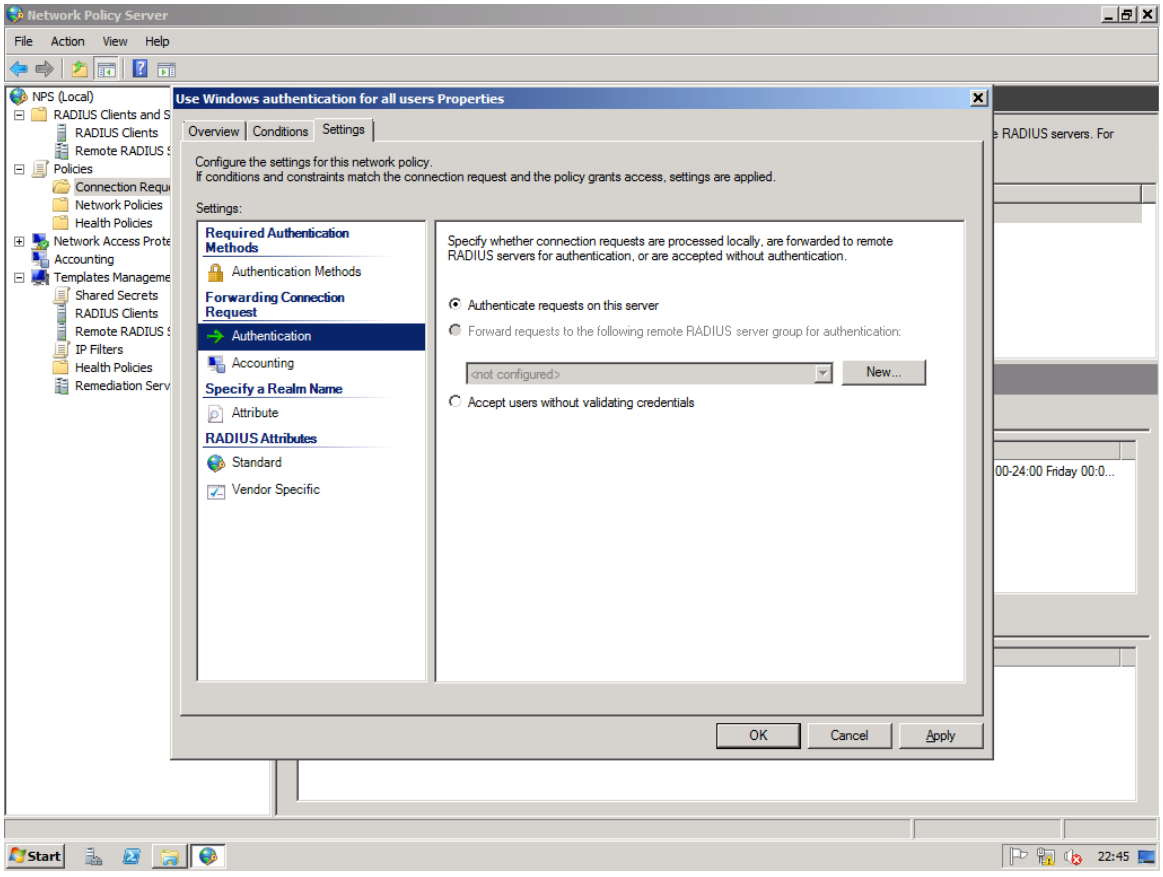


5.16 MINT A JÓ BOLTBAN...

5.3.1 Az NPS

Haladjunk akkor szépen sorban, kezdjük az NPS-sel, azaz a speciális házirend kiszolgálónkkal (gyakorlatilag semmi köze a Csoportházirendhez). Több fontos szerepe is van ennek a komponensnek, multifunkciósan használjuk, minimum három célra:

1. RADIUS (Remote Authentication Dial-In User Service) kiszolgálóként központi hitelesítést, engedélyezést és nyilvántartást (accounting) végez a vezeték nélküli, vezetékes, VPN és DUN kapcsolatok esetében. Ha az NPS-t RADIUS kiszolgálóként használjuk, akkor a hálózati elérést megvalósító kiszolgálókat (például Access Point-ok, VPN szerverek vagy akár egy Forefront TMG) RADIUS ügyfélként konfigurálhatjuk az NPS-ben. Ezenkívül beállíthatjuk azokat a hálózati házirendeket is, amelyeket a hálózati házirend-kiszolgáló a csatlakozási kérelmek engedélyezésére használ.
2. RADIUS proxy: Ha az NPS-t RADIUS proxyként szeretnénk használni, akkor a kapcsolatkérelmek házirendjén (Connection Request Policy) keresztül kell beállítani, hogy az NPS mely kapcsolatkérelmeket (és hova) továbbítsa más RADIUS kiszolgálóknak. Gyakorlatilag egy köztes elemként működik ilyenkor.
3. Network Access Protection (NAP) policy server: később kitárgyaljuk.



5.17 HITELESÍTÉS TOVÁBBÍTÁS EGY HÁZIRENDBEN

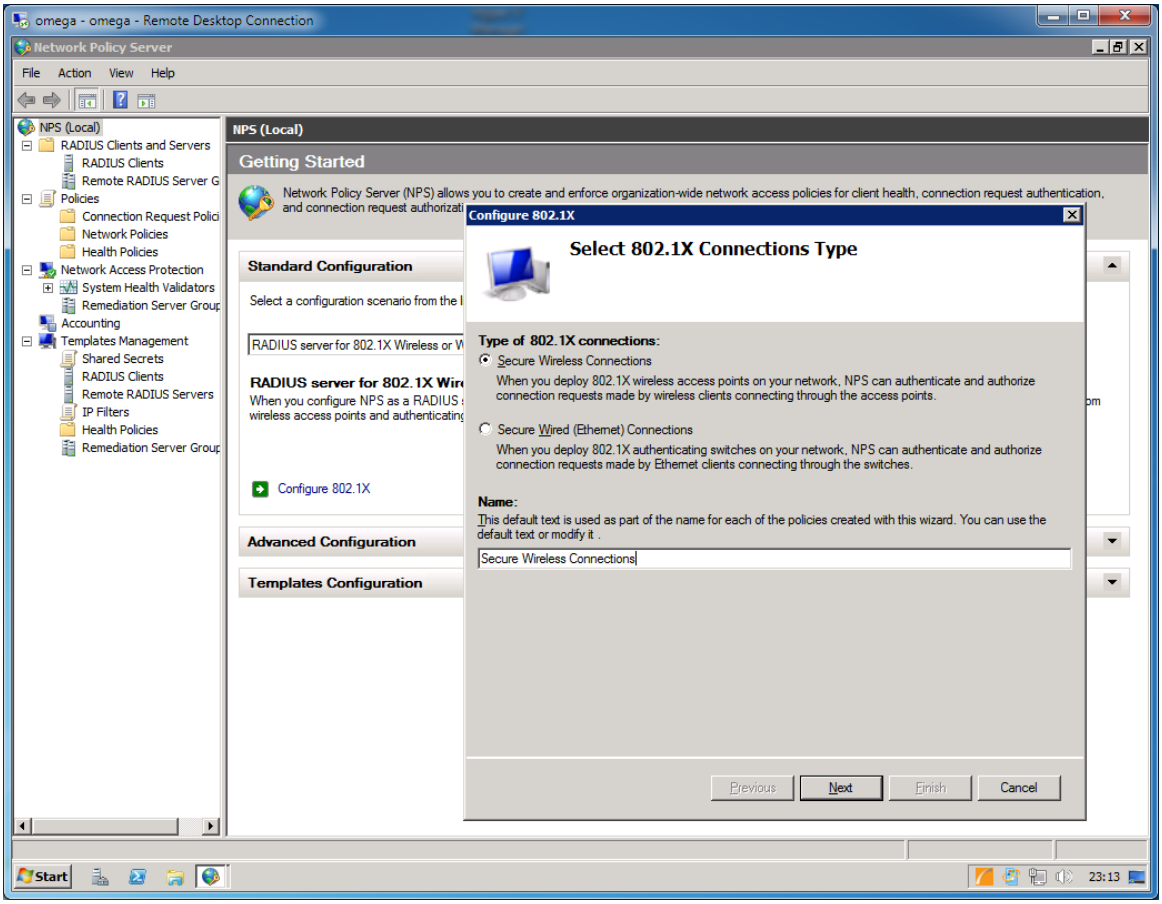
Ez így eléggé fárasztónak tűnik, de nézzünk meg egy gyakorlati példát: a feladat az lesz, hogy a szanaszét szórt Access Point-jainkon keresztül belépő laptopok RADIUS-szal kapcsolódjanak a tartományba, meghatározott feltételek mentén, konkrétan kizárólag a „Wireless Users" AD csoport tagjai tudják használni a vezeték nélküli hálózatunkat (persze bármelyik AP-n keresztül a cégünknél) a saját tartományi felhasználónevükkel és jelszavukkal belépve.

Az előfeltételek:

- A csatlakozó laptopokat be kell léptetni a tartományba
- Némi csoport konfigurálásra is szükség lesz a címtárban, illetve ha okosan és persze központilag akarjuk megoldani a kliensek beállítását, akkor a Csoportházirendet is használnunk kell
- Szükséges az AD Certificate Services, az NPS-t igazoló tanúsítvány használatához, és persze a kliensnek el kell fogadnia hitelesként ennek a tanúsítványnak a kiadóját[58]
- És persze az NPS-t is telepíteni kell (5.16 ábra).

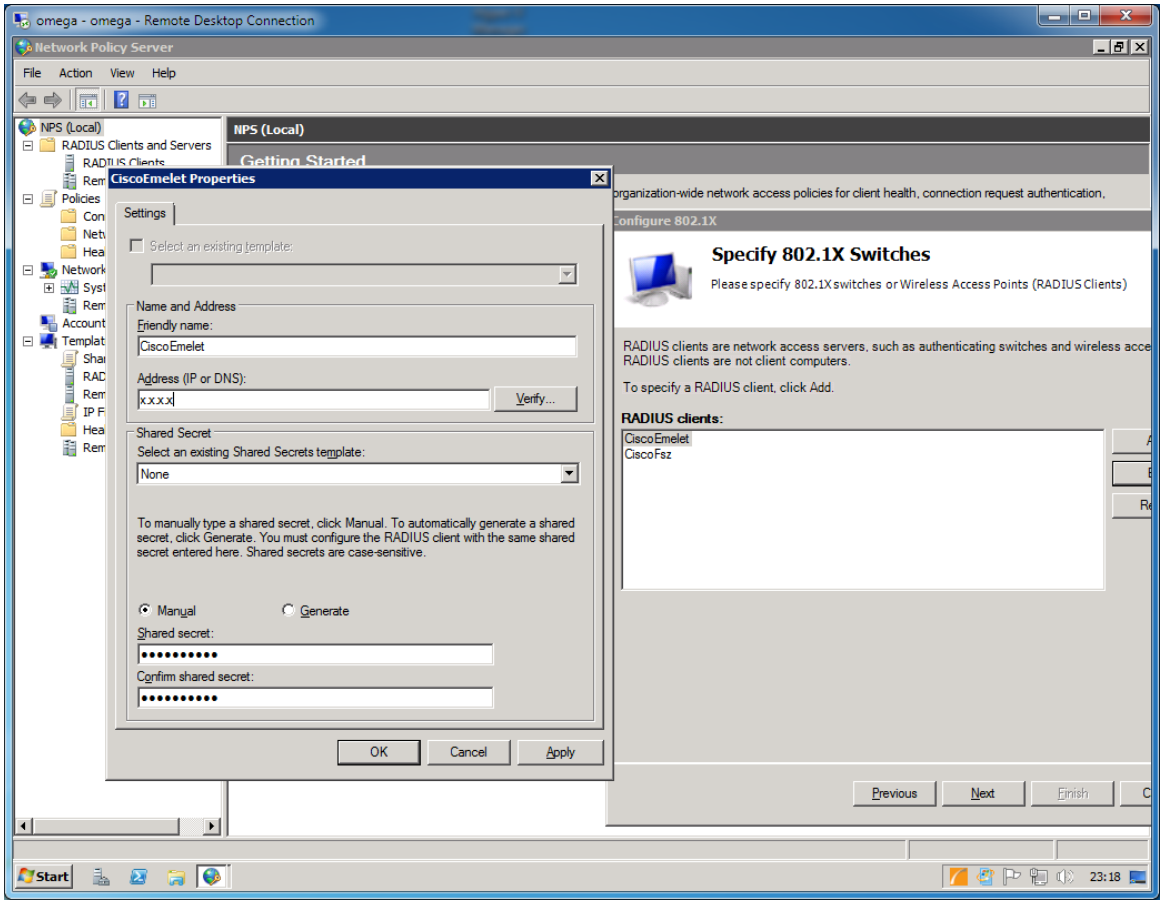
1. Ha van már NPS, akkor indítsuk el, majd a „Getting Started" oldalon válasszuk a „RADIUS server for 802.1x Wireless or Wired Connection" menüpontot.
2. A következő panelen értelemszerűen válasszuk a „Secure Wireless Connections" pontot!

[58] Ez a tartományba tartozó gépek esetén nem lesz probléma, ha például saját PKI infrastruktúrával rendelkezünk.



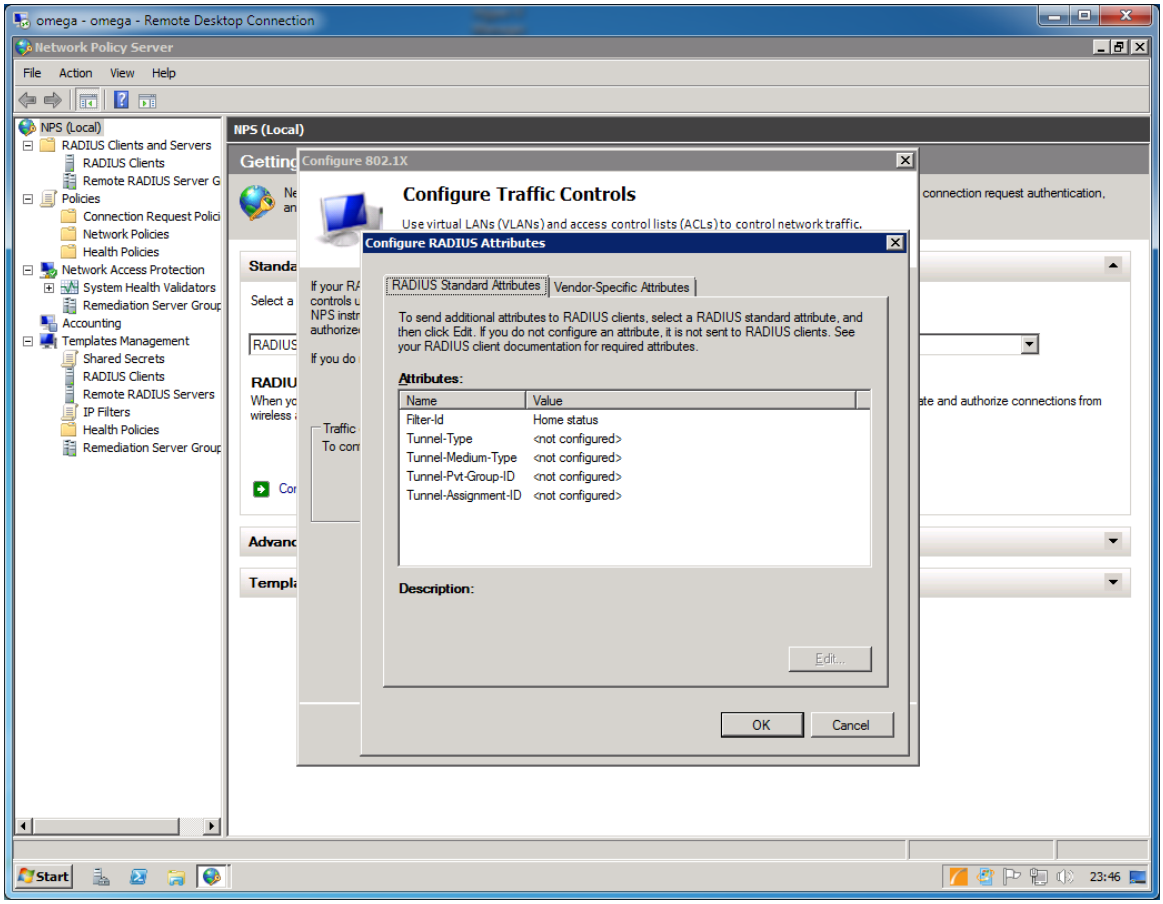
5.18 ÁBRA MINT LÁTHATÓ, A VEZETÉKES KAPCSOLATOKRA IS RÁHÚZHATÓ EZ A MÓDSZER

3. Ezután adjuk meg a RADIUS klienseinket, amelyek jelen esetben az AP-k lesznek, mivel ezeken keresztül csatlakoznak a laptopok majd a hálózathoz. DNS név vagy IP cím kell, ha több is van, akkor később mindet vegyük fel! Persze ezeket az AP-kat is konfigurálni kell majd, hiszen tudniuk kell, hogy ki az Úr, azaz ki a RADIUS szerver a hálózatban, és azt is, hogy mi a megosztott jelszó.



5.19 ÁBRA KÉT AP-M IS VAN

4. Most jön a hitelesítési metódus, tipikusan ebben az esetben a PEAP-ot (Protected EAP) fogjuk választani, bár lehetne pl. a smartcard is egy opció, ha rendelkezünk ilyen infrastruktúrával. Viszont bármit is választunk konfigurálni kell, például a PEAP-nál az NPS szerver tanúsítványát kell megadni, az EAP típust, illetve választhatunk olyan lehetőségeket, mint az „Enable Fast Reconnect”.
5. Most jön azon felhasználók kiválasztása, akik ilyetén módon kapcsolódhatnak, tipikusan csoportok formájában tesszük meg ezt, pl. „Wireless Users”. De az is elképzelhető, hogy gépeket vagy gépcsoportokat szeretnénk itt megadni mint a hitelesítés alanyait, így adott esetben a „Domain Computers” csoportot.
6. Itt akár vége is lehetne a mulatságnak, de ha óhajtjuk, akkor tovább szűrhetünk, de csak akkor, ha az AP-k támogatják az adott RADIUS attribútum használatát, pl. a képen a „Home status” a Filter-Id attribútumon keresztül majd a „Domain Users” lesz.
7. Ezután jön a szumma képernyő, és az NPS konfigurálással készen is vagyunk.



5.20 ÁBRA TOVÁBBI SZŰRÉS, DE CSAK ÓVATOSAN, AZ AP MEGKÖTHETI A KEZÜNKET

Persze a teljes folyamathoz még hozzátartozik a kliens operációs rendszer WLAN kapcsolatának beállítása (amihez például a Csoportházirendet kiválóan alkalmazhatjuk) Vista és Windows 7 esetén. Illetve feladat még az AP-k megfelelő konfigurálása is, de mi most csak a szerver oldallal foglakoztunk egy tipikus esetet figyelembe véve.

5.3.2 Az RRAS

Ha visszanézünk az 5.16-os ábrára, akkor a következő két komponens a már jól ismert RRAS-hoz tartozik. Igazából az itt is megjelenő IPv6 kompatibilitáson kívül az RRAS-ban sok újdonság nincs, azért a két[59] új VPN típusról azért emlékezzünk meg.

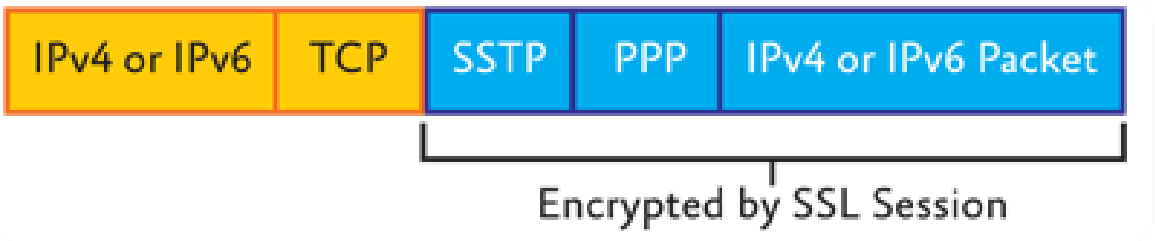
Secure Socket Tunneling Protocol (SSTP)

Sokan lesznek, akik azt mondják majd, miután beüzemelték ezt a szolgáltatást: - Na végre! Ezzel nem a művelet hosszúságára, hanem inkább e komponens szükségességére gondoltunk. Mert az SSTP olyan lehetőség, ami jól beleillik abba a tendenciába, amely alapján – ez személyes vélemény - pár generáció múlva csak a HTTP/S protokollokat kell majd kinyitni a tűzfalakban. Na de leplezzük le végre: az

[59] Egy, azaz az első érkezett a Windows Server 2008-ban, és a következő pedig az R2-ben.

SSTP-vel a hagyományos VPN kapcsolatok helyett/mellett HTTPS-en keresztül is képesek leszünk teljes értékű VPN kapcsolatokat kezdeményezni.

> A tendencia tényleg a HTTP/S-be bújtatás, efelé sodródnak a különböző szolgáltatások, és erről a TMG könyvben is számos bizonyítékot hoztam fel.
> A kapun túl - Forefront Threat Management Gateway 2010"
> https://technetklub.hu/content/TMGKonyv.aspx



5.21 ÁBRA SZOKVÁNYOS SSL CSOMAGKÉNT LÁTSZIK (A KÜLSŐ IP ÉS A TCP HEADER TITKOSÍTATLAN)

Legalább három fő érvet tudunk felsorakoztatni a VPN over HTTPS (illetve inkább az SSL VPN elnevezés a hivatalos) mellett a hagyományos típusokkal szemben:

- A speciális VPN portokat nem tudjuk, nem lehetséges minden körülmények között használni, egyszerűen egy sereg helyen (pl. szállodákban, publikus helyeken vagy más cégek hálózatában) tiltják.
- Bármelyik hagyományos VPN típust nézzük, a tunnelt a legtöbb esetben „át kell vezetni" egy NAT szerveren. Ez van mikor kisebb, van viszont, hogy nagyobb (L2TP) problémát is okozhat.
- A VPN kapcsolatok tipikusan egy „végpont egy csomópont" típusúak. Ha a két helyszín LAN IP tartománya megegyezik, és közöttük NAT-ot alkalmazunk, akkor szintén konfliktus lehet.

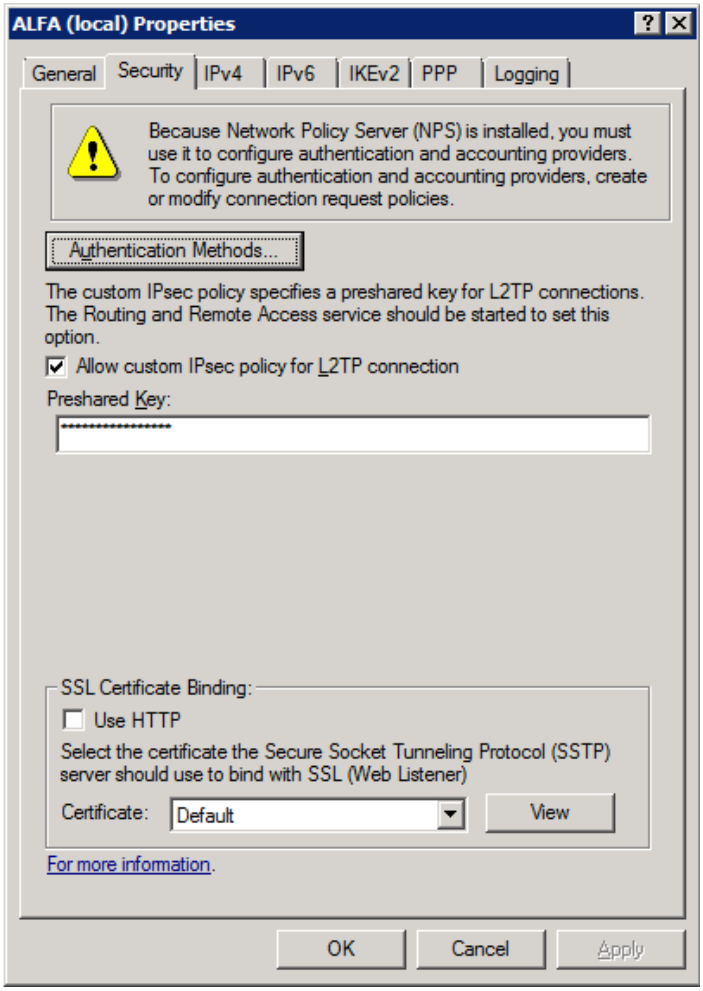
Persze, az utóbbi két problémára léteznek ajánlott és működő megoldások, de könnyen beláthatjuk, hogy egyetlen portot kinyitva, a NAT és más hálózati nehézségek nélkül egyszerűbb lenne működtetni egy VPN infrastruktúrát.

Az SSTP viszont egy az alkalmazási rétegben működő protokoll, tipikusan két program közötti kommunikációra felkészítve, viszont egy hálózati kapcsolaton belül akár többre is (gyakorlatilag a teljes hálózatban), ergo jobban képes kihasználni a sávszélességet. Az SSTP ugyanazon SSL háttérre támaszkodik, mint pl. az L2TP/IPSec (egymás mellet mindhárom típus jól elfér) és ugyanúgy a TCP 443-as portot használja, de tudnunk kell, hogy úgy, ahogy az L2TP IPSec nélkül, az SSTP SSL nélkül sem más, mint egy kicsit különlegesebb tunneling protokoll. Hátránya közé tartozik még az is, hogy a Site-to-Site kapcsolatokban nem vehetjük majd használt.

Mielőtt azonban leírnánk végleg, egy-két további pozitív tulajdonságát is tekintsük át:

- Nincs szükség külön kliensre, és nincs szükség például extra IP címekre.

- Teljesen transzparens a felhasználó számára, és nem kell speciális útválasztást illetve metrikát sem használnunk. Nem számítanak akadálynak a kapcsolat két pontja között működő routerek, tűzfalak, web proxy-k és NAT szerverek. Nem függ a kapcsolat olyan extra protokolloktól, mint a PPTP GRE vagy az L2TP ESP.
- Kompatibilis az IPv6-tal, a NAP-pal, az RRAS-sal, akár a multifaktoros azonosítással is.
- Az alkalmazási rétegbeli működés miatt majd igazán kényelmesen szűrhetjük a forgalmat egy olyan tűzfallal, amely erre képes (pl. ISA Server 2004/2006, Forefront TMG), persze ehhez a speciális, ún. SSL Bridging módszerrel kell majd kipublikálnunk.



5.22 ÁBRA AZ EGYETLEN R2-ES VÁLTOZÁS AZ, HOGY VÁLASZTHATUNK TANÚSÍTVÁNYT

Az SSTP-t tehát a Windows Server 2008 már tartalmazza (kliens oldalon viszont először a Vista SP1-ben használhattuk), de alapértelmezés szerint nincs élesítve. Igazából nem kell semmi extrára gondolnunk, az RRAS-ban a szokásos módon összehozunk egy VPN szervert, beállítjuk a portok számát (alapértelmezés szerint 128 van), az NPS-ben lehetőséget adunk a VPN „tárcsázás” jogára (Connections to

MS RRAS házirend > Network Policies > Access Permission), és tulajdonképpen készen is vagyunk.

Illetve majdnem, mert ami viszont fontos, az az, hogy még az RRAS indítása előtt rendelkeznünk kell megfelelő kiszolgáló tanúsítvánnyal, hiszen az SSTP HTTPS listener-éhez ez alapfeltétel. És még egy, még ennél is kritikusabb pont: a tanúsítványkiadó visszavonási listáját (CRL) is el kell érnünk majd a távoli kliensről, tehát pl. a tűzfalunkban ki kell publikálni a root CA többnyire a 80-as porton elérhető CRL listáját [60] . Persze, ha publikus, külső tanúsítványkiadótól származó a tanúsítványunk, akkor ez az Ő gondjuk lesz, és persze ebben az esetben biztosan működni is fog.

IKEv2

Ez a megoldás nagyon különleges, de csak a Windows7/R2 páros esetén használható. A Microsoft implementációjában „VPN Reconnect" néven is fut. De jöjjön egy idézet a kedvenc TCP/IP könyvünkből (Petrényi József - TCP/IP alapok, 2. kötet, V1.0[61]):

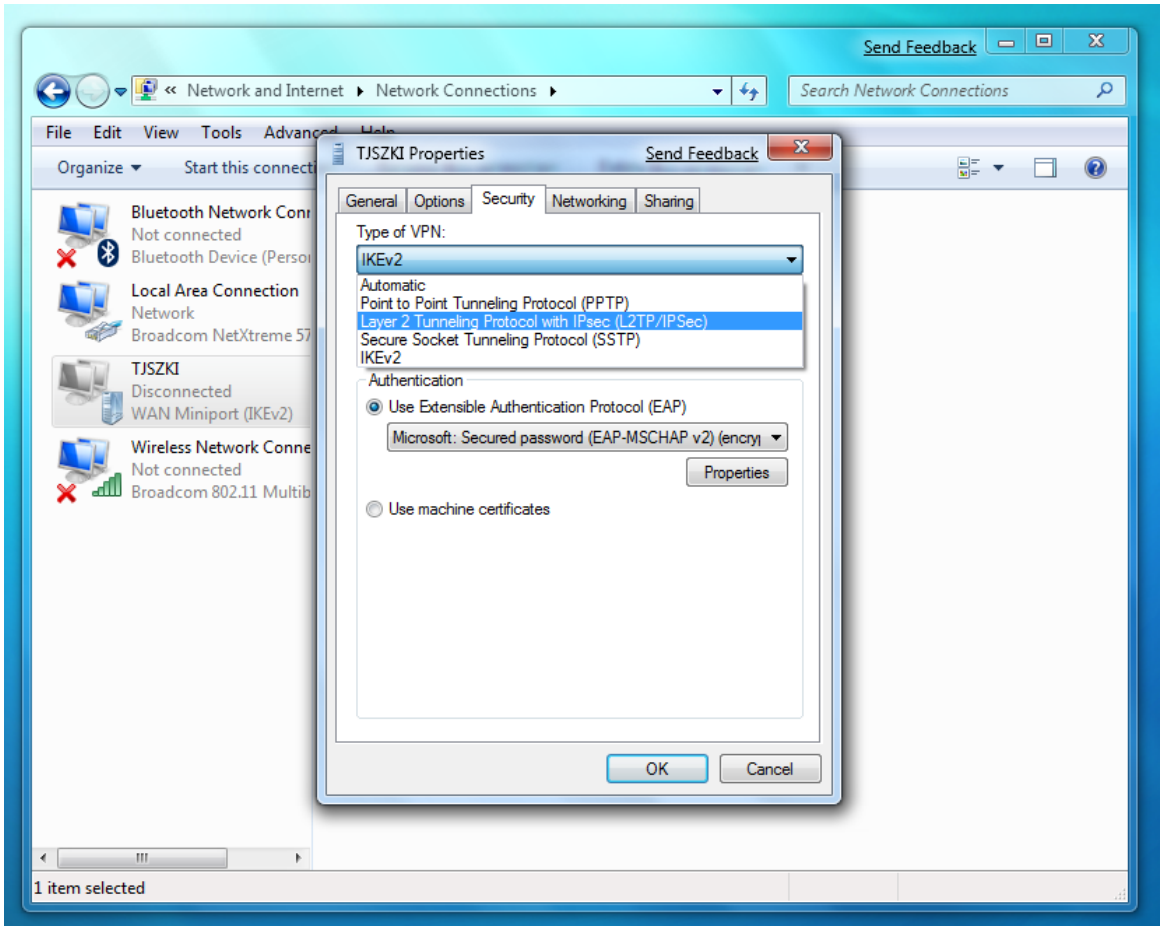
> Érdekes játék ez a security. Időnként olyan, mint egy nagy doboz Lego: előveszem a darabokat, és ha így rakom össze, akkor kávédaráló, ha másképpen, akkor meg tank lesz belőle.
> A VPN Reconnect is ilyen legós-összedugdosós VPN protokoll. Megfogtuk az L2TP/IPSec modellt, leszedtük róla az L2TP kockát, félretettük az UDP kockát, a megmaradt IPSec blokkban meg kicseréltük az IKE SA-t IKEv2-re. Ami keletkezett, azt elneveztük VPN Reconnect-nek.
>
> Most az egyszer az átnevezésnek tényleg volt értelme is. Ha emlékszünk, írtam, hogy az IKEv2-höz kijött később egy kiegészítés MOBIKE néven. Nos, ez pont a mobil kliensek kiszolgálására hivatott. Azaz olyan kliensekére, akik nagy sebességgel mozognak, miközben tolják az iwiw-et, VPN-en keresztül belépve a céges hálózatukba. Aztán ha mozgás közben megszakad a kapcsolatuk, átváltanak egy másik cellára - és borzasztóan nem szeretnék, ha erről bármilyen módon is tudomást szereznének. Azaz a VPN legyen olyan kedves, oldja meg az újracsatlakozást magától. Csak hogy ne legyen egyszerű az élet, MS berkekben a VPN Reconnect és az IKEv2 teljesen szinonim kifejezések. De mi tudjunk róla, hogy az egyik egy VPN protokoll, a másik pedig egy SA!

[60] Vagy haladunk a korral és OCSP-t használunk: http://forum.jvangent.nl/blog/?p=31 (a lektor megjegyzése).

[61] http://www.microsoft.com/hun/technet/article/?id=3effd5d3-139c-471a-adeb-a71a6885562f

Néhány további jellemző és előny, most már csak egy felsorolás formájában:

- Az IKEv2 egy IPSec tunnel módra épülő megoldás
- Az „IKEv2 Mobility and Multihoming Protocol” (MOBIKE) használatával variálja a VPN kapcsolat felhasználó oldali végpontját
- „Dormant” mód: szakadás esetén vár és vár, mindaddig vár, míg újra lesz kapcsolat az RRAS-sal
- Gyorsabban működik és gyorsabban visszaáll mint a többi típus
- Képes IPv4-ről IPv6-ra váltani és vissza
- Az automatikus NAT-T lehetőség is rendelkezésre áll
- NAP kompatibilis
- SSTP fall-back, azaz ha valamiért nem sikerül IKEv2 kapcsolatot létesíteni, akkor automatikusan az SSTP-vel próbálkozik



5.23 ÁBRA A WINDOWS 7-BEN MÁR 4 VPN TÍPUS KÖZÜL VÁLASZTHATUNK[62]

A szükséges követelmények:

- R2 RRAS
- Tanúsítvány

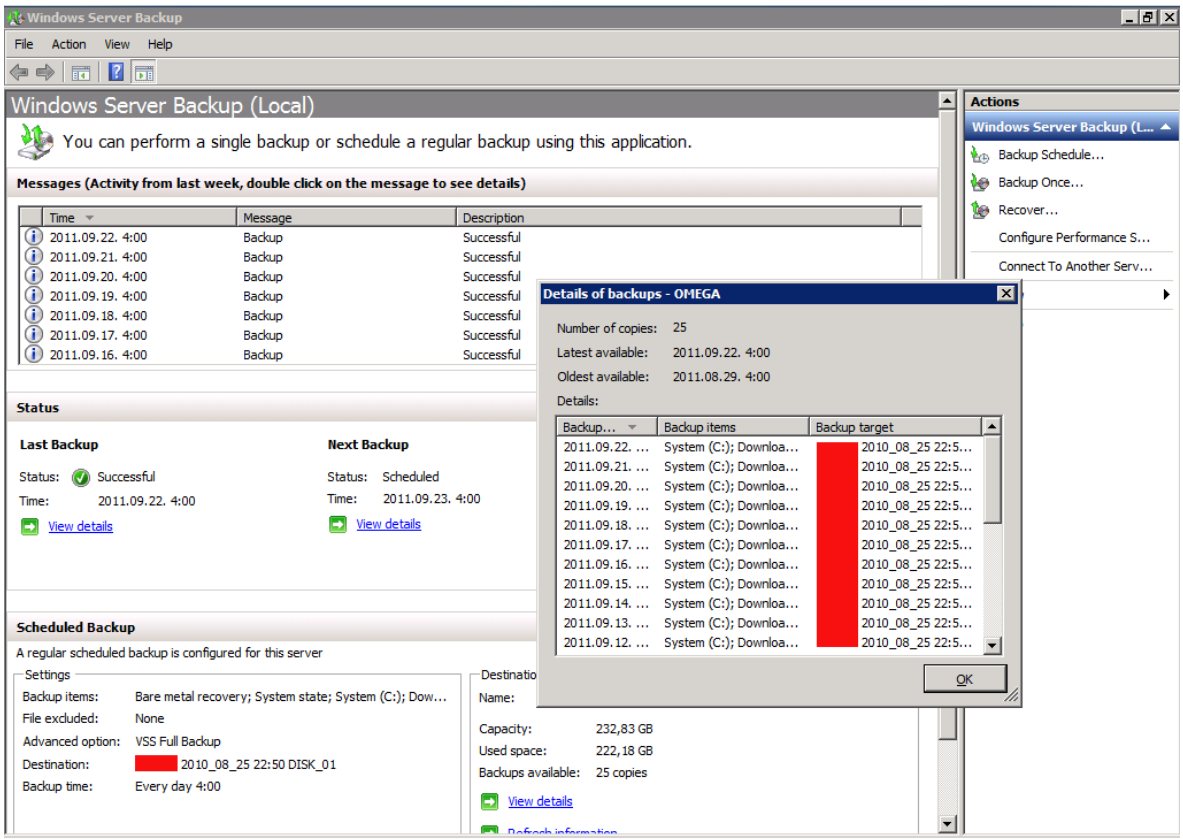
[62] Az automatikus választás esetén a sorrend a következő: IKEv2, SSTP, L2TP, PPTP

- Figyeljünk a „Common Name” mezőre, mivel VPN kapcsolatról van szó, valószínűleg publikus DNS nevet kell használnunk, hiszen ezzel érjük majd el a belső szervert
- A tanúsítvány Enchanced Key Usage (EKU) mezejében két dolog szerepeljen: az „IP security IKE intermediate” és a szokásos „Server Authentication” (az IPSEc sablon duplikálásával + a Server Auth felvételével az EKU mezőbe, ez egyszerűen megoldható)

- A hitelesítés kétféle lehet, számítógép („Client” tanúsítvány), vagy a felhasználó (jelszó: EAP-MSCHAPv2 és tanúsítvány[63]) alapú.

5.4 Windows Server Backup

Nos ebben az alfejezetben kivételesen nem lesz gond a két operációs rendszer verzió váltogatása vagy összehasonlítása. Ugyanis a Windows Server 2008-ban leledző beépített mentő és visszaállító képességről inkább nem írnék semmit, illetve csak annyit, hogy ez volt az első *próbálkozás* egy újfajta működésű és szemléletű eszközzel, a régi és ugyan helyenként korlátos, de azért sokrétű lehetőségekkel operáló NTBackup után. De a második menet már lényegesen jobban sikerült, az R2-ben immár egész jól lehet használni a Windows Server Backup komponenst[64].



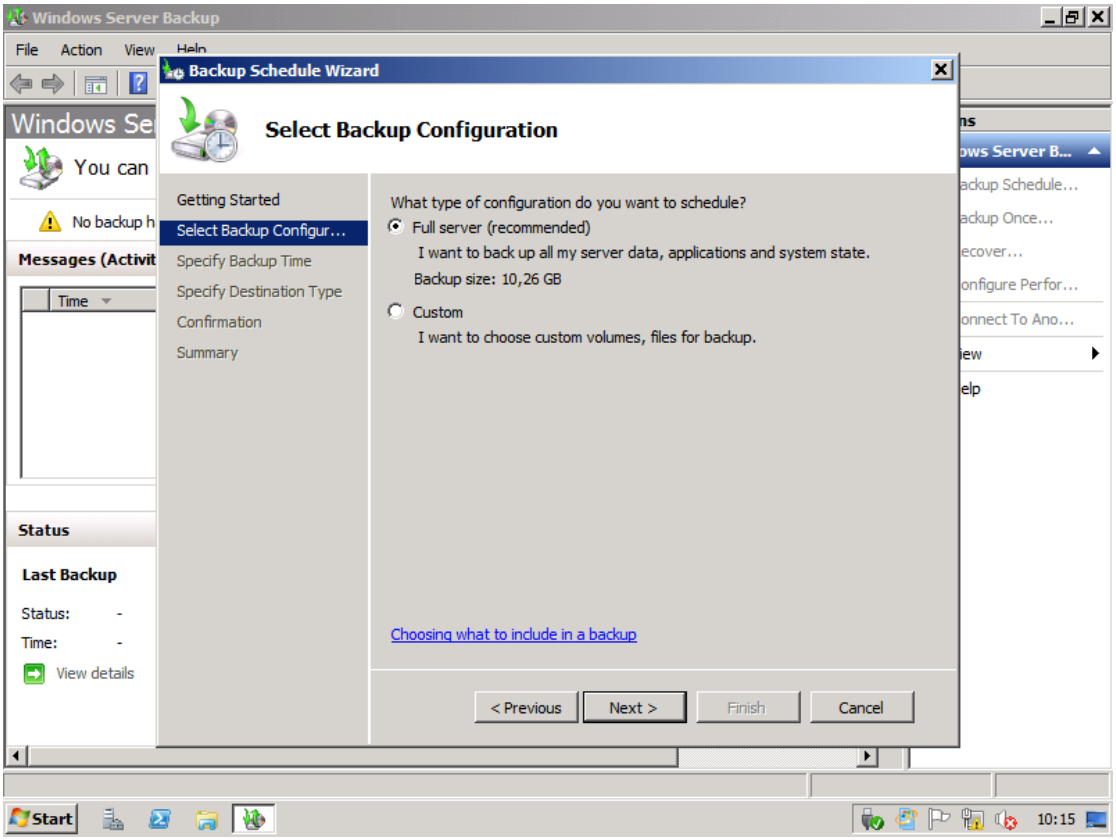
5.24 ábra Sok-sok növekményes mentés

[63] Ez utóbbi lehet természetesen egy smartcard-on is.
[64] Persze nagyvállalati környezetben a System Center Data Protection Manager az ajánlott megoldás.

A Windows Server Backup egy MMC beépülő modulból, a parancssori eszközökből és Windows PowerShell cmdlet-ekből áll. A Windows Server biztonsági másolattal a teljes kiszolgálóról, az összes kötetről, adott kötetekről, a rendszerállapotról, illetve konkrét fájlokról vagy mappákról is készíthetünk biztonsági mentést, helyben vagy távoli módban, illetve ütemezve is. Valamint az operációs rendszer nélküli helyreállításra (értsd > „krach") alkalmas biztonsági másolat is készíthető, csont nélkül.

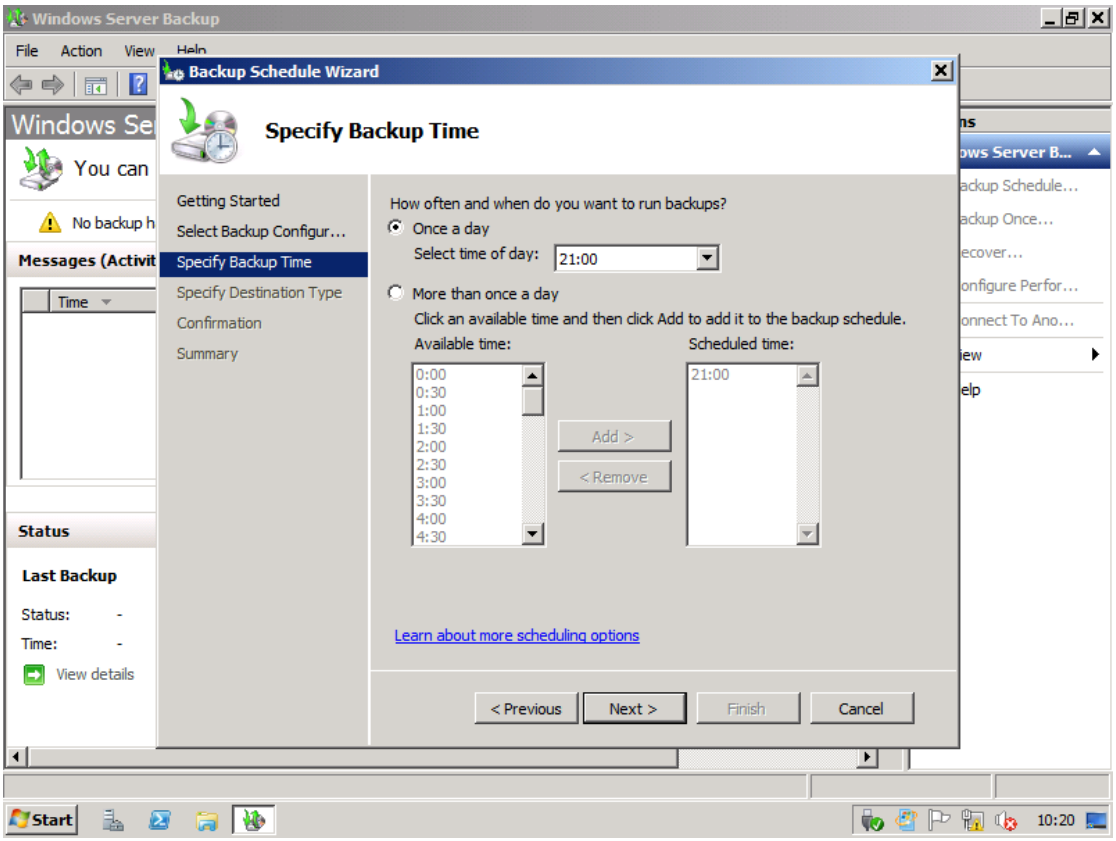
A biztonsági mentés segítségével kötetek, mappák, fájlok, bizonyos alkalmazások és a rendszerállapot állítható helyre. A merevlemez meghibásodása vagy egyéb katasztrófa esetén pedig végrehajtható az operációs rendszer nélküli helyreállítás. (Ehhez a teljes kiszolgálóról vagy az operációs rendszer fájljait tartalmazó kötetekről készült biztonsági másolat, illetve a Windows helyreállítási környezet szükséges - ez állítja helyre a teljes rendszert a régi rendszerre vagy egy teljesen új diszkre).

Javaslom, hogy menjünk is végig a folyamaton, azaz egy újabb képes beszámoló következik, helyi és teljes mentéssel, dedikált lemezre, és egyből rögtön ütemezve.

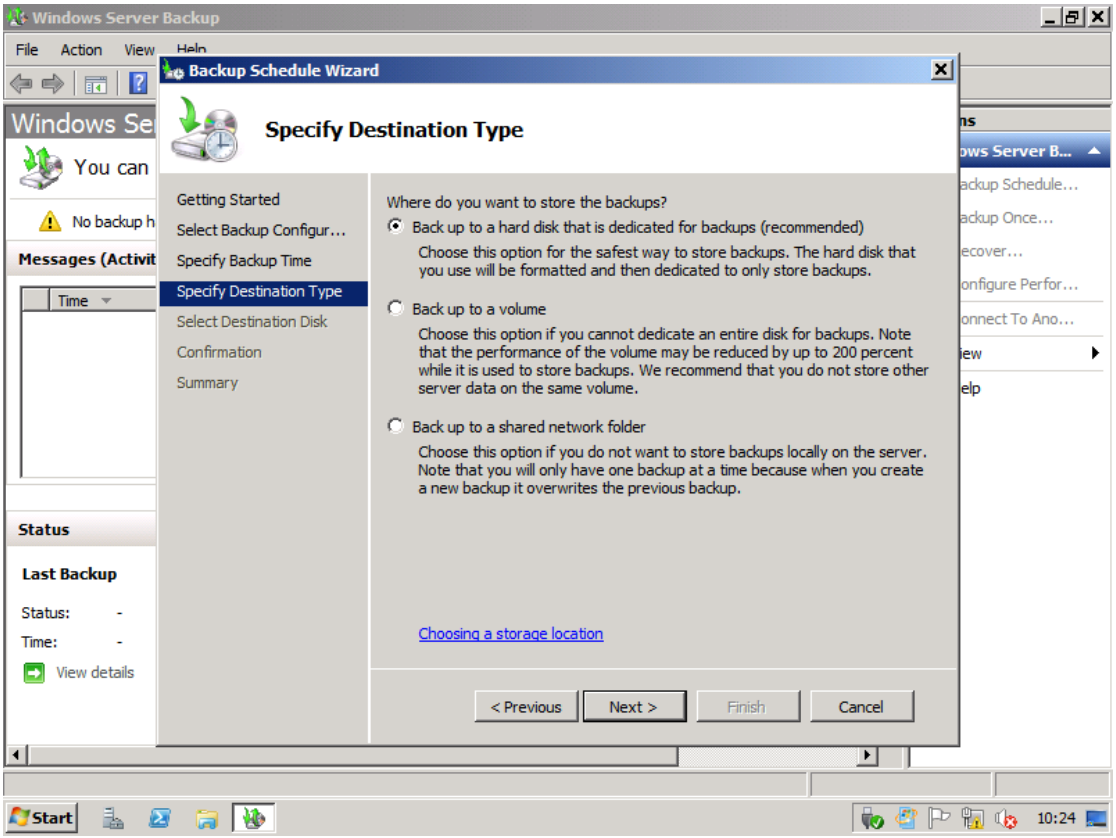


5.25 ÁBRA TELJES VAGY EGYÉNI, MOST TELJES

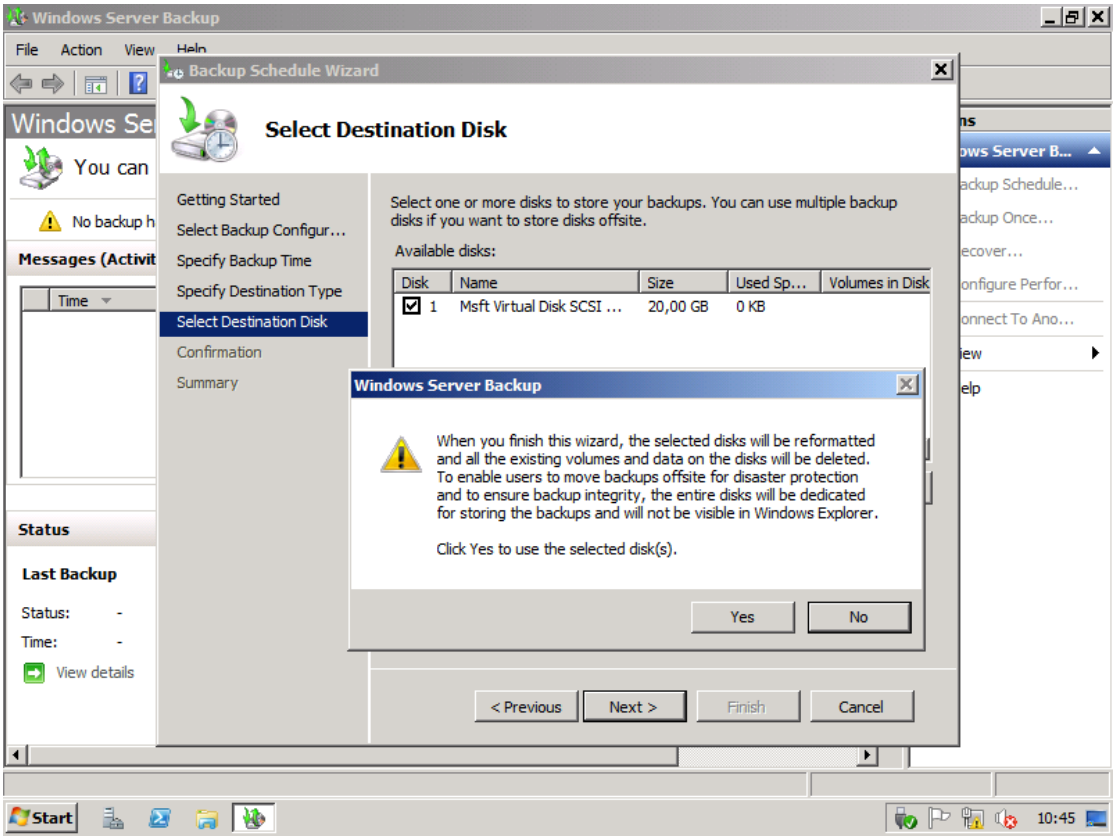
Ha egyébként a „Custom” opciót választjuk, akkor célpontként megkapjuk az összes lemezünket, ,partíciónkat, a „System State” és a „Bare metal recovery”mentés típusokat (ez utóbbi ugye az OS nélküli visszaállítás esete).



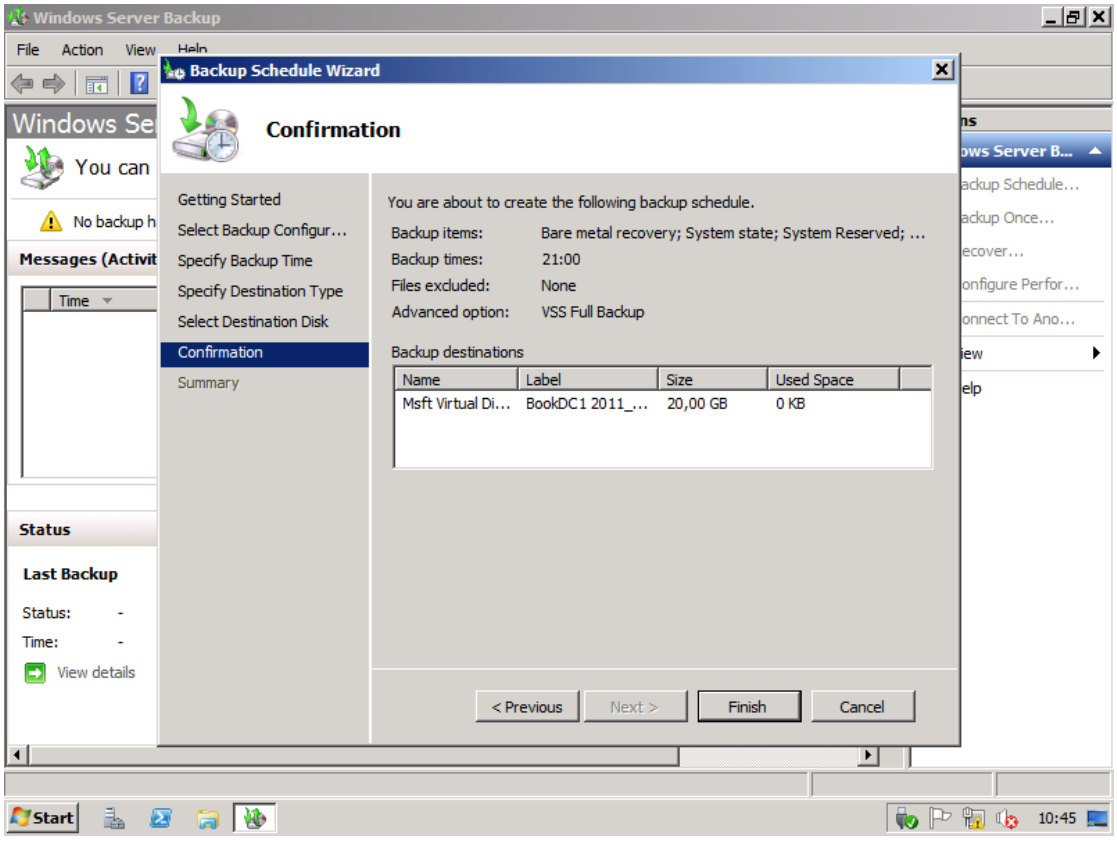
5.26 ÁBRA IDŐZÍTSÜNK, HETI KETTŐ NAP NINCS, DE MAJD KÉSŐBB TRÜKKÖZÜNK



5.27 ÁBRA A CÉLPONT EGY DEDIKÁLT LEMEZ, EGY KÖTET, VAGY EGY HÁLÓZATI MEGOSZTÁS LEHET, SZALAG NEM ☺



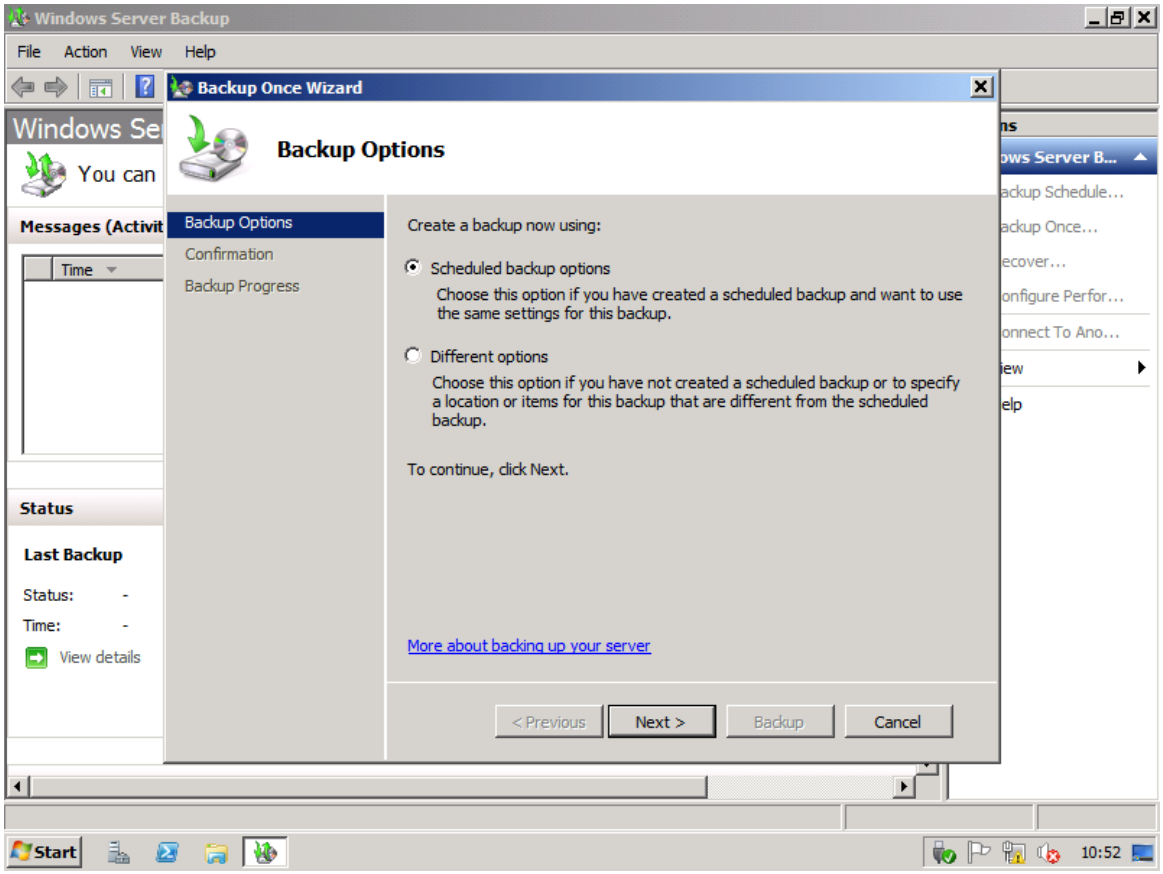
5.28 ÁBRA A DEDIKÁLT LEMEZT MÁSRA NEM TUDJUK MAJD HASZNÁLNI A WINDOWS ALATT, DE NEM BAJ, JÓ LESZ



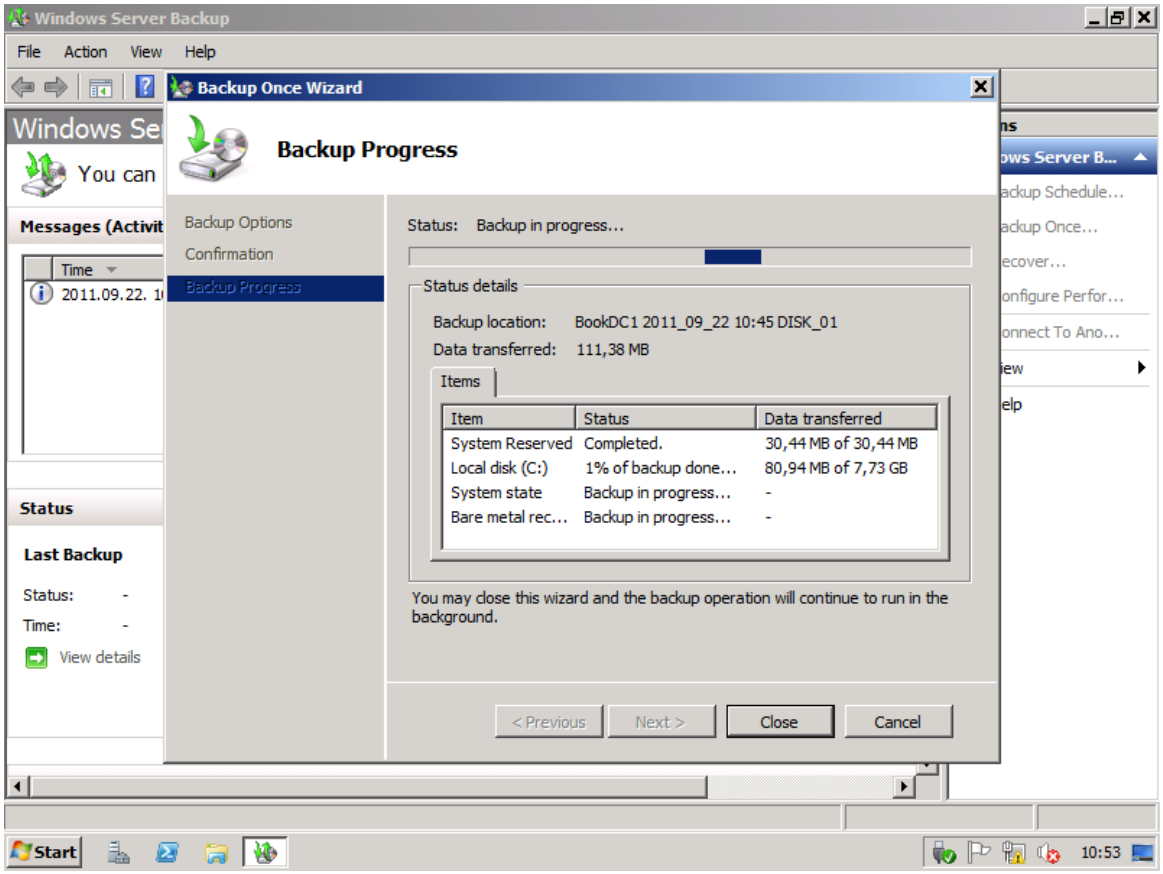
5.29 ÁBRA A SZUMMA TETSZETŐS EREDMÉNYT SEJTET

> Feltűnt, hogy a varázsló nem kérdezett rá arra, hogy teljes vagy növekményes, vagy különbségi legyen? Nem hát, mert nem szükséges. A teljes és növekményes biztonsági másolatokat automatikusan kezeli a Windows Backup, azaz egy teljes biztonsági másolatként *viselkedő* növekményes biztonsági másolatot hoz létre. Ez azzal jár, hogy az eseti biztonsági másolatok tetszőleges eleme helyreállítható lesz majd, de a mentés csupán a növekményes biztonsági másolathoz szükséges helyet foglalja el. Sőt, nem kell kézzel törölgetnünk sem, a rendelkezésre álló hely függvényében a régebbi biztonsági másolatok automatikusan törlődnek. Magyarul, teljesen magára hagyhatod a mentést, és ha nagy a diszk, akkor nagyon sokáig kényelmes helyzetben vagy.

Nos, ezután formázza a dedikált lemezt, és kész is. Csináljunk most egy az időzítéstől eltérő példányt, ergo válasszuk a „Backup Once” opciót az Action pane keretből.



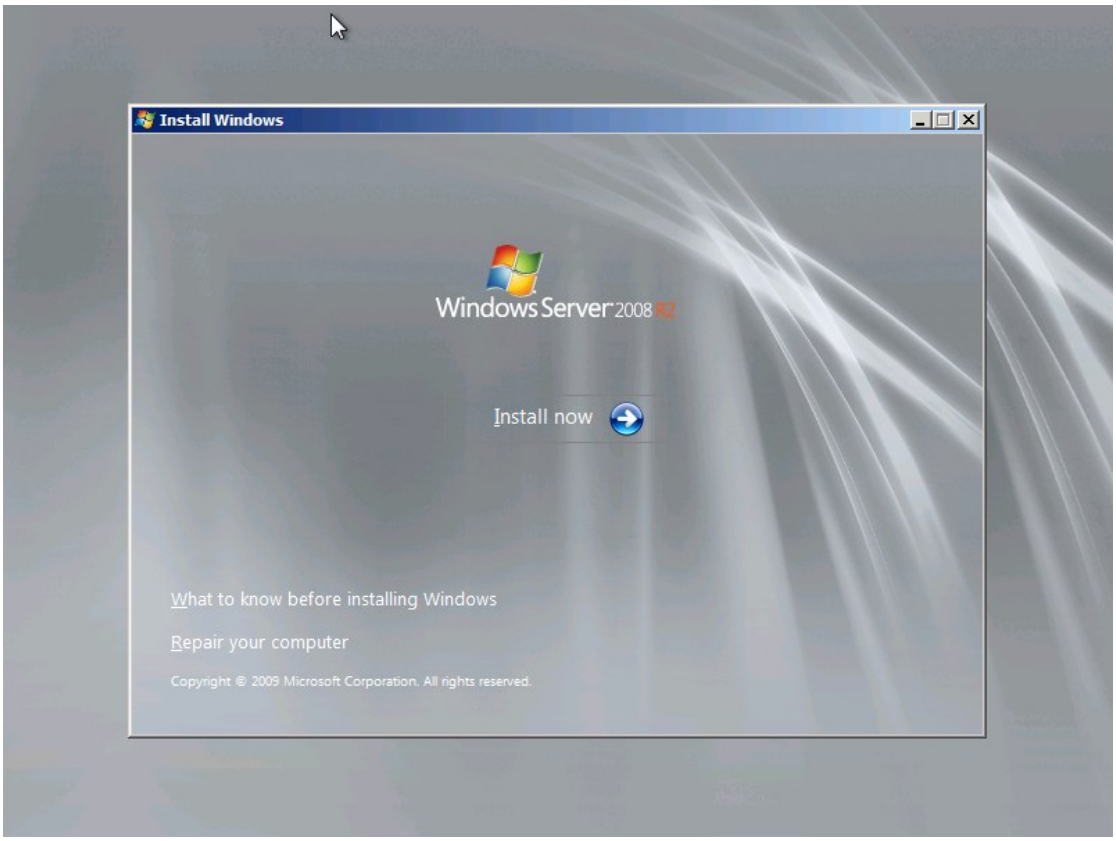
5.30 ÁBRA NYOMHATUNK EGY KORÁBBAN IDŐZÍTETTET VAGY EGY TELJESEN EGYEDIT



5.31 ÁBRA JUST DO IT!

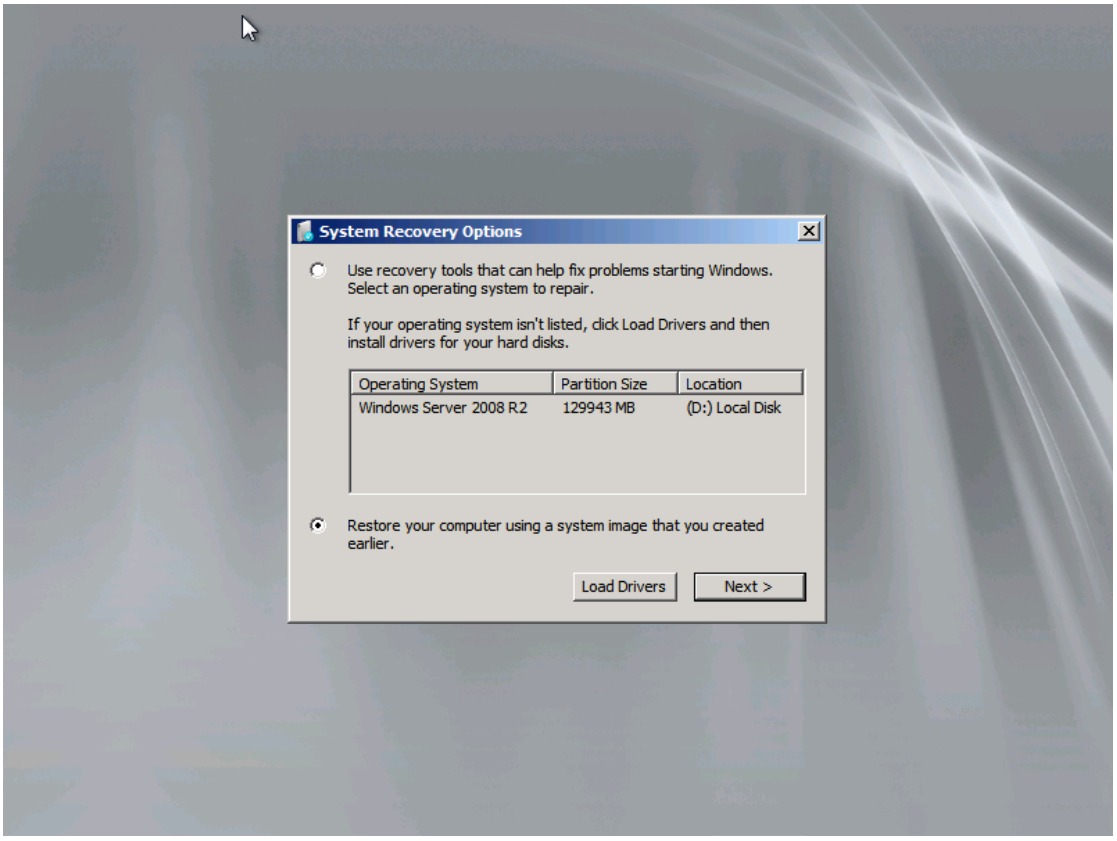
És most az történt, amitől a legjobban tartunk, feladta a szerver hardver (de a backup diszk nem ☺), de már beszereztük az új HDD-ket, és vissza fogunk állítani mindent.

A visszaállítás viszonylag egyszerű lesz[65], el kell indítanunk a telepítő DVD-t, majd még a telepítés előtt, a Repair your Computer" opciót választva a „Windows Recovery Environment" üzemmódban, automatikusan megtalálva a helyi mentést, vagy tallózva a hálózatot visszaállíthatjuk a szerverünket – csont nélkül.

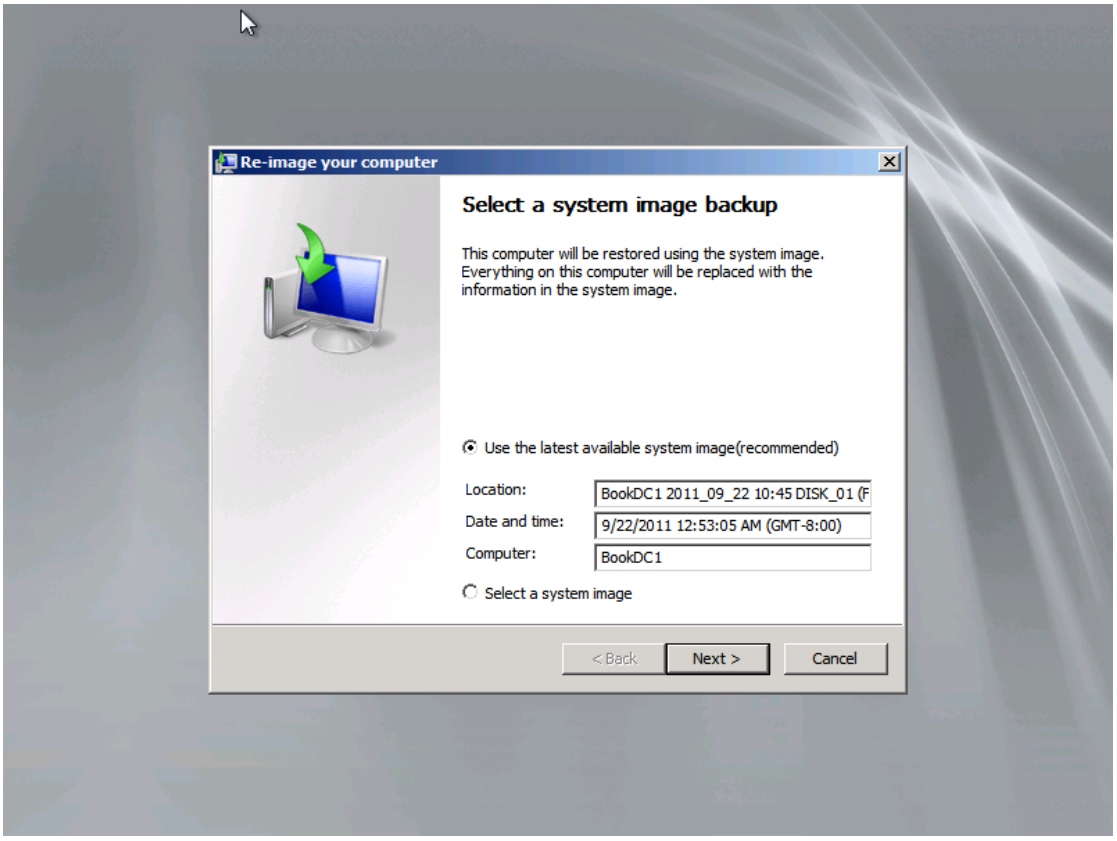


5.32 ÁBRA A REPAIR YOUR COMPUTER A BARÁTUNK

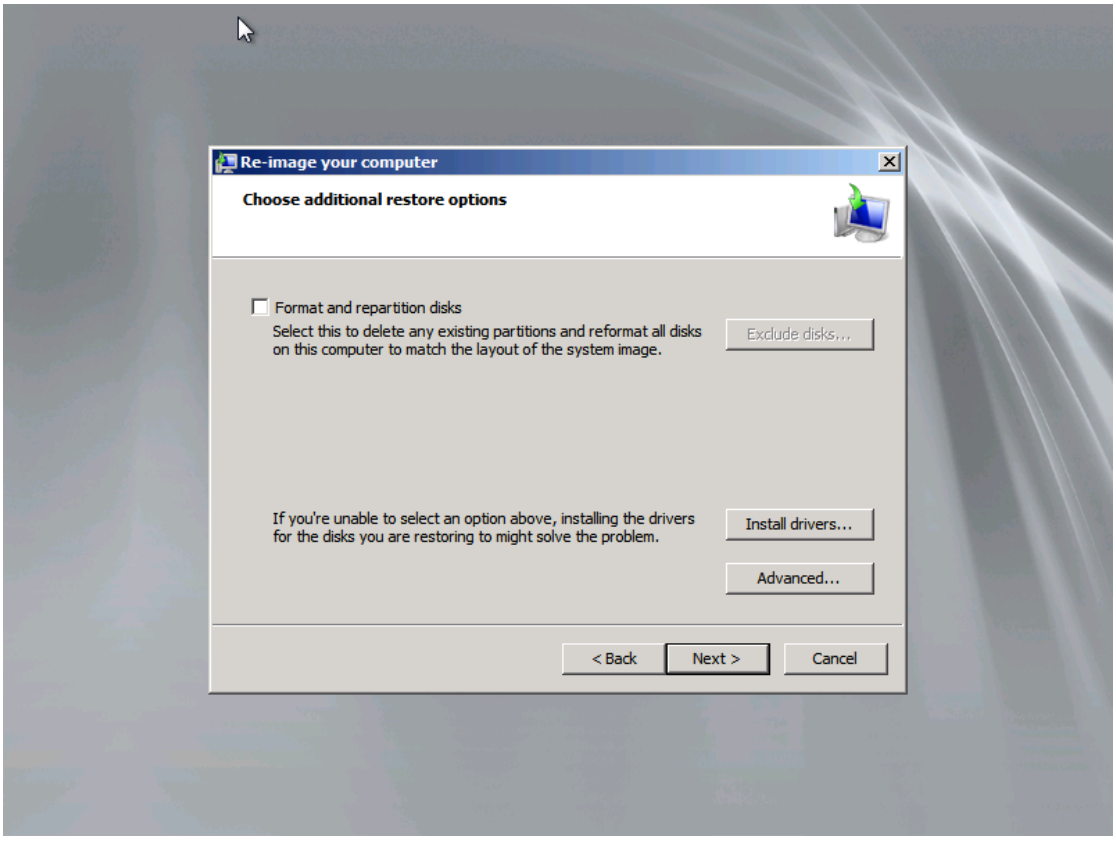
[65] Ehhez persze a teljes szerverről vagy az operációs rendszer fájljait tartalmazó kötetekről készült mentés szükséges mindig, és ha okosan csináltuk, és egy dedikált lemezen van mindez, akkor valószínűleg nagyon gyors is lesz.



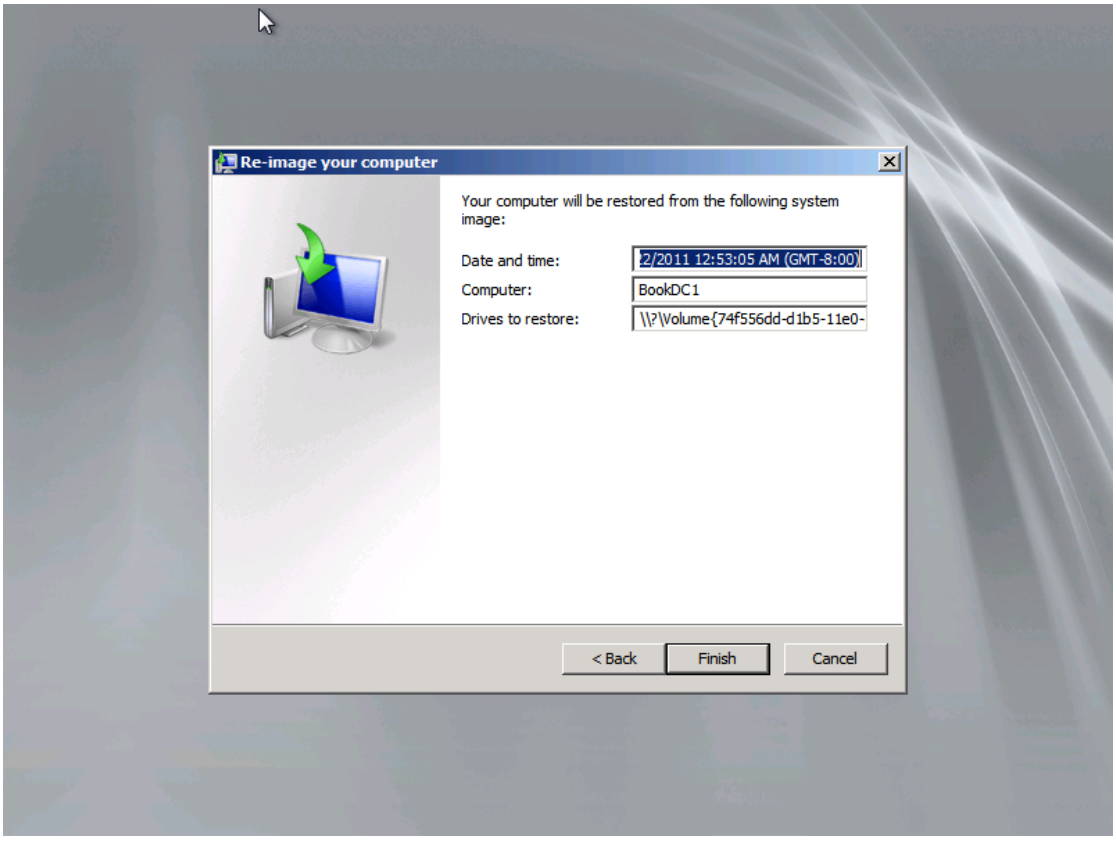
5.33 ÁBRA KICSIT CSALTAM, MERT NEKEM NEM HALT MEG, DE AZ ALSÓ LESZ A LÉNYEG



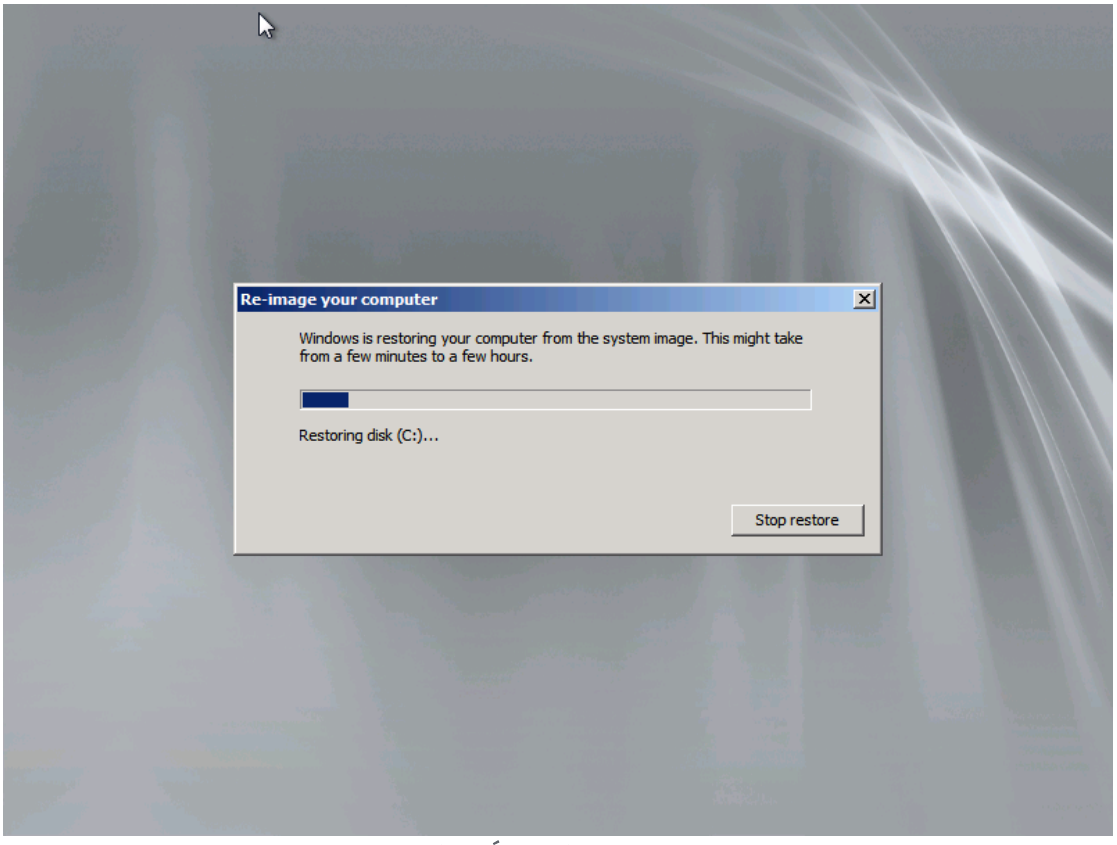
5.34 ÁBRA MEG IS VAN, HURRÁ, ALUL VISZONT VÁLOGATHATNÁNK, HA LENNE TÖBB MENTETT PÉLDÁNY



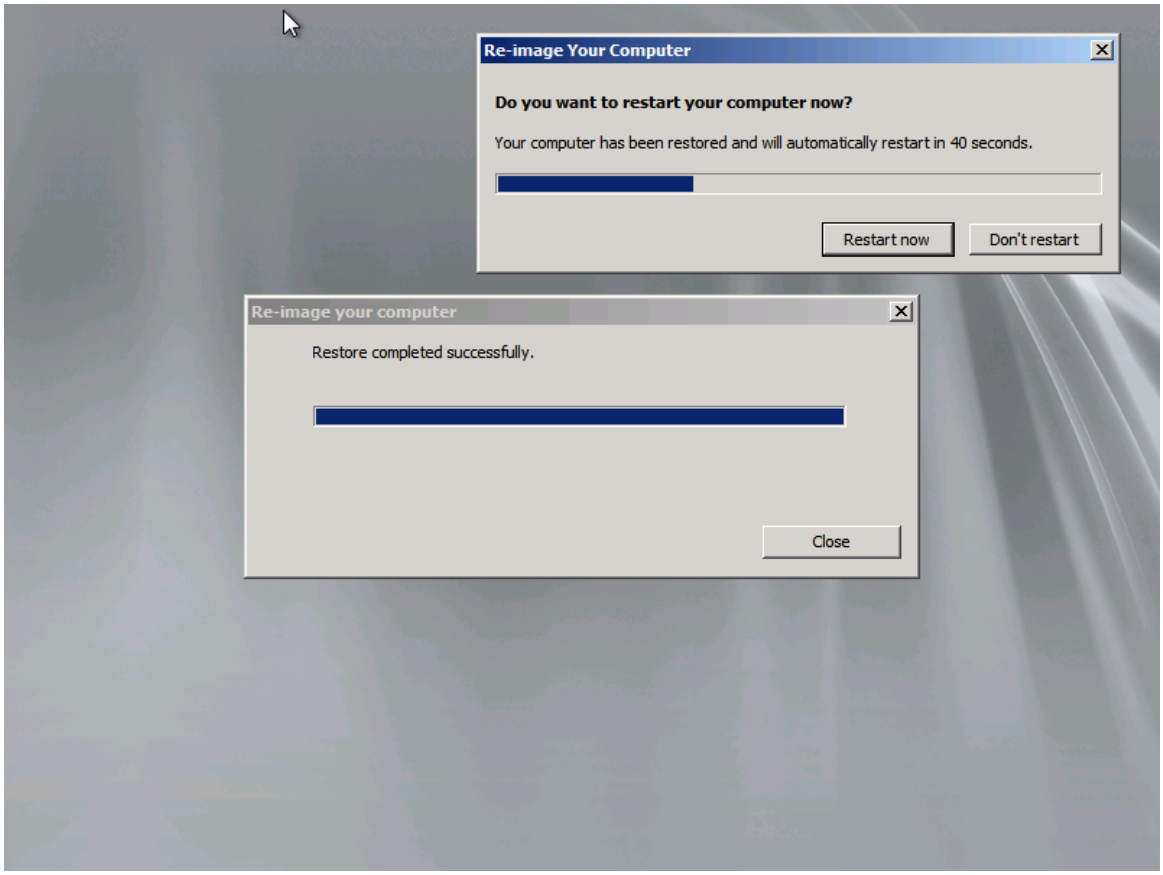
5.35 ÁBRA LEGYEN FORMÁZÁS? AKARUNK DRIVEREKET PÓTOLNI? AKARUNK ELLENŐRZÉST (ADVANCED)?



5.36 ÁBRA LESZ, AMI LESZ



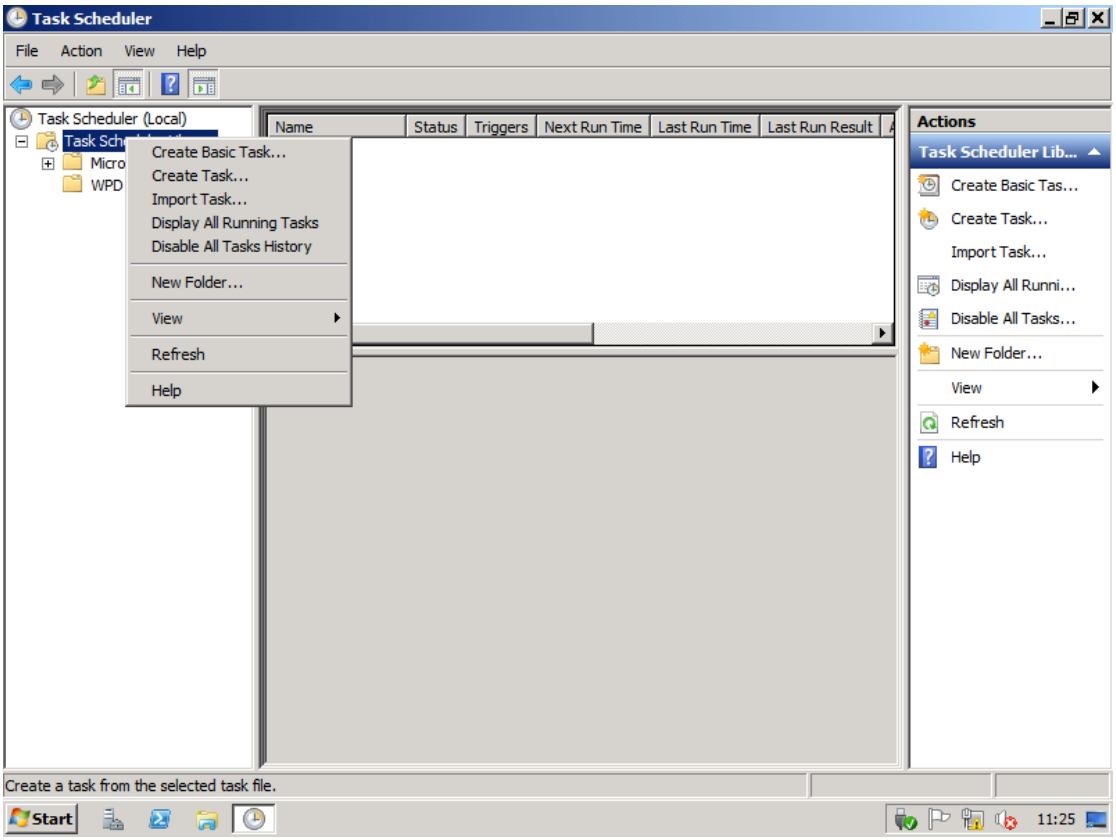
5.37 ÁBRA ÉN A CSÍKNAK DRUKKOLOK



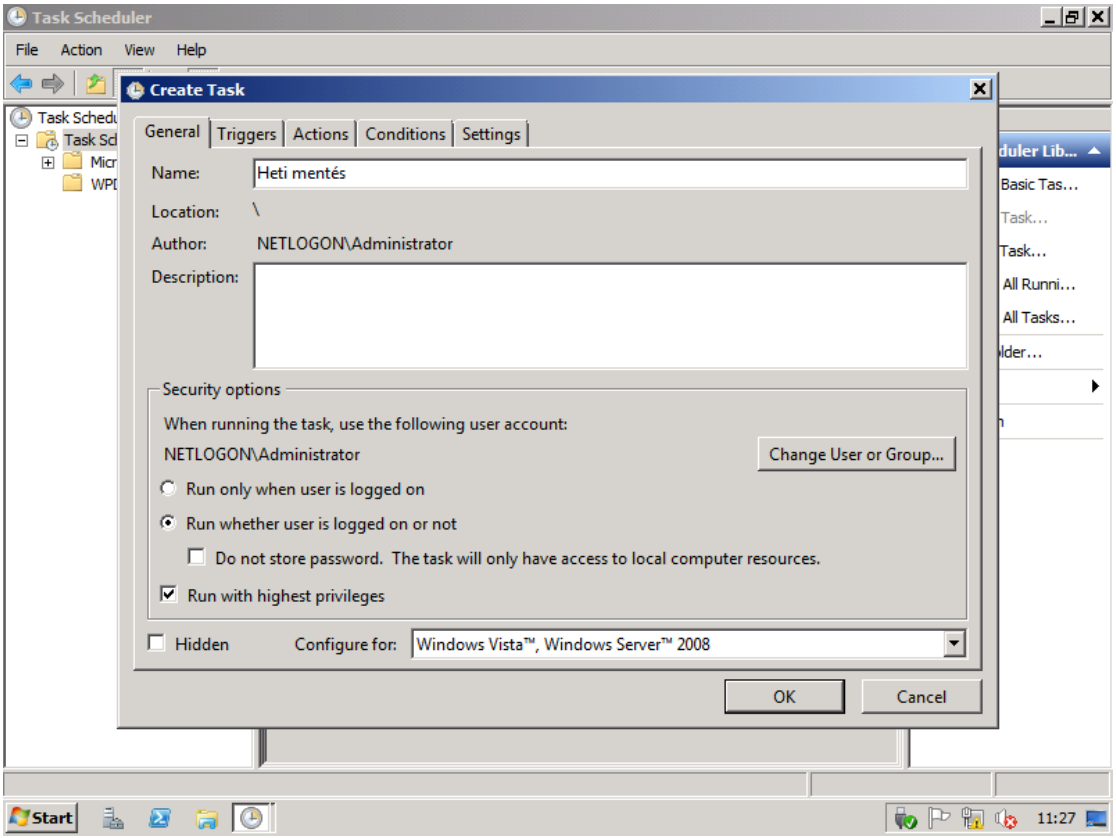
5.38 ÁBRA SŰRŰN NEM KELL ILYEN ÉLMÉNY, DE MOST SIKERESEN KORRIGÁLTUNK

Az 5.25 ábra alatt volt egy megjegyzésem, ami kissé gúnyosnak tűnhet, de helytálló, valóban nem tudunk, csak napi időzítést elvégezni. Mármint ha csak a GUI-t kapargatjuk, mert egyébként a „wbadmin” és a Task Scheduler segítségével simán. Ezért fontos, hogy amikor telepítjük a Server Managerben, akkor a „Windows Server Backup Features” alatt a „Command-line Tools” részt is pakoljuk fel.

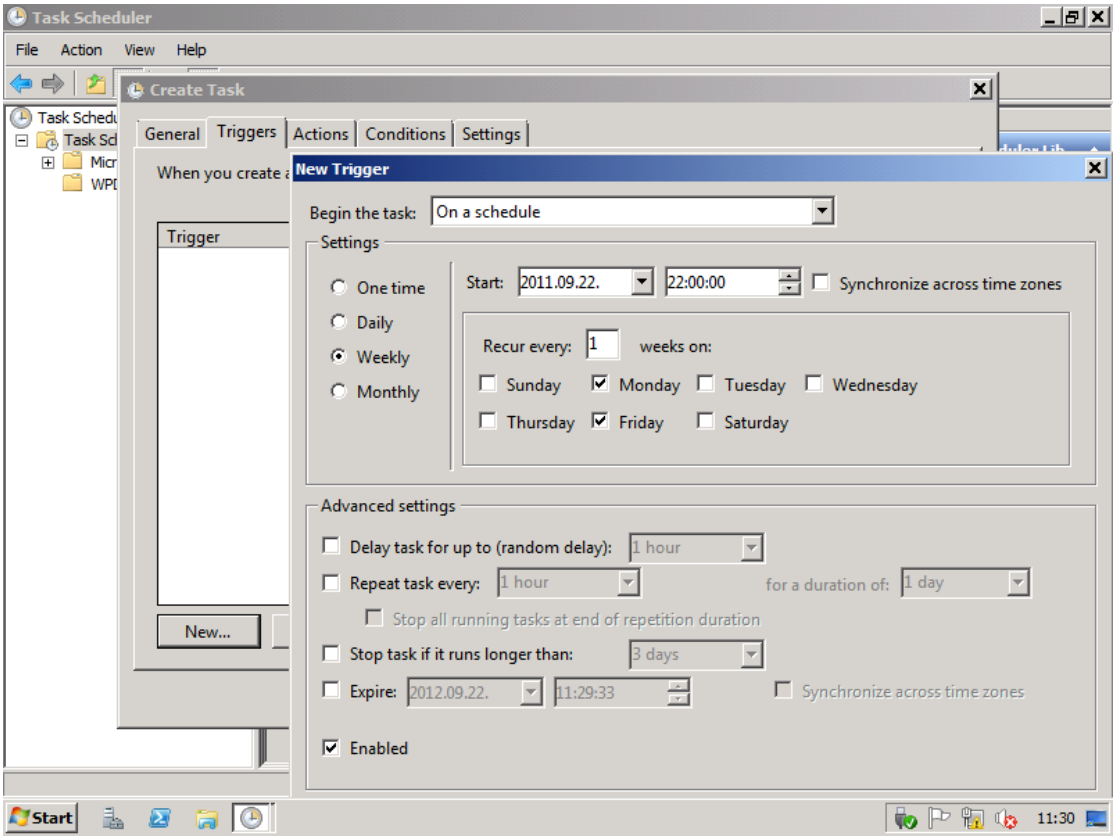
Ha megvan, akkor használjuk ki, indítsuk el a Task Scheduler-ből (Administrative Tools) a „Create Task” menüpontot!



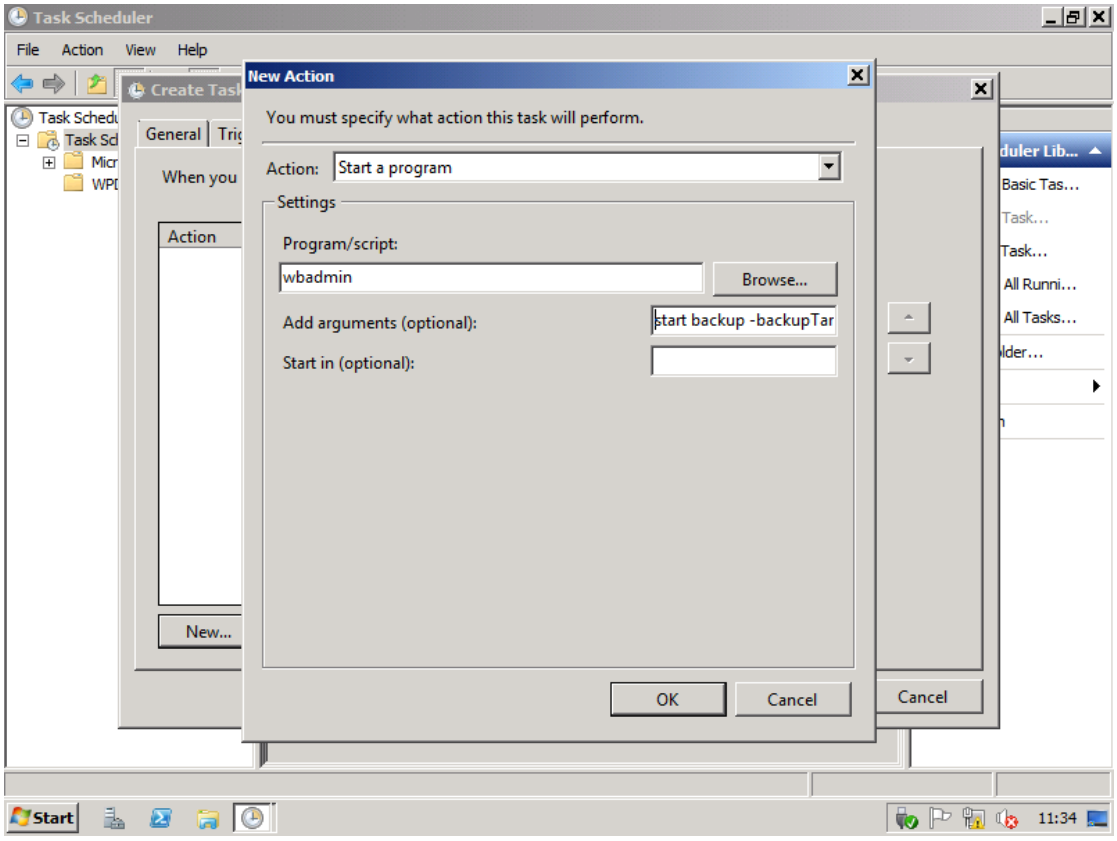
5.39 ÁBRA NAGYON KELLEMES ESZKÖZ, SOKAT SEGÍT



5.40 ÁBRA MINDEN LÉNYEGES DOLGOT BEÁLLÍTOTTAM



5.41 ÁBRA EGY ÚJ TRIGGERT VETTEM FEL, HETI 2 NAPRA, NE FELEJTSÜK ALUL AZ „ENABLED”-ET!

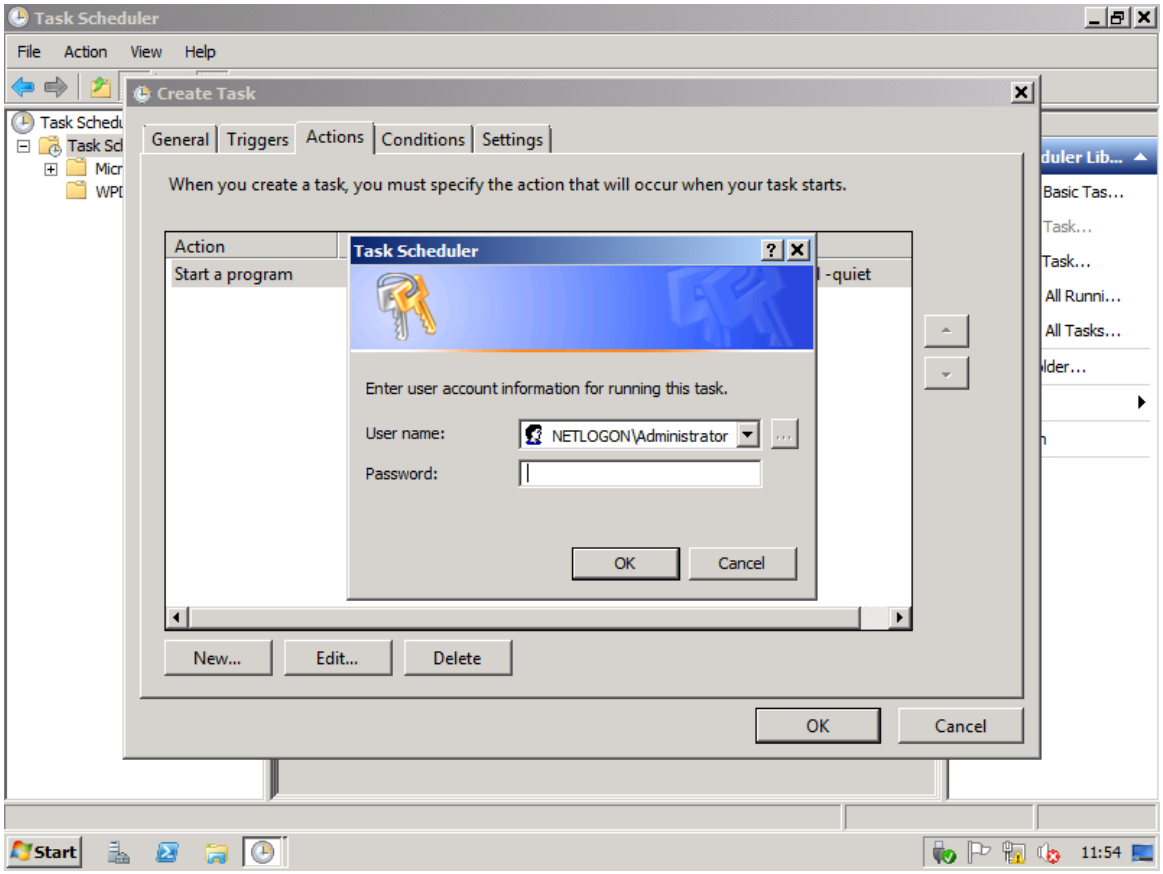


5.42 ÁBRA AZ AKCIÓ A PARANCSSOROS ESZKÖZ FUTTATÁSA

Nos, itt álljunk meg egy kicsit! A parancs így néz ki jelen esetben:

wbadmin start backup -backupTarget:F: -include:E: -allCritical -quiet

- start backup: a wbadmin.exe indítása
- backupTarget: a célhely, jelen esetben kivételesen egy másik kötet, az F:
- include: milyen egyéb köteteket vegyen bele a mentésbe, pl. most az E:-t
- allCritical: ezzel azt jelezzük, hogy legyen System State és System volume mentés is, tehát a teljes diszk nélküli visszaállítás is
- quiet: a háttérben, mindenféle megjelenés nélkül fusson



5.43 ÁBRA JOGOSULTSÁG SZÜKSÉGES

Ha ezzel megvagyunk, a Task Scheduler Library alatt egy új feladatunk született, és teszi a dolgát szépen.

Még két dologról beszélni szeretnék a Windows Server Backup apropóján, éspedig a Hyper-V és az Exchange Server mentéséről. Mindkettő kicsit „szegény ember vízzel főz" megoldás, tehát nekünk kell kicsit piszkálni manuálisan a rendszert, de működik.

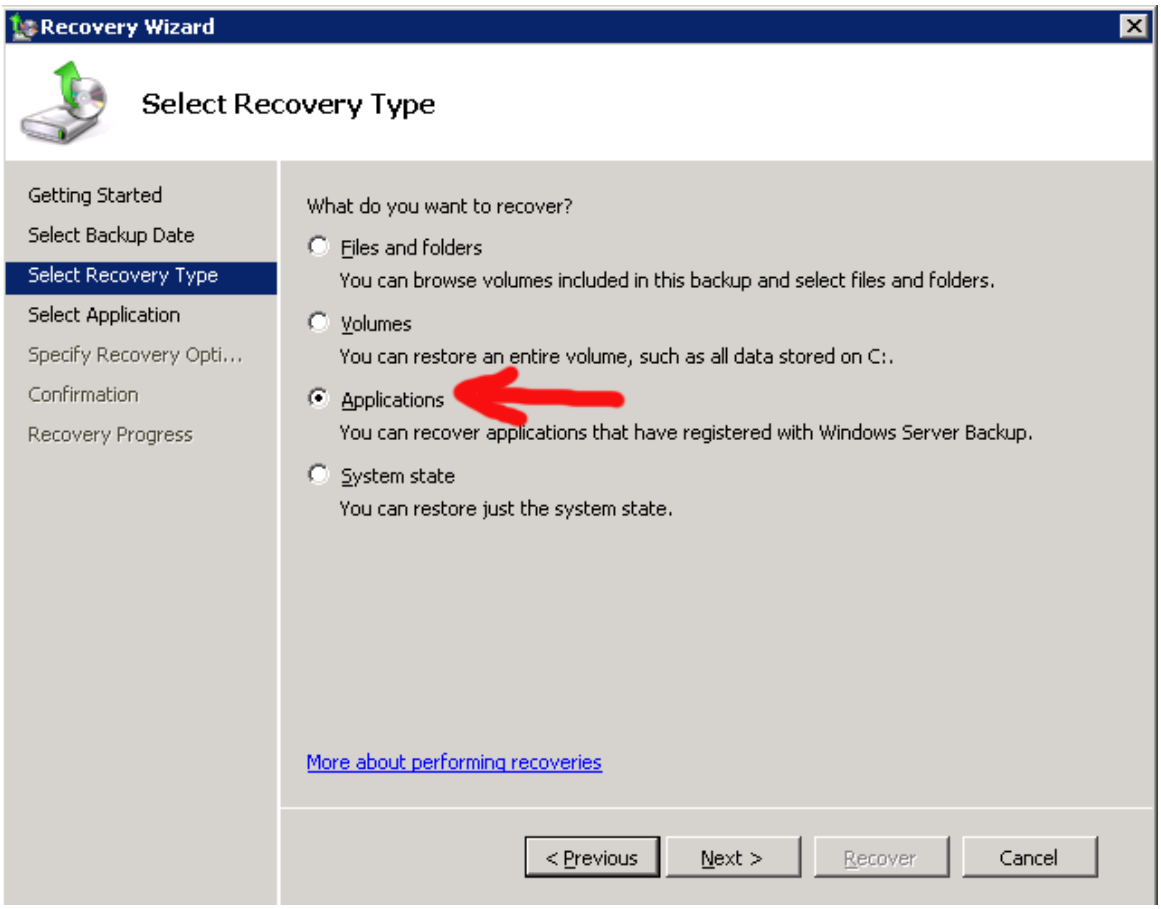
A Hyper-V esetén egy registry kulcsot kell hozzáadnunk ahhoz, hogy a Windows Backup VSS alapú virtuális gép mentést is tudjon. Ez az a kulcs, amelyet létre kell hoznunk (figyeljünk oda, már a „WindowsServerBackup" sincs felvéve):

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT \CurrentVersion\WindowsServerBackup\Application Support\{66841CD4-6DED-4F4B-8F17-FD23F8DDC3DE}

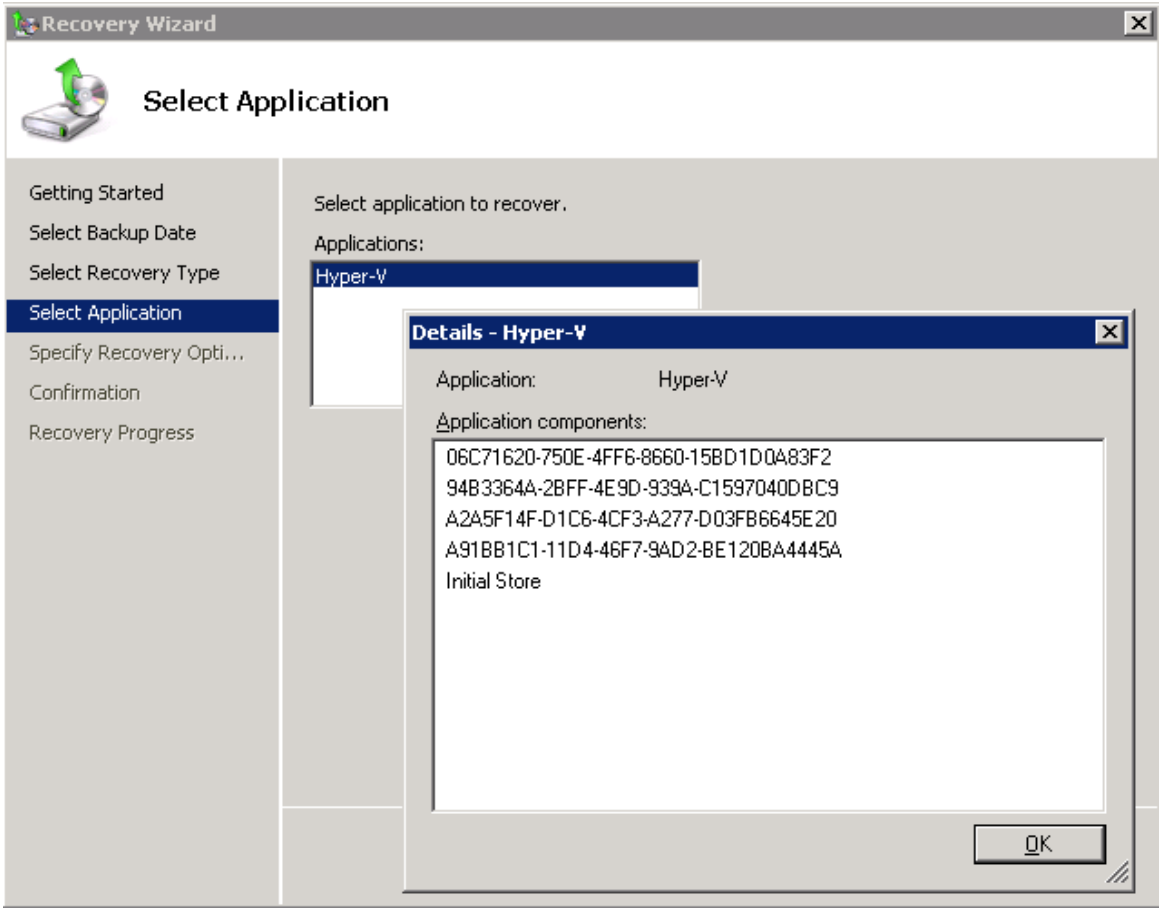
Ha ez megvan, akkor hozzunk létre ez alá egy String Value-t:

Name: Application Identifier
Type: REG_SZ
Value: Hyper-V

Ha ez megvan, akkor mentsük le a Hyper-V gépek állományait (mindet) tartalmazó egész kötetet, majd nézzük meg, hogy ezután, a visszaállítást megpróbálva, az „Applications” típus alatt látjuk-e a Hyper-V gépeket!



5.44 ÁBRA A REGISZTRÁLT ALKALMAZÁSOK VISSZAÁLLÍTHATÓAK...



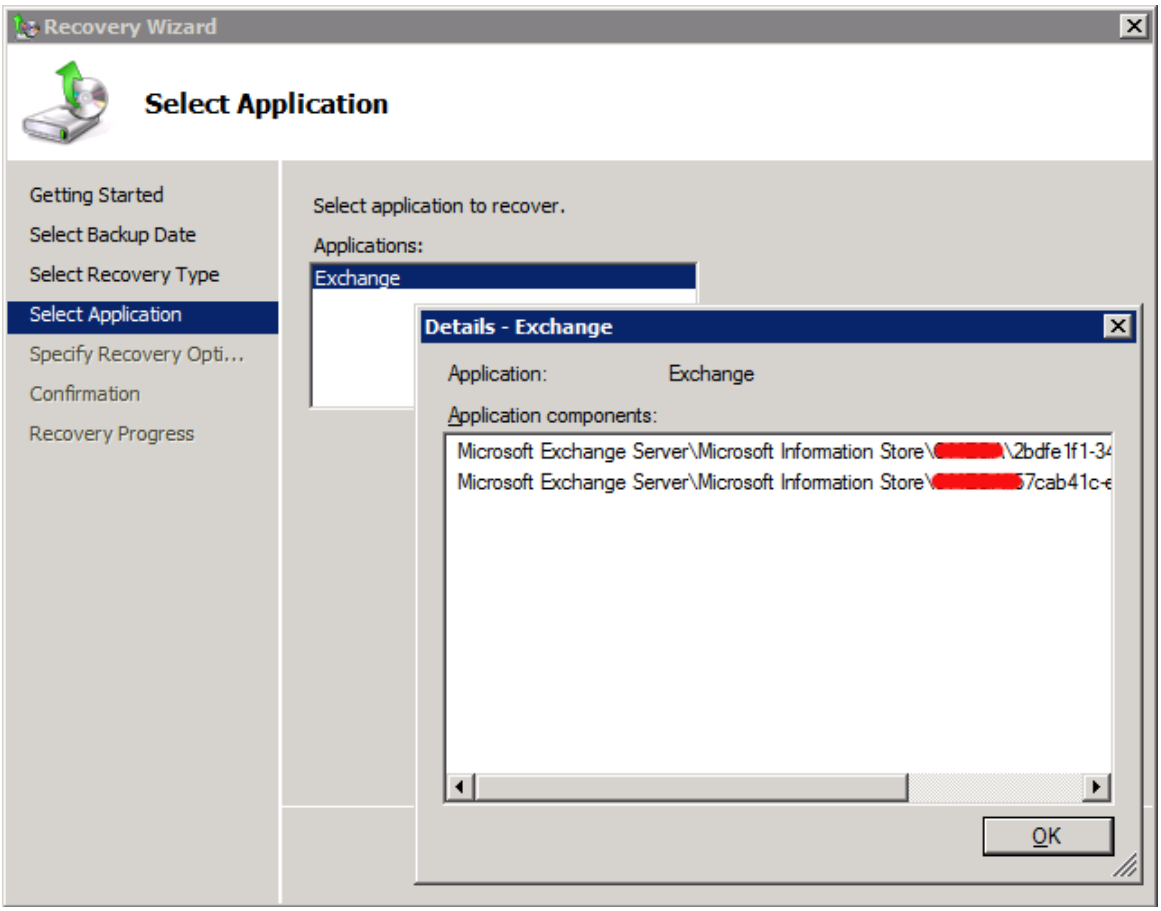
5.45 ÁBRA ...ÍGY A HYPER-V VIRTUÁLIS GÉPEI IS

Sajnos két-három korlátunk is van e téma kapcsán[66], az egyik, hogy a Microsoft támogatás a dinamikus lemezekkel rendelkező guest gépek esetén csak az offline állapot mentésére vonatkozik, a másik pedig az, hogy VSS-t nem támogató OS-ek (Windows 2000, XP), illetve a Integration Services nélküli gépek (lásd: 9. fejezet) az effajta mentés közben „saved state" állapotba kerülnek. No és persze a virtuális gépeket egyesével nem tudjuk visszaállítani, csak az egész kötetet, szóval azért ez közel sem tökéletes megoldás.

> Az olvasó a „saved state" miatt „shutdown"-ra gondolhat, pedig nem ez történik. A „saved state" során a virtuális CPU megáll, a regisztereit a rendszer elmenti, a virtuális gép memóriatartalmát pedig a gép a merevlemezre menti. Ezután megtörténik a mentés, majd a mentés után a futási állapot helyreáll. A virtuális gép operációs rendszere azt érzékeli, hogy „ugrás történik az időben" – pont mint a Mátrix-ban ☺ (A lektor megjegyzése)

[66] A Windows 8 Server Developer Preview változatában ez az egész mahináció nem szükséges, a Hyper-V 3.0 gépeit egyből és külön-külön látja a Windows Backup.

Az Exchange Server mentése már kevésbé kacifántos[67], viszont az R2 + Exchange 2010 páros kell hozzá (mivel az utóbbi már tartalmazza a Windows Backup alá, a VSS-hez szükséges bővítményt) és az adatbázisok mappaszintű mentése.



5.46 ÁBRA EXCHANGE STORE-OK VISSZÁLLÍTÁS LEHETŐSÉGE WINDOWS BACKUP-PAL

Nos ezzel az hosszú-hosszú 5. fejezet véget ért, sok-sok apró és néhány nagyobb változást áttekintettünk, most viszont jöjjenek az igazán „nagyok”.

[67] http://technet.microsoft.com/en-us/library/dd876854.aspx

6 AD*

A címtárszolgáltatással kapcsolatos változások és fejlesztések minden új Windows kiszolgáló esetén a fókuszba kerülnek. Nyilván nem véletlenül, hiszen a címtár hierarchia rugalmassága és alkalmazhatósága miatt a tíz és a tízezer gépet tartalmazó hálózatok esetén egyaránt jól használható az Active Directory, mégpedig a minden szervezet számára legfontosabb célra: a felhasználók, a számítógépek és egyéb erőforrások tárolására és kezelésére. Persze, emellett a biztonsági „erőtér" megteremtése és egyéb fontos kiszolgáló alkalmazások, megoldások (Exchange, Csoportházirend, stb.) működésének támogatása is kritikus feladat.

De először az elnevezések változásairól és a Microsoft „családteremtő" szándékáról kell beszélnünk. Ugyanis az „Active Directory" egy gyűjtőnév lett, és több eddig külsősként nyilvántartott szerepkör is megkapta ezt az előtagot.

- Active Directory Domain Services
  - Az eddigi, szimpla „Active Directory" helyett
- Active Directory Lightweight Directory Services
  - Az „ADAM", azaz az AD Application Services helyett, lásd mini címtár
- Active Directory Certificate Services
  - A lokális PKI infrastruktúra megteremtője
- Active Directory Federation Services
  - Azonosítás kezelő, tipikusan a http/s alapú kliensek extranetes erőforrás eléréséhez
- Active Directory Rights Management Services
  - Központi szabályzású, információvédelmi megoldás

Itt és most mi szinte csak az első tétellel, azaz a címtárszolgáltatásokkal foglalkozunk, de a Windows Server 2008 és az R2 olyan rengeteg újdonságot hozott ezen az egy téren is, hogy muszáj minimum ketté és aztán még tovább szabdalni ezt a nagy-nagy fejezetet, így aztán először kezdjük a „régivel", azaz a Windows Server 2008-cal!

6.1 Az első szakasz: a Windows Server 2008

6.1.1 Read-Only tartományvezérlők (RODC)

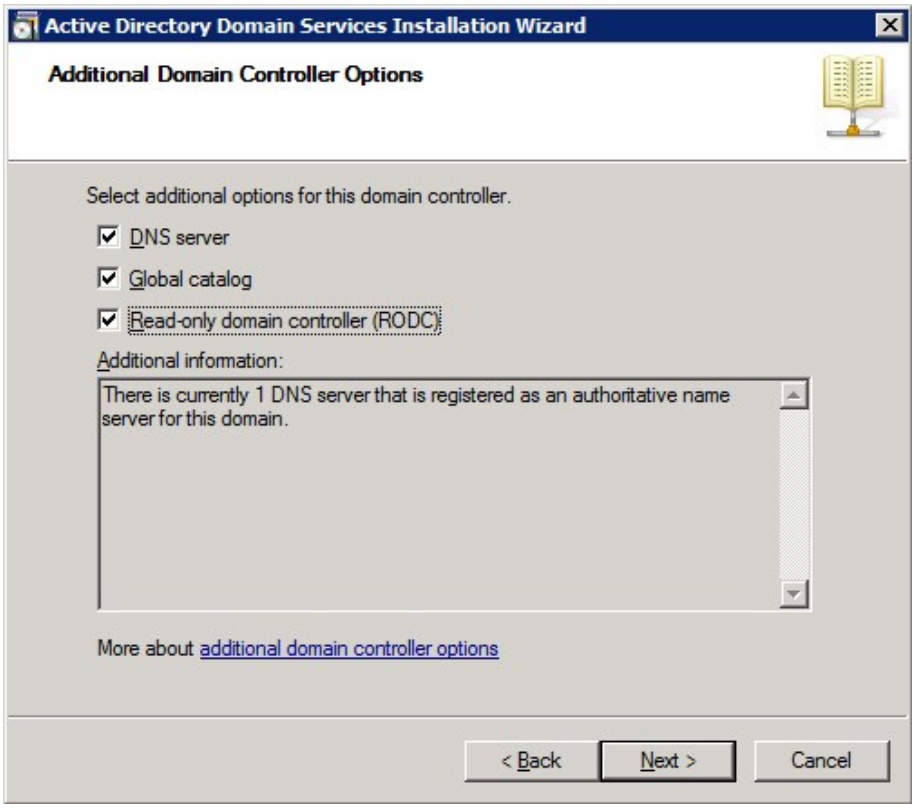
Anno megdöbbentő volt, hogy a Microsoft egy teljesen új tartományvezérlő típussal rukkol elő, de mára már megszoktuk és szeretjük, már csak azért is, mert valóban elmondható, hogy ténylegesen valós igények hozták létre ezt a típust.
Egy mondatban összefoglalva, a RODC egy olyan DC, amely tartalmazza a címtár egy példányát, azaz képes az összes tartományvezérlő feladat ellátására, de a címtár tartalma nem változtatható meg helyben. Miért előnyös ez?

- Biztonságos: mivel nincs globális AD módosítási lehetőség, olyan környezetbe is ajánlható, ahol fizikailag nem garantálható a biztonság, pl. egy védett szerverszobát nélkülöző telephelyre. Ha esetleg aztán az adott szervert helyben megpróbálják feltörni, vagy történetesen eltulajdonítják, az igazán szenzitív, globális tartományi adatokhoz nem lehet majd hozzáférni semmilyen módon, hiszen helyben ezek alapértelmezés szerint nem tárolódnak.

- Sávszélesség és erőforrás takarékos: mivel egy telephelyre biztonságosan telepíthető, a hitelesítési folyamatokhoz (pl. belépés, helyi erőforrás elérés) nincs szükség a WAN hálózatra vagy az internetre, igaz, ekkor némi kompromisszumra kényszerülünk, lásd később.

- Alkalmazás- és üzemeltetés barát: előfordulhat, hogy üzleti szempontból is fontos alkalmazások megkövetelik a tartományvezérlőt mintegy host gépként, vagy legalább a gyors elérését. Az is elképzelhető, hogy ezt az alkalmazást más szerver híján az egyetlen (telephelyi) szerverünkre kell feltelepíteni. Sőt, az is előfordulhat, hogy a speciális alkalmazást egy külső cég üzemelteti, azaz szüksége van interaktív belépésre, magas jogosultsági szinttel.
  Ki az, aki szívesen ad tartomány rendszergazda jogot egy ilyen esetben a külső szervezetnek? Viszont eddig - egy DC esetén - majdnem minden esetben muszáj volt, hiszen más lehetőségünk nem állt rendelkezésre. Nos, a RODC esetén nyugodtabbak lehetünk, hiszen 1.; nem lehet módosítani a címtár adott példányát helyben, és 2., tartományvezérlő mivolta ellenére van helyi Administrator csoport, azaz lehetséges az AD-n kívüli minden mást üzemeltetni egy nem Domain Admin felhasználói fiókkal.

- Üzemeltetés mentes: nincs AD üzemeltetés, ergo nincs szükség magasabb szaktudású, Domain Admins jogosultsággal rendelkező szakemberre, hiszen nincs semmilyen a tartományhoz, erdőhöz kapcsolódó üzemeltetési feladat.



6.1 ÁBRA LEHET ILYET IS

Folytassuk a RODC megismerését a megoldandó technikai problémákkal, hiszen mivel teljesen új szerepkörről van szó, a garantált működéséhez szükség volt az ismert címtár és címtár támogató megoldások alapos és mélyreható korrekciójára.

A Read-Only címtár adatbázis és a replikáció

A RODC „alatt" működő címtár adatbázis példánynak teljesen ugyanúgy kell kinéznie, mint egy hagyományos DC-nél (a jelszavakat kivéve, de erről majd később), mert különben hogyan megy le a replikáció, azaz hogyan lesz kompatibilis? Viszont változásokat nem tárolhat el, és nem is replikálhat, azokat sem, amelyek esetleg szükségesek. Így aztán az összes változási kérelemnek el kell jutni valahogyan egy írható DC-ig, hogy aztán a hagyományos replikációval visszakerülhessen (ha akarjuk) a RODC címtár példányába. Ez az a plusz kör, amely kizárja a korábbi telephelyi, sima DC esetén egyszerűen bevihető, és esetlegesen az egész erdőt negatívan érintő adatbázis változásokat. Persze például a telephelyi alkalmazások továbbra is kaphatnak egyszerűen hozzáférést a címtár helyi példányához, de csak olvasási joggal. Ha ennél többre van szükség, akkor pl. LDAP-on keresztül továbbkerül a kérés automatikusan a hub site (a központi telephely, vagy ahol egy írható DC van) felé.

> Az ún. „unidirectional" replikáció következménye az a változás is, hogy az írható DC-k a replikációs folyamatban felismerik, hogy a partnerük egy Read-Only szerepkört tartalmaz, és ebben az esetben nem is kezdeményezik a „pull" típust, hiszen nem is jönne, nem is jöhetne semmilyen változás a RODC

irányából. Ez megint csak sávszélesség csökkentést jelent, és egyúttal a hídfő DC-ket sem terheljük annyira. Ide tartozik az is, hogy ez az új, egyoldalas replikáció nemcsak a címtárszolgáltatásoknál jelentkezik, hanem értelemszerűen az ugyanígy használható DFS-R-nél is.

A hitelesítési adatok gyorsítótárazása

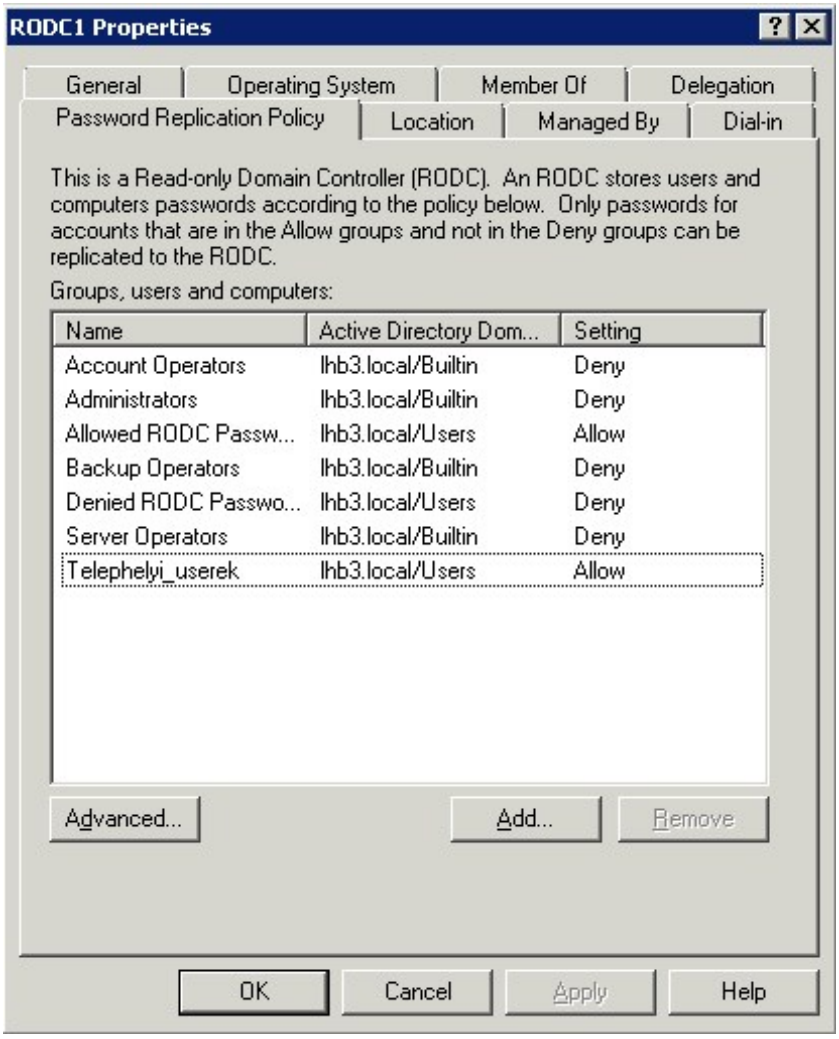
Alapértelmezés szerint a RODC - két kivételtől eltekintve - nem tartalmazza semmilyen felhasználói vagy számítógépfiók jelszavát. E két kivétel az RODC gépfiókja, illetve a speciális szerepet betöltő *krbtgt* fiók. Viszont arra van lehetőségünk, hogy bármely más fiók hitelesítési adatait gyorsítótárazzuk. Miért akarnánk ezt tenni? Egyszerű: ne kelljen „kimenni" az adott hálózatból, az esetlegesen lassú kapcsolaton keresztül egy központi DC-hez mondjuk minden felhasználói belépés vagy egyéb hitelesítés esetén. De hogyan lehetséges az ilyen típusú adat eltárolása és kiszolgálása?

A RODC képes KDC-ként (Key Distribution Center) viselkedni a telephely felhasználói és gépei felé, azaz képes lesz tökéletes és érvényes Kerberos kulcsokat kiadni, melyeket aztán a fiókok teljes körűen használhatnak is a hitelesítési folyamatban - a központi DC-k nélkül is. Viszont már most tudnunk kell, hogy a RODC a TGT kérések aláírásához és titkosításához a saját krbtgt fiókját és annak jelszavát is használhatja, amely nyilván különbözni fog egy központi DC ugyanerre a célra használt krbtgt fiókjának hitelesítési adataitól. A folyamatban e két forrás különbözősége lesz a kulcs.

Szóval, az első alkalommal a hitelesítés biztosan egy központi DC-vel fog csak menni, mert ugye a kliens az alapértelmezés szerint szeretné használni a RODC-t, de ekkor ez még csak *továbbítani* tudja a kérését. Ha ezzel a közvetítéssel sikerül a hitelesítés, akkor a RODC el fogja kérni az adott fiók hitelesítési adatait. Persze, az írható DC csak úgy nem adja oda, hanem - miután felismerte, hogy ez egy RODC kérése -, az ún. *Password Replication Policy* alapján dönti el, hogy szabad-e ezt tennie, vagy sem. A PRP gyakorlatilag egy mini táblázat, amelybe manuálisan kell felvennünk azokat a csoportokat, gép- vagy felhasználói fiókokat, amelyekről úgy ítéljük meg, hogy a hitelesítési adataikat nyugodt szívvel merjük gyorsítótárazni a RODC-n. Alapesetben ez a táblázat teljesen üres, azaz minden fiók és csoport számára tiltott ez a lehetőség. Ha viszont a kérdéses fiók számára engedélyezve van a gyorsítótárazás, akkor a központi DC átnyújtja a megfelelő adatokat a RODC-nek, amely meg szépen letárolja ezeket, majd - most jön a helyi krbtgt fiók szerepe - a saját fiókjával aláírt TGT-t adja oda a kliensnek.

De mi történik a második belépéskor? Merthogy immár van tárolt jelszó helyben is, azaz a RODC képes lenne ellátni a hitelesítést közvetlenül is, de honnan tudja, hogy ezt megteheti? Egyszerű, a RODC képes felfedezni az adott TGT-n a saját krbtgt

fiókjának nyomát, ergo ha megtalálja, akkor automatikusan nem küldi tovább a központi DC felé a kérést, hanem a helyben letárolt adatokkal gyorsan és problémamentesen megoldja a hitelesítést.



6.2 ÁBRA AZ „ALLOW" OSZLOPBAN VAN A LÉNYEG

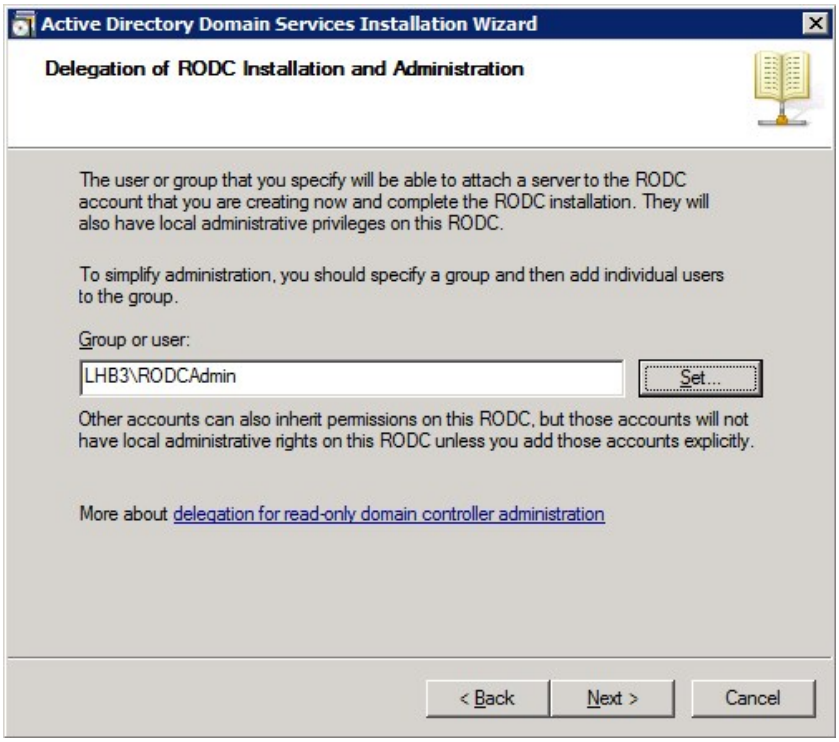
A Password Replication Policy „feltöltése" abszolút a mi döntésünk, mérlegelnünk kell tehát, hogy mely fiókok vagy csoportok azok, amelyek hitelesítési adatai lekerülhetnek a RODC-re. Ha minden a telephelyen használt fiókot engedélyezünk (és esetleg a tartományi admin fiókokat is!), mindig gyors lesz a belépés, viszont ha eltulajdonítják a gépet, hozzáférhetőek a jelszavak, ugyanúgy, mint egy hagyományos DC esetén. Ha csak néhány szimpla felhasználói fiókot engedélyezünk, akkor több idő megy el más fiókok esetén a belépésre, viszont nincs komoly biztonsági probléma.

Az admin jogok szétválasztása

Mint ahogyan már említettem, a RODC-n szükséges és fontos is egy helyi magas szintű jogosultság biztosítása, ami nagyjából a lokális admin jogkörrel egyenlő - anélkül, hogy a címtár objektumaira bármilyen befolyása lenne az ebbe a csoportba tartozó felhasználóknak. Egy ilyen fiók csak egy tartományi fiók lehet (célszerűen az

adott telephely egy felhasználója), és ami még fontos, hogy ha egy másik helyszínen, egy hagyományos tartományvezérlőn lépne be ez a felhasználó, akkor ez ugyanúgy nem fog sikerülni neki, mint mielőtt megkapta volna ezt a lehetőséget a RODC-n, mivel csak azon az egyetlen RODC-n számít adminnak. Egy fiók e csoportba történő belehelyezése egyébként kétféle módon történhet meg:

1) A parancssorból a „Dsmgmt" eszközzel
2) A RODC telepítése során a varázsló egyik lépéseként



6.3 ÁBRA A RODC HELYI ADMIN FIÓKJÁNAK KIJELÖLÉSE, MÉG A TELEPÍTÉS KÖZBEN

Ez egy igazán praktikus lehetőség, mivel így tényleg adhatunk úgy az alkalmazások és a hardver területén admin jogot, hogy a címtárat egy pillanatig sem veszélyeztetjük.

Read-Only DNS

„Ha DC, akkor DNS szerver is". Ezt a tételt a RODC esetén is tudjuk érvényesíteni. A RODC DNS szerver teljes értékű, pl. képes az összes a DNS által használt alkalmazáspartíciók replikálására (pl. a ForestDNSZones, DomainDNSZones) vagy a kliensek maradéktalan névfeloldási kéréseinek kiszolgálására. De… a RODC jellegéből adódóan minden művelet nem történhet meg. Melyek ezek? Nos, ide tartozik pl. a kliensek automatikus regisztrációja a DDNS segítségével, vagy saját maga felvétele pl. egy AD integrált zónába, egy NS rekord alá.

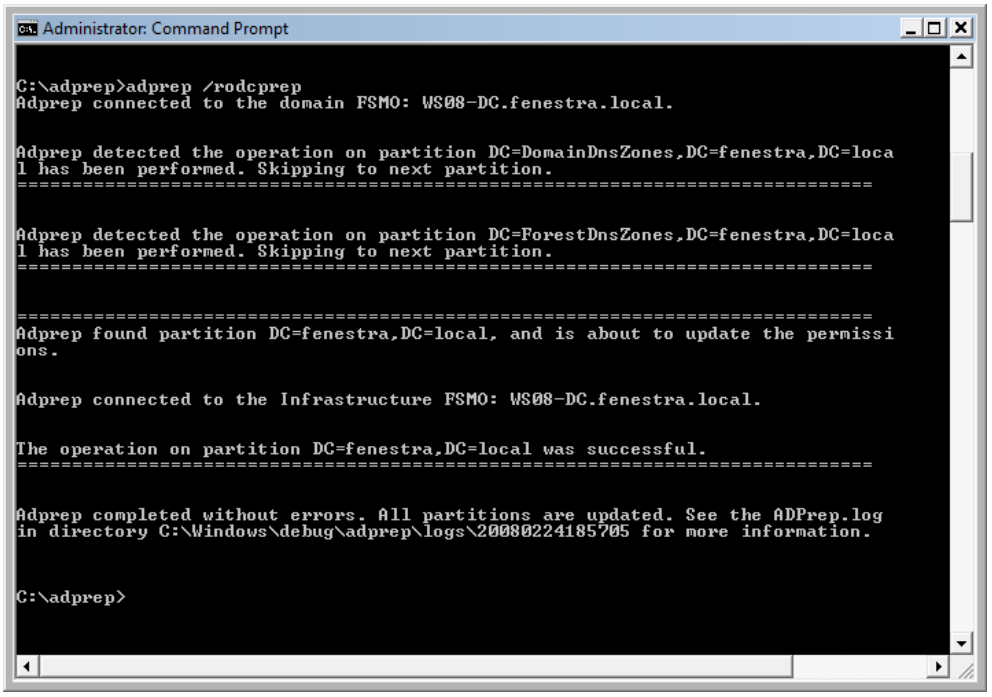
Így aztán, ha egy kliens gép saját rekordja frissítését végezné el, akkor a RODC DNS közli vele, hogy mely DNS szerveren teheti ezt meg, merthogy helyben szó sem lehet róla. Közben azért a - háttérben - megkísérli a megfelelő DNS szerverről lehúzni a kliensre vonatkozó változást azért hogy a következő pillanatban már ki tudja szolgálni

egy másik kérés során ezt a nevet/címet. Fontos az is, hogy szerencsére ez a replikáció csak az adott DNS rekordra vonatkozik, nem kell ezért tehát egy egész zónát „lehúzni” a folyamat során.

A RODC bevezetésének feltételei

Nem kevés „súlyos” elem van ebben a listában, de talán az eddigiek alapján látszik, hogy valóban mélyen bele kellett nyúlni a címtár működésébe a RODC-k bevezetése miatt:

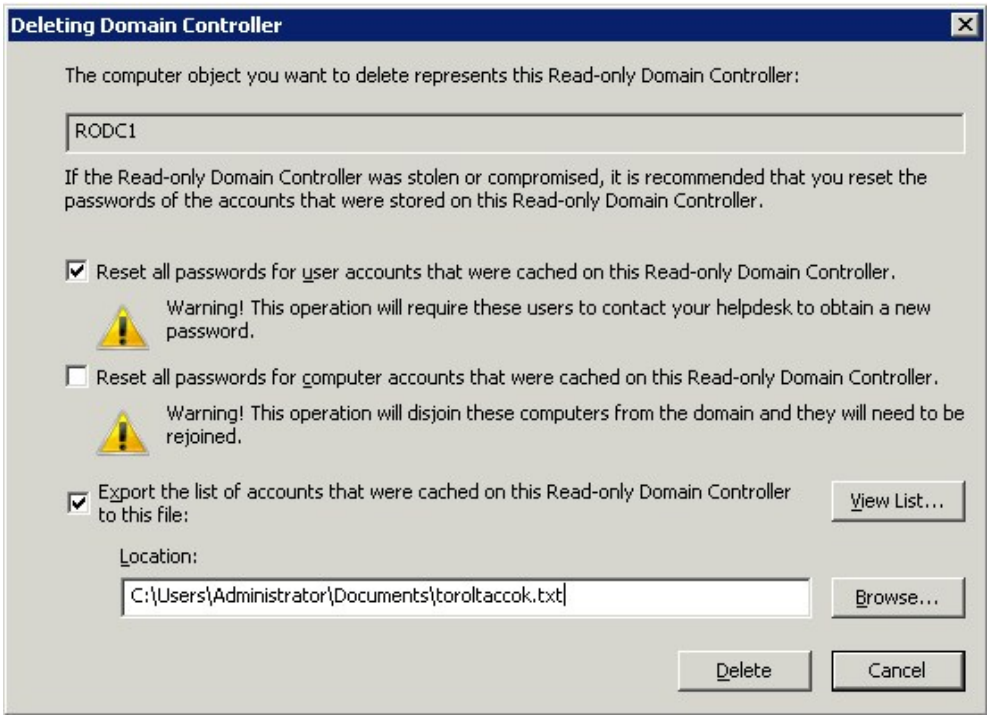
- Legalább egy darab írható Windows Server 2008 DC-nek lennie kell a tartományban. Ez elsősorban a replikációs partnerséghez szükséges.
- Az a DC, amelyhez a RODC a hitelesítési kéréseket intézi majd, csak minimum egy Windows Server 2008 Server lehet, ti. a Password Replication Policy csak az új szerverrel képes működni, illetve felismerni, hogy egy olyan speciális kérésről van szó, amelyet egy RODC adott ki.
- A tartomány működési szintje legalább Windows Server 2003 kell hogy legyen azért, hogy elérhetővé (azaz inkább kikényszeríthetővé) váljon a biztonságos Kerberos delegálás.
- Az erdő működési szintje tekintetében is kötelező a minimum Windows Server 2003-as szint, az ún. „*linked-value*” replikáció használata miatt, amely nagyobb replikációs megbízhatóságot nyújt, illetve lehetővé teszi, hogy ne az adott elemet tartalmazó egész tömb replikálódjon, hanem csak a ténylegesen megváltozott elem.
- A Password Replication Policy használatának alapfeltétele a sémabővítés (lásd később).
- Használnunk kell az Adprep /rodcprep parancsot az erdő szintjén, ami azért szükséges, hogy frissítsük az erdő összes DNS alkalmazáspartícióját, hogy aztán az összes RODC DNS szerver képes legyen (immár a megfelelő jogosultsággal) replikálni ezeket a rekordokat.



6.4 ÁBRA EGY ÚJABB TÍPUSÚ PREPARÁLÁS

A RODC eltávolítása

Ebben a témakörben is van némi praktikus változás, azaz a RODC törlésekor kapunk segítséget ahhoz, hogy gyorsan orvosoljuk az eltulajdonítás vagy valamely drasztikus változás okozta károkat. Egy ilyen esetben a törlés előtt (a következő ábrán jól látható módon) RODC által is tárolt hitelesítési adatokat lenullázhatjuk.



6.5 ÁBRA EGY ÚJABB TÍPUSÚ PREPARÁLÁS

6.1.2 Az újraindítható címtárszolgáltatás

A Windows Server 2008-tól kezdve a tartományvezérlőkön a címtár újraindítható. De miért? És hogyan?

Elsősorban azért, hogy ne kelljen újraindítani a gépet bizonyos esetekben, például a címtárt érintő frissítések vagy éppen az AD karbantartása (pl. offline defrag) apropóján[68]. Meg aztán amíg tart az újraindítás - ami általában, szinte függetlenül a gép teljesítményétől rengeteg idő -, ne essenek ki egyéb, a tartományvezérlőn futó kritikus szolgáltatások, pl. a DHCP szerver „csont nélkül" működik majd tovább. A címtár szervizek leállítása és újraindítása bármelyik új tartományvezérlőn lehetséges, és nincs semmilyen egyéb megkötés sem, azaz az eddigi általános helyzettel szemben szó sincs például arról, hogy ez a lehetőség funkcionalitási szint függő lenne.

> Az újraindítási opció minimális változást hoz a kezelésben, és nincsenek extra opciók sem ezzel kapcsolatban, azaz tényleg csak annyiról van szó, hogy a DC-ken lévő Services MMC-ben megjelenik a listában az Active Directory Domain Services nevű szerviz, amit a szokásos módon lehet kezelni. Az AD ily módon leállított állapotára egy külön, fantázia nélküli kifejezés van, úgy hívják: "AD DS Stopped" üzemmód.

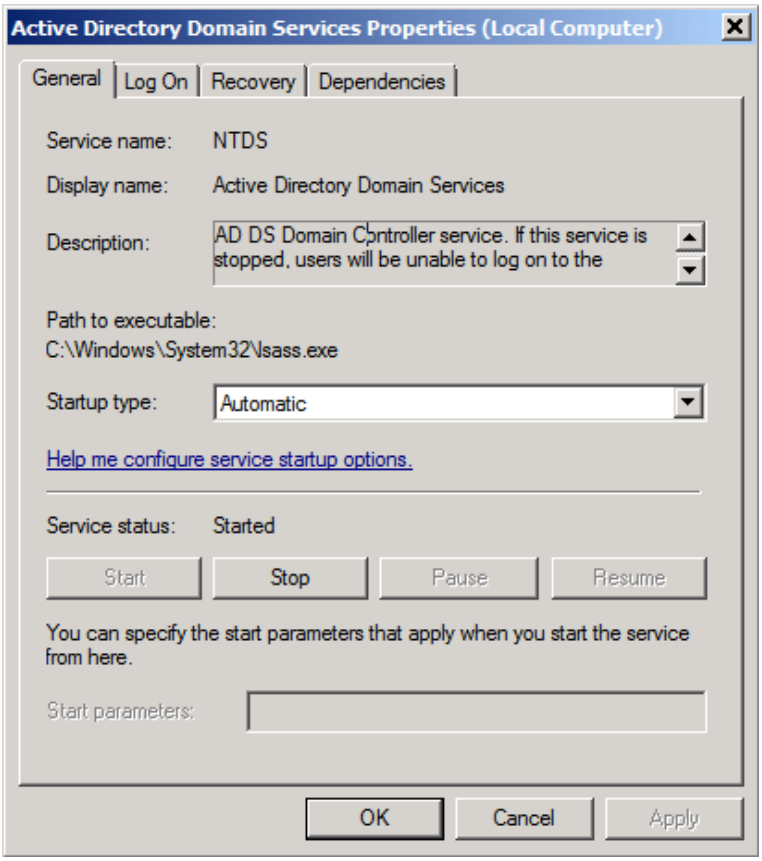
Igazából talán inkább az az érdekes, hogy ilyenkor mi történik a szerverrel a tartományban! Vagy újra lehet használni a helyi felhasználó adatbázist? Na azt azért nem ☺. Tag marad erre az időre egyáltalán a tartományban? Vagy tagkiszolgáló? Vagy egyik sem? Nos, ha egyedül van a tartományban, akkor azt gondolom, logikus, hogy egyik sem. Viszont ha több DC is van, akkor a tartományi tagsága él, és tagkiszolgálóként dolgozik addig is, amíg újra DC nem lesz. Így tehát például az interaktív vagy a hálózaton keresztüli bejelentkezés lehetősége ebben az esetben is adott. Valamennyire akkor is igaz ez, ha nincs elérhető másik DC, mert ekkor a helyi belépéshez a Directory Services Restore Mode jelszót kell használnunk[69].

Sokáig persze nem célszerű azért így hagyni a gépet, hiszen a beléptetés vagy a replikáció természetesen nem működik, az adatbázis (Ntds.dit) offline, és a szerviz leállítása értelemszerűen magával húz a sötétségbe más szolgáltatásokat is (DNS, KDC, FRS, stb.).

---

[68] De például nem egy System State mentés visszaállításra, ez a Microsoft által egyáltalán nem javasolt és támogatott megoldás.

[69] Tudjuk, ez az amit a telepítéskor megadunk, aztán szépen elfelejtjük, hogy aztán ebből óriási gond legyen később, mondjuk egy címtár adatbázis visszaállításkor ☺.



6.6 ÁBRA CSAK EGY SZERVIZ ÉS MÁS SEMMI

6.1.3 TÖBB TARTOMÁNYI JELSZÓ- ÉS KIZÁRÁSI HÁZIREND

Volt egy igazán komoly problémánk a Windows Server 2008 előtti időkben, ti. egy Windows Server 2003 tartományban semmilyen megoldást nem találhatunk az egy tartomány = egy jelszóházirend tétel kikerülésére. Ha valamilyen nyomatékos okból mégis muszáj egy új jelszóházirendet definiálni, akkor csak egyet lehet javasolni: egy új tartományt kell létrehozni, ami persze nem tökéletes megoldás, talán több is a hátránya, mint az előnye. De megszűnt ez a korlát, egy teljesen új módszerrel (*Fine-Grained Password Policy*) kreálhatunk azonos tartományban több jelszóházirendet is, sőt az új házirend kiterjed a fiók kizárási (account lockout) opciókra is.

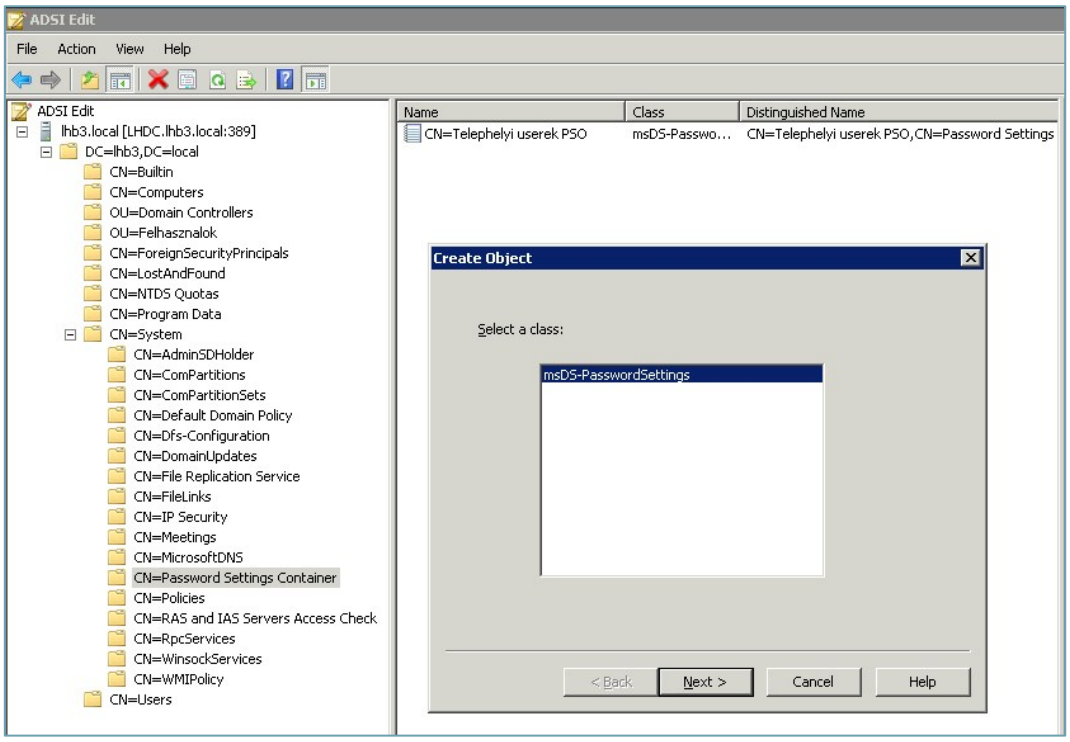
> Miért fontos a több tartományi jelszóházirend? Nos, ez eléggé értelemszerű, hiszen mivel a felhasználói fiókok „súlya” nem azonos, a magas jogosultságú fiókokat jobban kell(ene) védenünk, erősebb jelszavakat lenne célszerű megkövetelnünk azért, hogy az emberi tényező (hanyagság, felületesség, felelőtlenség) által okozott problémákat megelőzzük. Emellett a normál felhasználói fiókok jelszavával kapcsolatban nem minden esetben szükséges kőkemény restrikciókat alkalmazni, nem indokolt az átlagos felhasználókat „kínozni” az extra jelszó megadási kritériumokkal.

Egy alternatív jelszó- és kizárási házirend létrehozásának lépései három pontban foglalhatóak össze:

1. Készítsük el a megfelelő csoportot, és mozgassuk át a megfelelő fiókokat!
2. Készítsük el az új PSO-t (Password Settings Objects), azaz az új jelszóházirendet!
3. Rendeljük hozzá a PSO-t az adott csoport(ok)hoz, vagy akár egyesével a felhasználói fiók(ok)hoz!

Ebből már kiderülhetett, hogy az új jelszóházirendeket csak fiókokhoz vagy globális biztonsági csoportokhoz rendelhetjük. Mi lesz az OU-kkal? Nos, sajnos közvetlenül nem rendelhető hozzá egy PSO egy OU-hoz, ha maradunk ennél a hierarchiánál, akkor muszáj legyártani az „árnyék" biztonsági csoportokat. Ez kissé bonyolítja talán a folyamatot, de gondoljunk bele, mennyi csoportunk van viszont már készen, gyárilag létrehozva (Domain Admins, Enterprise Admins, Schema Admins, Server Operators, Backup Operators, stb.)!

A PSO-k létrehozása egyébként kétféle módon történhet, ADSI Edit-tel (immár beépítve: adsiedit.msc) vagy ldifde-vel. Az első módszer első lépése a következő útvonalon egy új objektum létrehozása itt: *<domain_name>,CN=System,CN=Password Settings, CN=Password Settings Container*

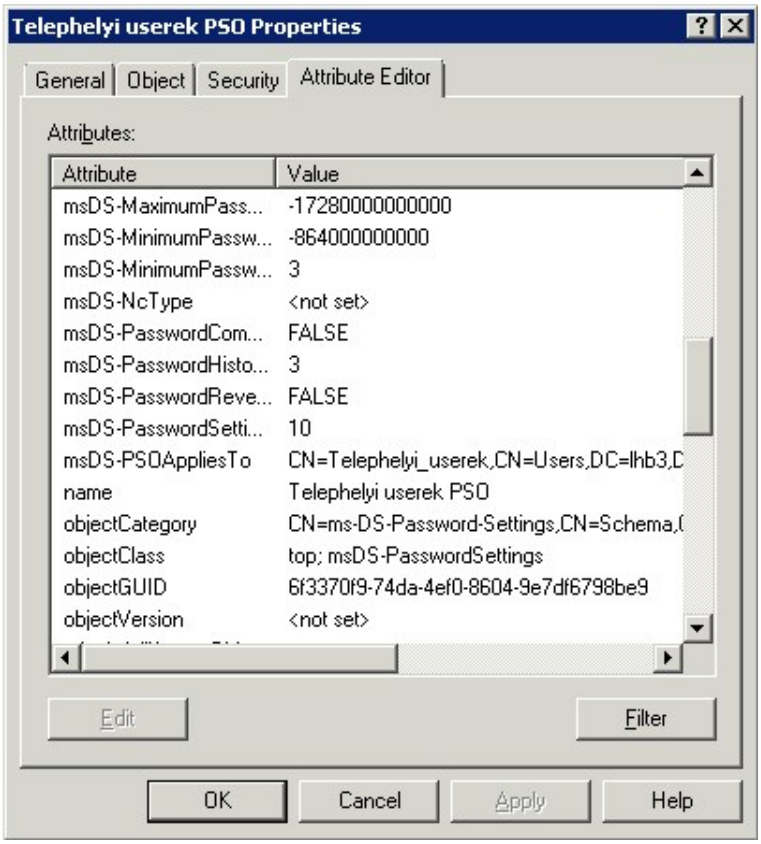


6.7 ÁBRA EGY PSO NEM PSO

Az ezután következő, tíznél is több lépést tartalmazó varázsló beállításai között ráismerhetünk a szokásos jelszó- illetve kizárási házirend opciókra. Időnként kissé

bonyolultabb a mezők kitöltése, pl. csak másodpercben lehetséges értéket megadni, vagy a érvényesítési területet csak a distinguishedName értékkel (CN=,DC=, stb.) lehetséges kijelölni.

Ha a varázslót végiglépkedtük, akkor kész van az új házirend, és már érvényre is jutott. Innentől viszont nem kell az ADSI Edit az esetleges korrekcióhoz, az ADUC-ban a System\Password Settings Container alatt megtaláljuk (feltéve, ha engedélyeztük a „View" alatt a „Advanced" opciót), és szerkeszthetjük az alternatív házirendeket. Hogyan? A szintén teljesen új (és szinte minden objektumnál elérhető) *Attribute Editor* fül segítségével.



6.8 EGY KÉSZ PSO UTÓLAGOS KONFIGURÁCIÓJA AZ ADUC-BÓL

> Itt jegyezném meg, hogy a hivatalos módszer eléggé fárasztó, de sajnos az R2-ben sem változott meg. Valószínűleg épp ezért születtek olyan külső programok, amelyeket a Microsoft nem támogat(hat), viszont kiválóan és nagyon egyszerűen működnek. Egyet be is linkelek: Fine Grain Password Policy Tool 1.0:
> http://itbloggen.se/cs/blogs/chrisse/archive/2009/01/11/fine-grain-password-policy-tool-1-0-2300-0-rtm.aspx

E rész végén jön a feketeleves, azaz a kritériumok és további megjegyzések:

- Először is az egész folyamat csak akkor indítható el, ha az adott tartomány funkcionalitási szintje minimum Windows Server 2008, és megtörtént a sémabővítés is (két teljesen új osztállyal kell kibővíteni a sémát). Ez ugye csak akkor érhető el, ha már likvidáltuk az összes Windows 2000/2003 Server DC-t.
- Csak a Domain Admins csoport tagjai készíthetnek és alkalmazhatnak PSO-kat a fiókokra vagy a csoportokra. Olvasási jogot szabadon delegálhatunk a PSO-ra, de egy viszonylag életszerű példát említve, egy helpdesk-es kolléga nem fogja tudni megváltozatni a jelszóházirendet (van, hogy ez jó hírnek számít ☺).
- Számítógép fiókokra semmilyen körülmények között nem alkalmazhatóak az új jelszó- és kizárási házirendek.
- A testreszabott jelszó filterekkel már szerencsésebbek vagyunk, mert minden további következmény nélkül használhatjuk ezeket továbbra is.

6.1.4 Database Mounting Tool

Ismét egy teljesen új megoldásról van szó, amely – tömören – abban segíti az üzemeltetőket, hogy egyszerűen azonosítsuk azokat a címtár objektumokat, amelyeket így vagy úgy, de töröltünk vagy éppen megváltoztattunk. Visszaállítani ugyan nem fogjuk tudni ezzel a módszerrel[70], de mielőtt nekiesnénk a tényleges visszaállításnak, gyorsan áttekinthetjük, hogy mit kell és mit lehet majd visszahozni. A legfontosabb viszont, hogy ezeket a „pillanatfelvételeket" vagy mentési példányokat anélkül tudjuk megtekinteni, hogy a speciális AD Restore Mode miatt újra kellene indítani a gépet.

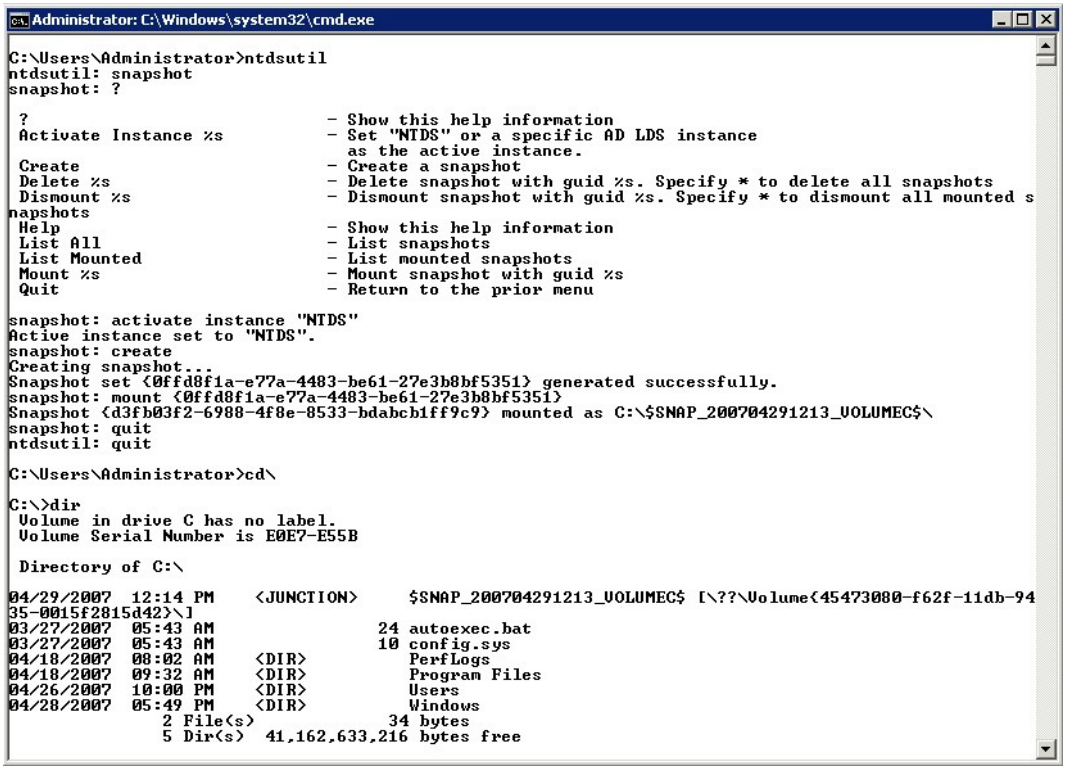
A megvalósítás lépései igényelnek némi szakértelmet és részben parancssorból történnek:

1. Indítsuk az Ntdsutil.exe-t és használjuk az új „snapshot" parancsot, amellyel készíthetünk egy mentést az AD-ról, majd ezt fel is csatolhatjuk a fájlrendszerbe.
2. Egy másik parancssori eszköz jön, a Dsamain.exe (Exchange örökség :D[71]), amivel az adott példányt LDAP szerverként tudjuk futtatni. A szintaxisra vigyázzunk, és persze arra is, hogy a kötelezően mellékelendő 4 port (LDAP, LDAP-SSL, GC, GC-SSL) mindegyike eltérő legyen a szokásostól, azaz bármi lehet, csak ne a szabvány, hiszen a működő AD pont ezeket használja éppen most is.

[70] De nemsokára azzal a módszerrel is megismerkedünk ☺.

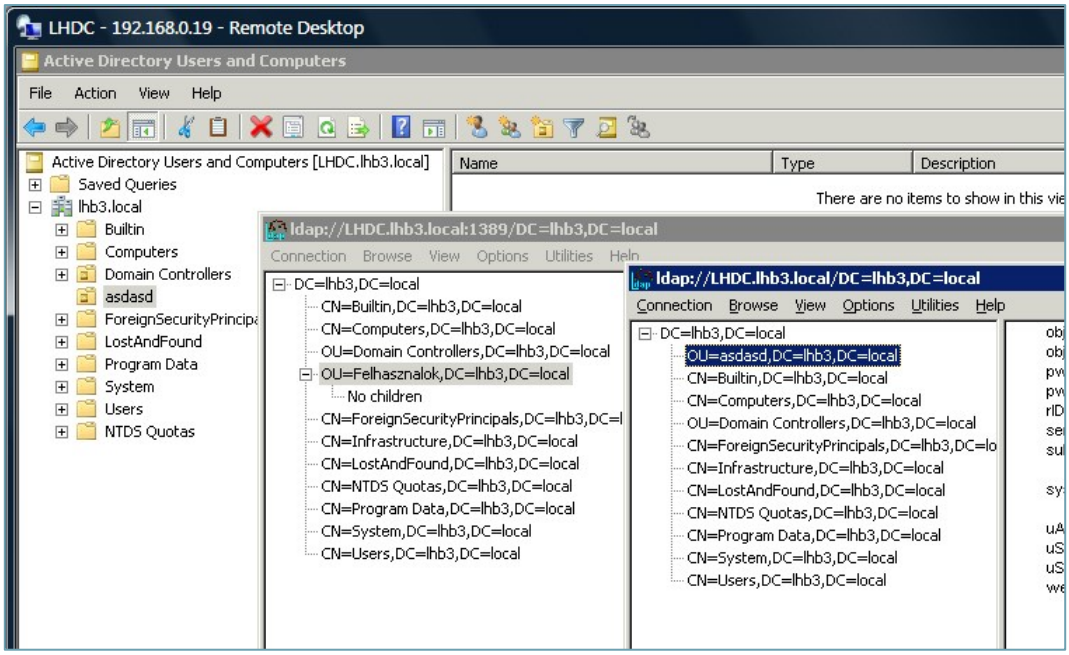
[71] A dsamain.exe az Exchange 5.5 rendszer Directory Service néven futó alkalmazása volt, mely tulajdonképpen az Active Directory ősének tekinthető. Itt tanulta meg az MS, hogyan kell multimaster replikációjú JET adatbázisokat hatékonyan kezelni (a lektor megjegyzése)

3. Futtassuk az ldp.exe-t a szokásos módon, de ne a szokásos porton, az LDAP port az legyen, amit az előbb megadtunk.
4. Kész, immár online tallózhatjuk az előző AD verziót!



6.9 EGY PILLANATFELVÉTEL KÉSZÍTÉSE, MOUNTOLÁSA ÉS KILISTÁZÁSA

5. Ha végeztünk, a Dsamain.exe ablakában állítsuk le az AD mentett példányát a CTRL+C-vel!
6. Az ntdsutil-t úgy is konfigurálhatjuk, hogy rendszeres időközönként megtegye az automatikus pillanatfelvétel készítést, így aztán valóban bármikor belenézhetünk majd a régebbi példányokba is.



6.10 KÉT AD PÉLDÁNY EGYSZERRE ELÉRHETŐ AZ LDP.EXE-VEL, ÉS LÁTSZIK A KÜLÖNBSÉG IS, MIVEL A PILLANATFELVÉTEL KÉSZÍTÉSE UTÁN ÁTNEVEZTEM AZ EGYIK CSOPORTOT

Egyetlen fontos dolog maradt még ezzel az újdonsággal kapcsolatban, amire nagyon oda kell figyelnünk, és ez pedig a biztonság. Alapesetben csak a Domain / Enterprise Admin csoport tagjai tekinthetik meg a pillanatfelvételeket, de sajna bármelyik erdőből! Azaz ha valaki átmásolja a fájlrendszerből a pillanatfelvételt egy másik erdőbe, ahol történetesen Domain Admin, akkor minden további nélkül belenézhet a mi címtárunkba. Ezért ezen példányok biztonságáról feltétlenül érdemes valamilyen egyéb módszerrel külön is gondoskodni.

6.2 A MÁSODIK SZAKASZ: AZ R2

Nem fogyott el a muníció az R2-re sem, újabb és újabb látványos és kevésbé látványos, de praktikus megoldásokat kaptunk a kezünkbe a címtár szolgáltatások területén.

6.2.1 AZ OFFLINE DOMAIN JOIN

Küzdöttél már ADS-sel, WDS-sel, Ghost-tal, newsid-dal, sysprep-pel (a lista szabadon bővíthető) a tartományi beléptetés apropóján? Szeretted volna azt, hogy a kliens OS (akár fizikai, akár virtuális gépekről beszélünk) a legelső indítás után már tartományi tag legyen, mégpedig úgy, hogy a DC a közelben sincs, amikor beléptetted? Akit ezen lehetőségek egyszerű, praktikus megoldása nem villanyoz fel, az ne olvassa tovább ☺. A többieknek viszont szeretném elárulni, hogy a Windows Server 2008 R2-vel, valamint a Windows 7 klienssel (de csak ezzel a kettővel) ez menni fog.

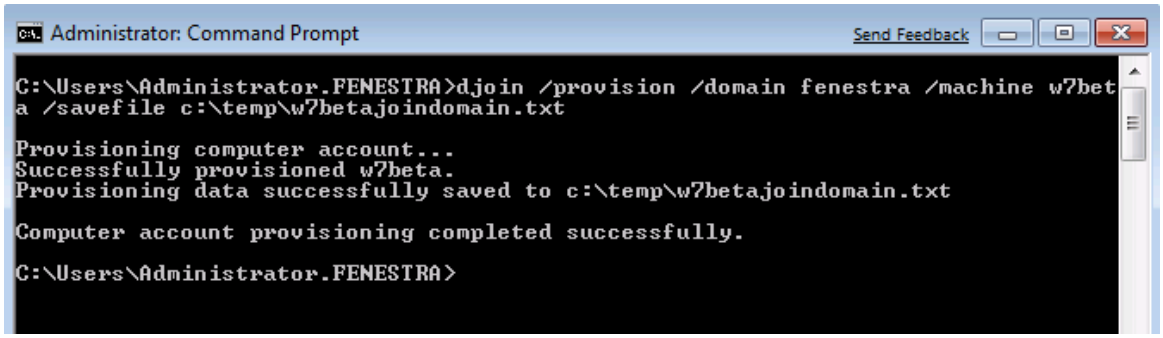
Eddig úgy tudtuk, hogy a tartományba léptetés megköveteli egy megbízható kapcsolat kialakítását a kliens OS és a tartomány, azaz a tartományt ebben az esetben

reprezentáló, a címtár egy példányát hordozó tartományvezérlő között. A beléptetés során egy el nem hagyható, instant változás történik a címtár állapotában, illetve természetesen a másik oldalon a kliensben is, ami nem ment eddig egy aktív hálózati kapcsolat nélkül - ami lehet akár persze egy VPN is[72], de valaminek muszáj lennie...

Nos, az R2-ben már nem, mind a DC, mind a kliens állapotát módosíthatjuk hálózati forgalom nélkül is, illetve teljesen eltérő időpillanatban is. Ráadásul viszonylag egyszerűen. Nézzük a szükséges lépéseket! Most (még) nem egy tömeges telepítési feladatról van szó, hanem mondjuk arról, hogy nálam van otthon a kliens gép, és holnap viszem be a céghez (vagy a központi irodában van, de a telephelyi domainben lesz a helye majd két nap múlva).

1. A folyamat azon részét, amely a gépfiók elkészítéséhez kell, elvégezhetjük egy R2-es DC-n vagy akár egy másik gépen is, amelyen egy Windows 7 vagy egy R2 van, és ami egyben jelenleg is a tartomány része. Akárhogy is, ez a gép lesz az ún. "beléptető" gép, amelyen a spéci parancssori eszközt, a djoin.exe-t használva a következő utasítást kell begépelni:

djoin /provision /domain /machine /savefile akarmi.txt



6.11 ÁBRA SIMÁN MEGY A FELVÉTEL A TARTOMÁNYBA[73]

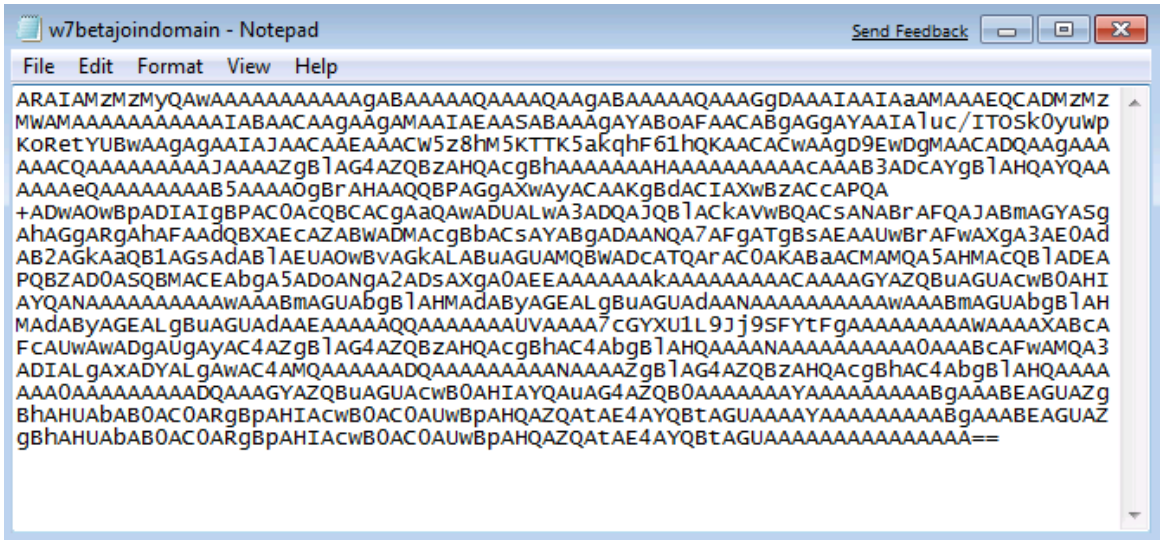
> Természetesen olyan jogosultsággal kell rendelkeznünk, amely lehetővé teszi egyrészt, hogy beléphessünk erre az R2-re adminként, másrészt, hogy beléptethessünk gépeket a tartományba. Ezt a jogkört persze egyrészt delegálhatjuk, másrészt ellenőrizhetjük és korrigálhatjuk a Csoportházirendben, a következő helyen: Computer Configuration > Windows

[72] Nekem pl. számtalanszor kellett már azzal a módszerrel élnem, hogy VPN-en keresztül beléptetem a gépet, majd a domain profil kialakításához lockolom a klienst (a logoff nem jó, mert megszakad a VPN kapcsolat), és ezek után már be tudok a domain userrel lépni, és így legközelebb már van egy cache-elt hitelesítési csomagom, ergo tudom használni a domain userrel a gépet - anélkül, hogy fizikailag eljutottam volna a kb. 85 km-re lévő tartományhoz ☺.

[73] Mondjuk ha valaki csinált már RODC-t, akkor tudja, hogy ez ott már egy varázsló formájában is működik, meg aztán a GUID alapján, általában a brand gépeknél eddig is lehetett felvenni gépfiókot, viszont beléptetni azért egyik esetben sem.

Settings > Security Settings > Local Policies > User Rights Assignment > Add workstations to domain.

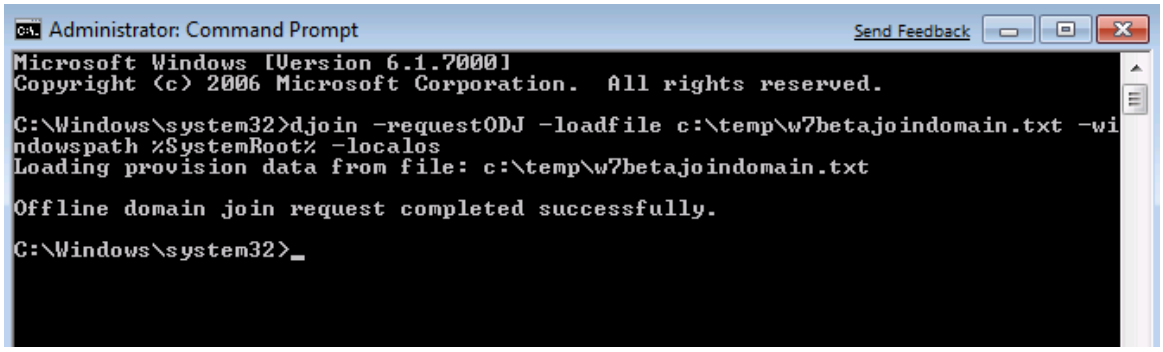
2. Az akarmi.txt-t valahogyan el kell juttatnunk arra a Windows 7 gépre, amelyet ezzel a módszerrel be akarunk léptetni.



6.12 ÁBRA AZ AKTUÁLIS AKARMI.TXT (BASE64 KÓDOLÁSÚ)

3. Használjuk a következő parancsot a leendő kliensen:

   djoin /requestODJ /loadfile akarmi.txt /windowspath %SystemRoot% /localos



6.13 ÁBRA A DJOIN.EXE HASZNÁLATA A KLIENSEN

4. Ezek után amikor a Windows 7 bekerül fizikailag is a tartományi hálózatba, akkor már nincs más dolgunk, csak elindítani, és rögvest használható is lesz, a tartományi felhasználók számára is.

A djoin.exe egy bonyolult "szerkezet", néhány opciót/paramétert az eddigieken kívül is érdemesnek találhatunk egy kis magyarázatra.

- /machineou: a cél szervezeti egység helye, okos dolog, hiszen az alapértelmezett Computers tárolóra nem hat a GP, így viszont egyrészt rögvest

a helyére kerül a gépfiók, másrészt az első belépéskor magára húzhatja a szükséges csoportházirend opciókat is.[74]

- /dcname: megmondhatjuk, hogy melyik DC-n szülessen meg a fiók, ha nem mondjuk meg, akkor a szokásos módon a DC Locator processz dönt.
- /downlevel: ha a cél DC a WS08R2-nél korábbi OS-t tartalmaz.
- /reuse: egy létező fiók újrahasznosítása, a fiók jelszava egyúttal törlődik.
- /nosearch: nincs a fióknevekkel kapcsolatos konfliktus detektálás, amit megadunk, az "létre lesz hozva", ellenben kell hozzá a /dcname paraméter.

Amennyiben viszont a tömeges telepítés a cél pl. a WSIM (Windows System Image Manager) használatával, és a célunk az, hogy a csendes telepítés része legyen az offline beléptetés, akkor az Unattend.xml-be kell belevinni a szükséges infót, méghozzá egy új szekcióba, merthogy a W7/WS08R2 számára használható Unattend.xml természetesen erre fel van készítve:

```
<Component>
 <Component name=Microsoft-Windows-UnattendedJoin>
    <Identification>
       <Provisioning>
          <AccountData>Base64Encoded Blob</AccountData>
       </Provisioning>
    </Identification>
</Component>
```

6.2.2 AD Administrative Center

Egy új, multi-domain/forest címtár kezelő és lekérdező felületről esik most egy kevés szó. Természetesen ez is Powershell alapú, és a rengeteget alkalmazott AD Users and Computer MMC-re hasonlít talán a legjobban, de a gyakorlat azt mutatja, hogy inkább párhuzamosan használjuk a klasszikus eszközzel együtt.

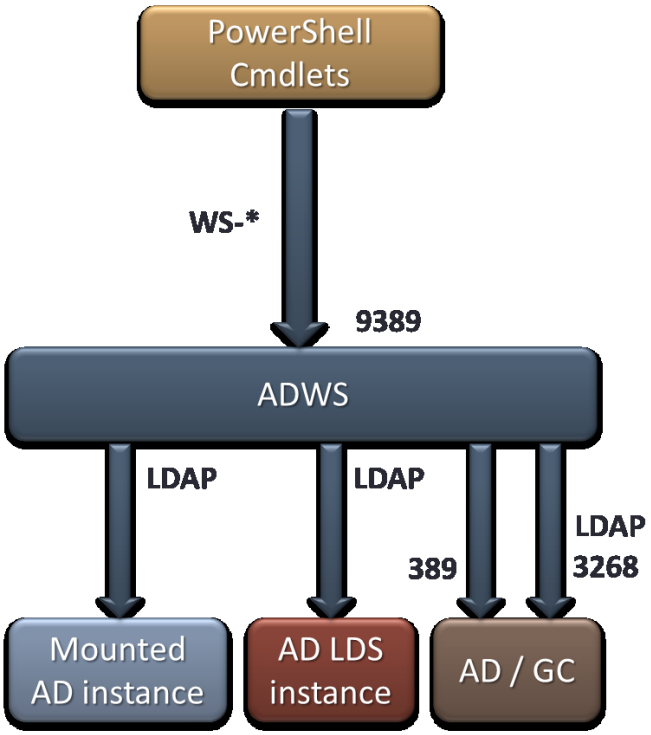
[74] Ilyet (azaz a beléptetett gép alapértelmezett helyének átirányítását) már eddig is csinálhattunk a *redircmp* paranccsal, de így összekötve az ODJ-vel még jobb.

Administrative Task	DSAC.exe	Dsa.msc
Create new user	Supported	Supported
Create new group	Supported	Supported
Create new OU	Supported	Supported
Modify existing user	Supported	Supported
Modify existing group	Supported	Supported
Modify existing OU	Supported	Supported
Reset user password	Supported	Supported
Copy user	Not Supported	Supported
Copy group	Not Supported	Supported
Search for objects	Supported	Supported
Filter objects based on attributes	Supported	Not Supported
Modify domain/forest functional levels	Supported	Supported

6.14 ÁBRA HASONLÓSÁGOK ÉS KÜLÖNBSÉGEK

No és az is fontos, hogy ez az eszköz az R2-ben jelent meg először, bár az is igaz, hogy a hatását kiterjeszthetjük. Ugyanis a szolgáltatás másik alapja az Active Directory Web Services, azaz a címtár elérése egy webszolgáltatáson keresztül, de rögtön jelzem, hogy még gondolatban se keverjük be ide az IIS-t, kivételesen[75] ez a rész teljesen önállóan működik, a TCP 9389-es porton. És ez az a pont, ahol az előbb említett kiterjesztéshez kapcsolódunk, ugyanis Active Directory Management Gateway Services [76] néven letölthető és feltelepíthető korábbi operációs rendszerekre is (Windows Server 2003 és 2008), és így egy R2-ről képesek leszünk elérni a régebbi tartományokat és erdőket is.

[75] Itt most arra gondolok, hogy az Exchange-től kezdve az RDS-ig minden webes szolgáltatás IIS virtuális mappákon keresztül működik.
[76] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2852

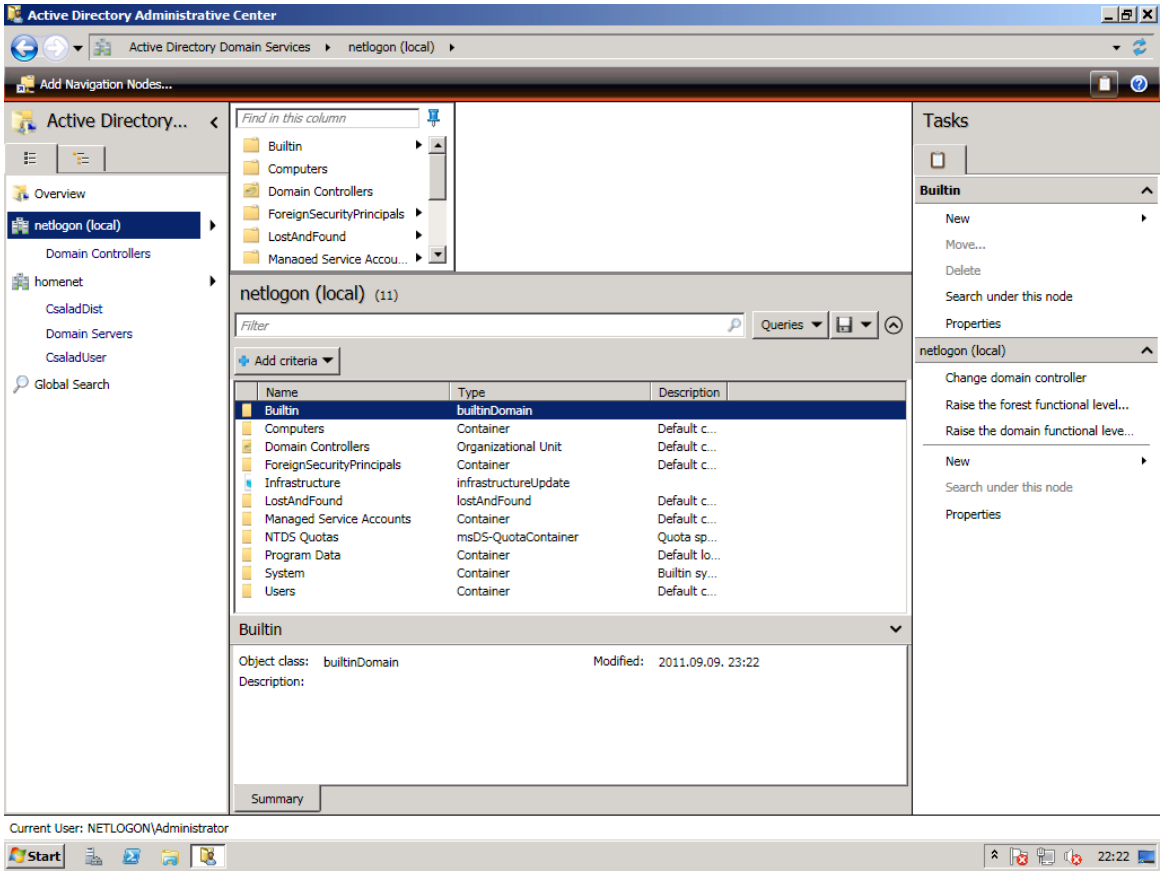


6.15 ÁBRA AD ÉS AD LDS ELÉRÉS EGYFORMÁN IS LEHETSÉGES AZ ADWS-SEL

Persze ezeken az ADAC-ot futtatni nem fogjuk tudni, de kliensként működni képesek lesznek. De ez határozottan egy olyan tulajdonság, amelyet az ADUC-szel soha nem tudtunk megoldani, azaz a több tartomány és erdő objektumainak egyetlen helyről történő kezelését.

Emellett a szűrés és keresés területén igen komoly fejlesztések történtek, valamint a nézetek elmentése is lehetővé vált. De pár hátrányról is szólnék, mert azért így korrekt:

- Nem bővíthető a klasszikus módon , pl. az acctinfo.dll vagy acctinfo2.dll bővítményekre célzok
- Nincs drag & drop
- Nincs RSOP Planning / Logging támogatás
- NTDS Settings sincs



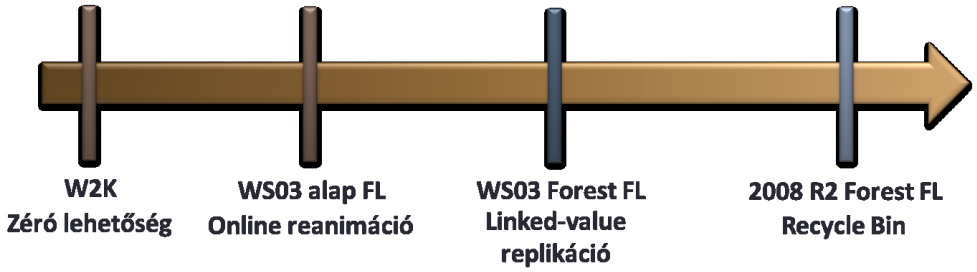
6.16 ÁBRA ÍGY NÉZ KI AZ ADAC FELÜLETE, CSILIVILI, ÉS ÉPPEN KÉT ERDŐM IS VAN BENNE

6.2.3 AD LOMTÁR

Az AD Recycle Bin csodálatos dolog, mivel egy olyan problémát old meg, amire nincs egyébként rendes megoldás: a humán erőforrás problémát ☺, ami állandó és állandóan megújulni képes. Ezzel szemben az AD RB lehetővé teszi bármilyen törölt AD objektum online, azonnali és *teljes körű* visszaállítását. Az AD RB jóval többet ér, mint az eddigi módszerek, mivel:

- A sírkövezést (és a reanimációt) elfelejthetjük
- Nem szükséges egy törlés miatt az offline AD állapot
- Nemcsak egy részleges visszaállítást tudunk megtenni

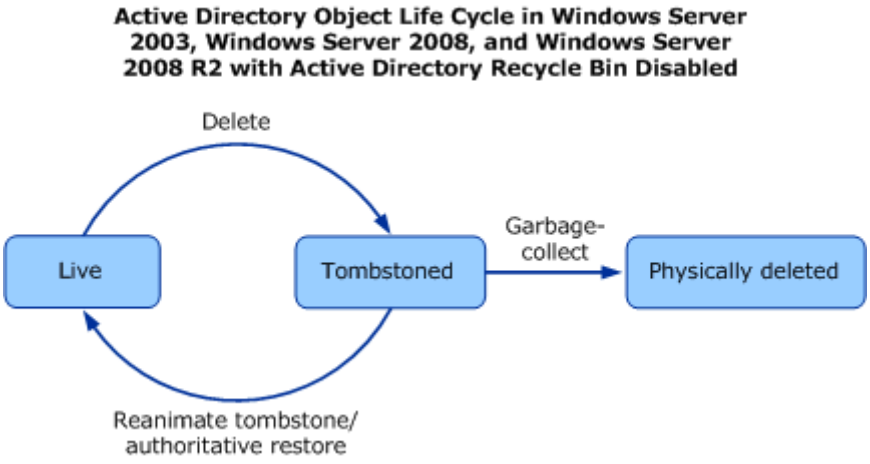
Szóval az nem meglepetés, hogy a statisztikák szerint a humán erőforrás által elkövetett hibák adják a címtárproblémák jelentős részét (is). Ezek közül magasra kiemelkedik a törlés, mint visszavonhatatlan művelet. Valóban visszavonhatatlan, mert bár ha rendelkezünk megfelelő mentéssel (újabb humán erőforrás kérdés :D), megoldhatjuk a problémát, van Directory Services Restore Mode, van ntdsutil, van autoritatív módszer és egyéb trükkök is, amellyel visszahozhatóak a törölt objektumok, de ez mindenképpen működéskieséssel jár, és nem is válhat be mindig - hiszen több külső tényezőtől is függ a sikeressége.



6.17 ÁBRA AZ EVOLÚCIÓS FOLYAMAT, FL = MŰKÖDÉSI SZINT

> A Windows Server 2008-ban már volt próbálkozás a grafikus felületen a nem szándékos törlés visszaszorítására is, pl. ha egy OU létrehozásakor bekapcsolva hagytuk az újdonságnak számító "*Protect contanier from accidental deletion*" opciót, akkor csak körülményesen, a szokásos egyszerű törlés helyett minimum 3-4 plusz kattintással és csak a speciális nézetet bekapcsolva lehetett visszaállítani a szimpla törlés lehetőségét. De ez csak kiegészítő, elkerülő megoldás, és pl. a már meglévő objektumoknál vagy a user fiókoknál nincs is ilyen, illetve pl. a szkriptből törlés ellen sem véd.

Szó volt viszont korábban arról, hogy előbb-utóbb lesz változás ezen a téren is, és jelentem az R2-vel eljött ez a változás, és - kitűnően működik. Nézzük meg lépésről lépésre, hogy hogyan, illetve először azt, hogy mi van a háttérben, valamint azt, hogy mely kritériumok teljesülése után lesz lehetőség egy objektum online visszaállítására az AD Lomtárból!

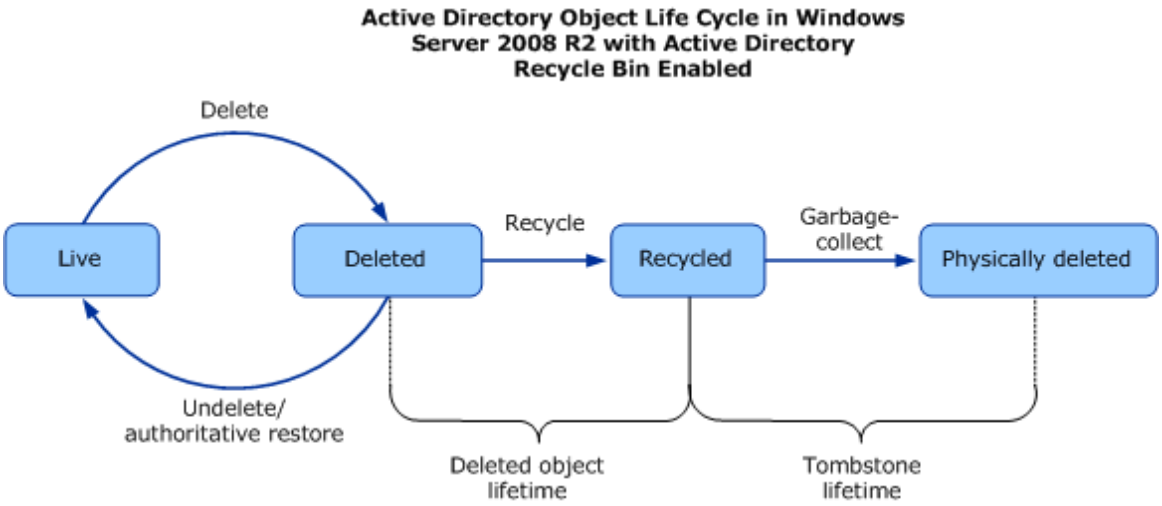


6.18 ÁBRA ELEDDIG ÍGY MENT

A működés változásait legjobban az előző és a következő ábrával tudom szemléltetni, plusz azzal az infóköteggel, ami ezután jön. Az alapállás az, hogy eddig egy címtár objektum törlés szintén nem teljesen végleges (fizikai) törlést jelentett rögtön az általunk felszabadultan elvégzett, megerősítő "Yes" gomb után, hanem egy "sírkővé" (tombstone) átalakulást illetve még jobb, ha úgy képzeljük el, hogy az objektum

dalolva befekszik a marha nagy sírkő alá, de még a felszínen :), eltemetve viszont még nem lesz.

Ez együtt jár pl. a "Deleted Objects" tárolóba bekerüléssel, illetve többek között pl. az objektum "isDeleted" attribútumának "TRUE"-re billenésével (merthogy nehogy még egyszer törölni tudjuk az általunk nem kedvelt user fiókját :D), azonban a szimpla visszaállításra mégsincs ilyenkor mód - csak mentésből, és csak a DSRM-ben. Ez azért van így, mivel az adott objektumhoz tartozó DN (distinguished name, tudjuk, OU=,DC=, stb.) meggyalázásra került (az RDN + a "\0ADEL: " lett a helyes kis DN-jéből), a legtöbb ún. non-link-valued attribútum lenullázódott, a link-valued attribútumok (pl. egy user csoporttagsága) pedig tényleg fizikai törlésre került.



6.19 ÁBRA VAN VÁLTOZÁS BŐVEN

A "*sírkövem már van, de még csak alatta fekszem...*" állapot alapesetben 180 napig volt élvezhető. Ezalatt is kaptunk azért egy apró visszaállítási lehetőséget a kezünkbe, páratlan képzavarral én ezt a "*a zombi, aki kibújt a sírkő alól*" névvel illetném, amúgy "tombstone reanimation" a becsületes neve, ami egyrészt alapesetben szintén egy offline művelet (illetve a Sysinternals segédprogramja[77] révén nem is), másrészt a fentiek miatt nem is lehet teljesen sikeres eljárás, ergo tényleg csak a mentésből visszatöltés lehet korrekt.

Viszont ha békén hagytuk az objektumot, akkor jöhetett végre az automatikus, végleges fizikai törlés, azaz a sírkő elporladt (ami végeredményben jó, mert azért az AD a sírkőre 41 db különböző attribútumot szorgosan felfirkált, tehát megtartott), az objektum meg a föld alá került, a végleges helyére. Uff.

Nos, ebbe a folyamatba került be az R2-ben a Lomtár, közvetlenül a "sírköves" állapot elé, ahogyan az előző ábrából ez szépen ki is derül. A változás pedig abban

[77] AdRestore 1.1.: http://technet.microsoft.com/en-us/sysinternals/bb963906

jelentkezik, hogy linked- és non-linked value attribútumok csak logikai törlésre kerülnek az R2-ben. Következő kérdés: meddig? Egyszerű, ha már bekapcsoltuk a Lomtárat, akkor alapesetben ez az érték is 180 nap. Ha viszont megnézzük az *msDS-deletedObjectLifetime* attribútumot, akkor azt látjuk, hogy az értéke 0 :). De higgyük el, ez 180 napot jelent, mivel - ugyanúgy mint a tombstoneLifetime-nál - ha 0, akkor az valójában 180 nap. De ha bármelyiket megváltoztatjuk, akkor onnantól az az érték számít, és - természetesen - nem is hatnak egymásra többé. Egyszerű? ☺

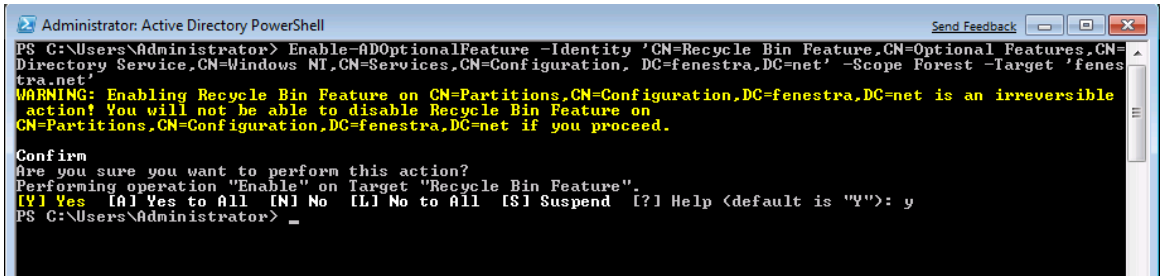
> Még egy dolog. Ha majd bekapcsoljuk, akkor a korábbi összes törölt objektum (amelyek az aktuális sírkövek alatt fekszenek) eltűnik a "Deleted Objects" konténerből, de nem-nem, kedves optimista Olvasó, nem az új csilivili Lomtárba kerülnek be, hanem egyszeriben köddé válnak, azaz ekkor már csak az autoritatív restore segíthet rajtuk.

Nademostmáraztán kapcsoljuk be ezt a *dzsuvás* Lomtárat, ennyi felvezetés után már tényleg megérdemeljük :). Merthogy alapértelmezés szerint az R2 címtárban a Lomtár letiltott.

Kétféle módon kapcsolhatjuk be: vagy az AD Powershellt (Administrative Tools) adminként indítva, vagy az ldp.exe-vel. De még előtte van két fontos teendőnk: egyrészt át kell kapcsolni az erdő/tartomány működési szintjét a legfrissebbre, azaz az R2-esre (erről még rengeteg szó lesz ezután). A másik teendő: az előléptetés előtt természetesen preparálnunk kell a sémát (erről is beszélünk még).

Amit még fontos tudni, hogy - jelen állás szerint - ha egyszer bekapcsoljuk a Lomtárat, akkor vissza nem fogjuk tudni kapcsolni. Ez, akárhogyan is gondolkozom, nekem ez nem tűnik problémának, de a "*...jöhet még a kutyára úthenger*" elv alapján érdemes megjegyezni ezt is.

És akkor kezdődhet a képes beszámoló.

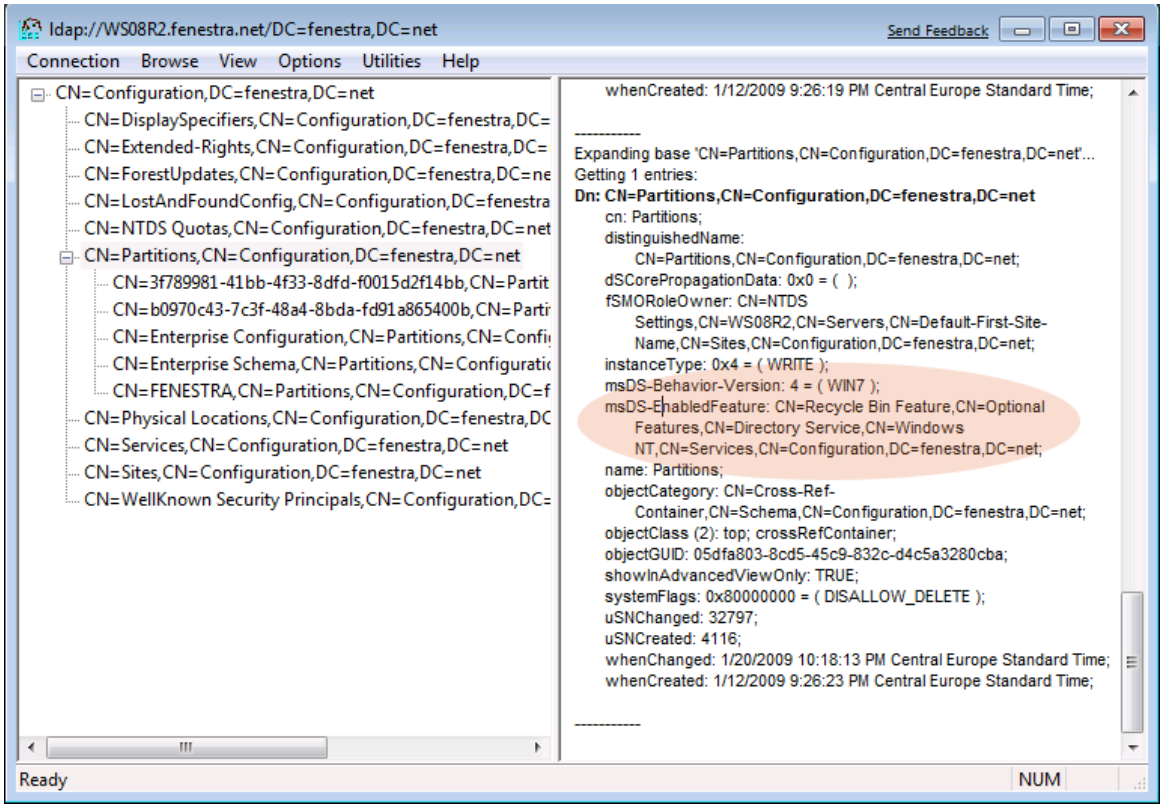


6.20 ÁBRA AZ AD PS PARANCSSOR JÓVAL HATÉKONYABB, MINT AZ LDP.EXE

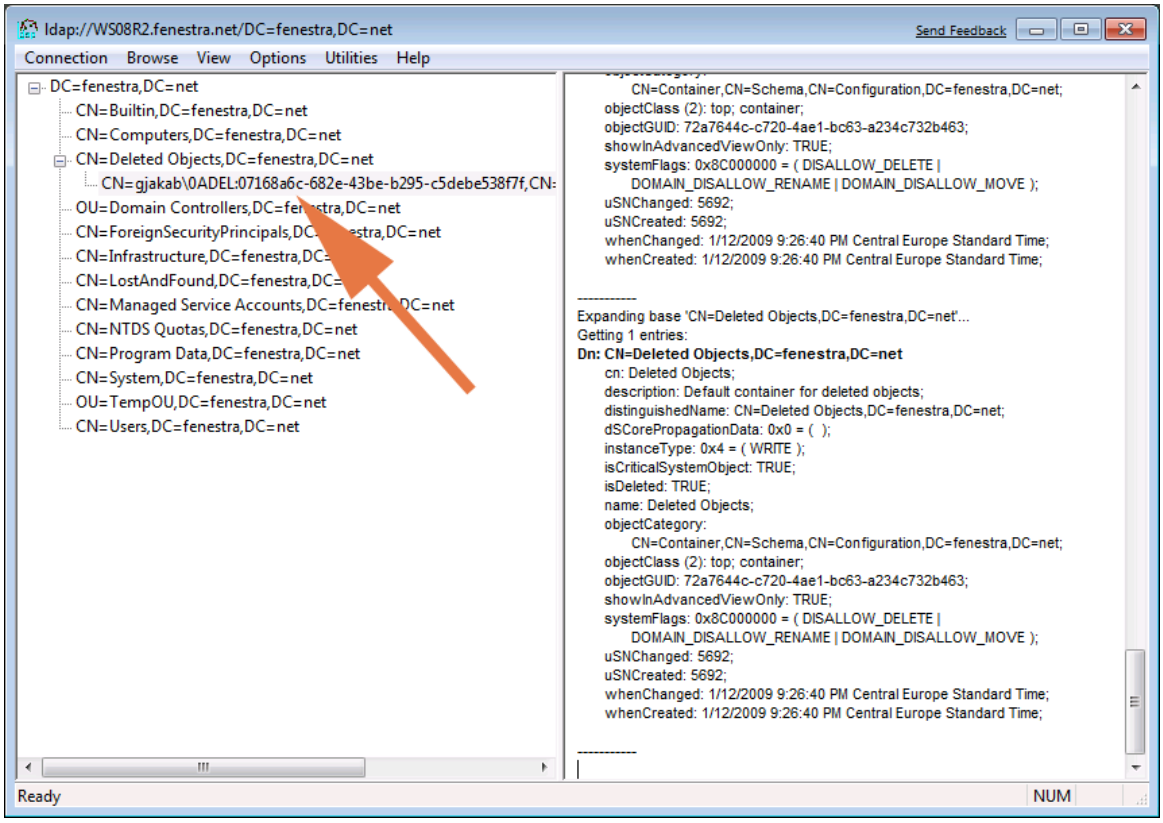
Az AD RB engedélyezés parancsa pl. a netlogon.priv tartományban a következő:

Enable-ADOptionalFeature –Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=netlogon,DC=priv' –Scope ForestOrConfigurationSet –Target 'netlogon.priv'

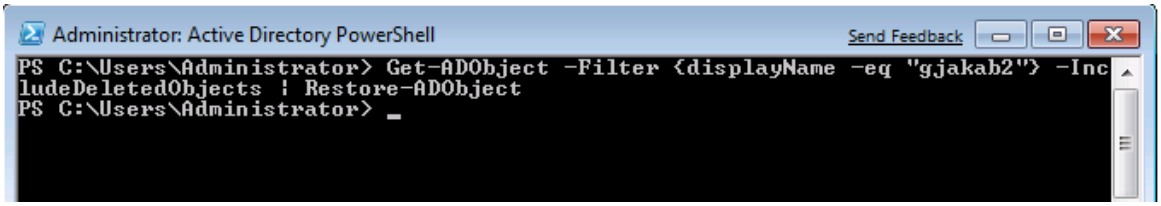
Jelzem, hogy a sortörések ellenére ez egy darab parancs, és a kimenete az előző képen látható.



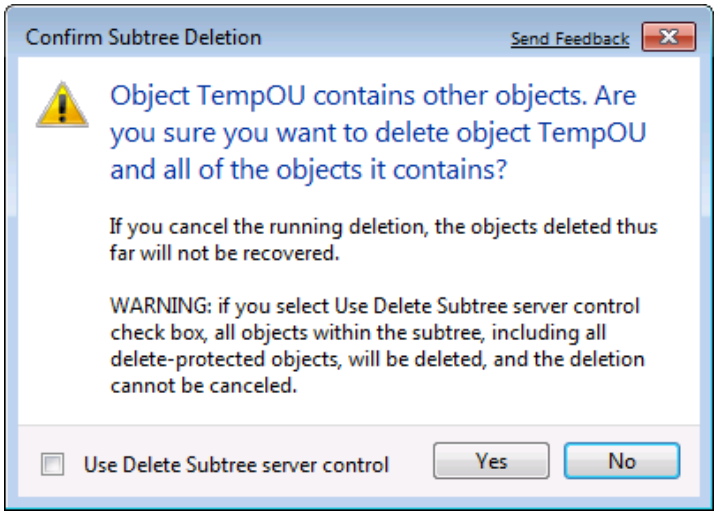
6.21 VISZONT AZ LDP-VEL LÁTVÁNYOSABBAN ELLENŐRIZHETŐ, HOGY TÉNYLEG BEKAPCSOLTUK-E



6.22 ÁBRA VALAMINT AZ IS LÁTSZIK, HOGY GJAKAB-UNK JELENLEG TÖRÖLT ÁLLAPOTBAN LELEDZIK, A DN-JE ENNEK MEGFELELŐEN ELÉGGÉ CSOFFADT



6.23 ÁBRA DE MÁR KÉSZ IS A VISSZAÁLLÍTÁS (GJAKAB2-VEL) ÉS A PS-SEL. UGYE NEM AZT KÉPZELTÜK, HOGY KAPUNK EGY AD LOMTÁR IKONT??? :D)



6.24 ÁBRA AZ OU TÖRLÉS BONYOLULTABBÁ VÁLT, ÉS LÁTHATÓAN FEL VAN KÉSZÍTVE A LOMTÁRAS IDŐKRE

Még néhány tudnivaló és ajánlás:

- Group Policy, Exchange objektumokra nem támogatott ez a módszer (de a reanimation + restore sem)
- Van viszont direkt törlés is
    - Get-ADObject –Filter {<suitable filter>} –IncludeDeletedObjects | Remove-ADObject
- Számítsunk a DIT, azaz az AD adatbázis növekedésre, kb. 10-15%-kal
- Természetesen AD LDS-ben is működik, csak kicsit máshogy kell bekapcsolni, és ha minden példány WS08 R2-on fut (és persze sémabővítés is kell itt is, LDIFDE > MS-ADAM-Upgrade-2.LDF)

De mint ahogy az előző képeken látható, a visszaállításhoz is szintén az AD PS-re vagy az ldp.exe-re van szükség. Én az előbbit javaslom, egyszerűbb. És az élet is az lesz, ha uralmunk alá hajtjuk az AD lomtárat. Hajrá!

6.2.4 Kisebb mutatványok (MSA, AMA, DSRM PS)

A Managed Service Accounts (MSA)

Mit teszünk, ha egy alkalmazásnak vagy egy kiszolgáló szoftvernek egy dedikált felhasználói fiókra van szüksége? Hát létrehozunk egyet, régen ez nagy divat volt (egy Exchange 5.5-nél például kötelező volt, de ma is megmaradt ez az ajánlás, pl. a Forefront Identity Manager-nél). Viszont egy ilyen fiktív fiókra nem figyel senki, ergo vagy azt mondjuk, hogy pl. a jelszóházirend nem fog vonatkozni rá, vagy kézzel variáljuk a jelszavát, pl. 42 naponként. Az első biztonsági szempontból nincs rendben, a másodikat pedig úgyis el fogjuk felejteni, és akkor majd nem indul az alkalmazás, és pont akkor fogunk majd nyaralni, és stb. és stb., szóval ez szintén nem megoldás.

De az MSA megoldja. Ez egy teljesen új objektum osztályt jelent a címtárban, és gyakorlatilag az adott számítógépfiók „gyermekének” számít. És ami a legfontosabb: a jelszava nem függ sem a szimpla, sem a FGPP jelszóházirendtől, hanem a gépfiók jelszavával párhuzamosan változik, alapértelmezés szerint 30 naponta, de ez szabályozható, na mivel? Hát a Csoportházirenddel! ☺

Egyébként 240 karakteres jelszavakkal dolgozik, és muszáj, akkor a *Reset-ADServiceAccountPassword* cmdlet-tel nullázható. A fiók létrehozása a

New-ADServiceAccount –Name {MSA name} –Path {directory path}

Hozzárendelése a szerverhez:

Add-ADServiceAccount –Identity {FQDN} -ServiceAccount {MSA}

„Telepítése” a helyi szerveren:

Install-ADServiceAccount –Identity {MSA}

Ezután már csak a fiókot használó alkalmazás beállítására kell sort kerítenünk.

De azért itt is vannak korlátok:

- Egy MSA = egy szerver, ergo nem megosztható pl. egy a tartományban, vagy például akkor, ha az alkalmazás egy klaszterben több node-on is működik
- Csak Windows 7 vagy Windows Server 2008 R2 esetén használható
- A teljes SPN kezelés csak az R2-es tartomány működési szinttől elérhető, de az egyszerűbb SPN műveletek, mint pl. a delegálás más adminok számára azért már korábban is

Authentication Mechanism Assurance (AMA)
A magyarázat tömören: egy multifaktoros [78] bejelentkezéssel több jogunk lehet például egy fájlmegosztáson. Tekintsünk bele egy kicsit az alkalmazásának a folyamatába:

- Az admin csoportokat linkel a smartcard házirendek alapján
- Ha egy speciális OID van a user SmartCard-ján akkor, amikor belép, kap egy másik SID-et
- Így aztán változik az Access token, és így más biztonsági csoportba kerül
- Hozzáfér erősebb jogokkal is az adott megosztáshoz
- DE ha a smartcard nélkül lép be (pl. egy usernév/jelszó párossal), akkor nem

Feltételek:

- Csak R2 erdő működési szint és csak Kerberos hitelesítés
- A szükséges szkriptek (set-IssuancePolicyToGroupLink.ps1, get-IssuancePolicy.ps1) letölthetőek. [79]

Directory Services Restore Mode Password Reset
Messziről kezdjük.
Minden DC-n az előléptetés közben (lásd 6. ábra) megadunk egy jelszót azért, hogy a helyi felhasználói adatbázis híján is legyen azért egy-egy admin jelszavunk, például a címtár visszaállításához, amikor is úgysem megy a címtár – mivel ha menne, nem tudnánk visszaállítani.

[78] Olyan hitelesítés megoldás, amikor több módszert használunk egyszerre, pl. egy felhasználói név + jelszó, plusz egy OTP (One Time Password) vagy SecureID hardveres eszköz hatjegyű számkódja, vagy pl. egy smartcardon lévő tanúsítvány + a PIN kód.
[79] http://technet.microsoft.com/en-us/library/dd378897%28WS.10%29.aspx

Amikor nem megy a címtár, az a Directory Services Restore üzemmód (F8 a boot folyamat közben, majd a menüpont). Szóval ez egy kritikus dolog, mert ugyan mi adjuk meg ezt a jelszót, de ez nem azonos az esetleg nap mint nap használt Administrator fiók jelszavával. Nem bizony.

Ezt a jelszót aztán a saját érdekünkben rendszeresen változtatjuk, a jelszóházirend hat is rá, de közben szépen elfeledkezünk a DSRM jelszóról. Évek múlva, mikor összedől a címtár az adott gépen, és vissza szeretnénk állítani, akkor jön a pánik, elfelejtettük a telepítéskor megadott jelszót, ergo nem tudunk belépni a DSRM módba, ergo nincs visszaállítás, pedig kecskét is áldoztunk éjfélkor egy *echte* német nemesacél tőrrel.
De hiába.

A megoldásra több módszer is van. Soroljuk fel:

- Nem felejtjük el (de nem írom le hogy leírjuk, mert jelszót nem írunk le sose ☺)
- Amikor még megy a címtár az ntdsutil-lal, admin jogosultsággal megváltoztatjuk ezt a jelszót
- Amikor még megy a címtár, egy új ntdsutil kapcsolóval szinkronizáljuk egy tetszőleges tartományi felhasználóhoz (nyilván nem Gizikéjéhez a titkárságról)

Megkötések (restrikciók):

- Csak Windows Server 2008 és R2 esetén
- EGYSZERI művelet, amely azonnal átmásolja a jelszót
- Nem tartományi, csak helyi (az ntdsutil blokkol különben)

A parancs pedig konkrétan így néz ki:

ntdsutil "Set DSRM Password" "Sync from domain account <suitable user> " q q

6.3 A terep előkészítése

6.3.1 A sémafrissítés

Egy új Windows szerver változattal tipikusan együtt jár a címtárszolgáltatás változása, a különböző kisebb-nagyobb újdonságok megjelenése is. Ezek - ahogy láttuk az előző oldalakon - általában kényelmes és kellemes változások, de ez előkészítés, a tartomány és/vagy az erdő felkészítése a legtöbb esetben azért némi terhet is jelenthet (még ha általában édeset is).
Ha másért nem, akkor azért mivel egy alapos áttekintést és mérlegelést követel meg az üzemeltetőktől, mivel a sémafrissítés egyik különlegessége abban rejlik, hogy visszafordíthatatlan, visszavonhatatlan folyamat, azaz igencsak körültekintően kell eljárnunk a változtatásokkal, főképp nagyobb és/vagy bonyolultabb környezetben. Az

R2 apropóján tehát az OS frissítési tudnivalók után a sémafrissítésről is feltétlenül meg kell emlékeznünk.

Köztudomású, hogy mielőtt egy új verziójú operációs rendszert tartalmazó tartományvezérlőt akarunk telepíteni egy előző verziójú AD környezetbe, a sémát mindig frissítenünk kell. Ennek oka az új szolgáltatások és tulajdonságok megjelenése, amelyek *új és újfajta* bejegyzéseket jelentenek a címtáradatbázisban, tehát a sémában, azaz a címtárban tárolható objektumok definícióinak „tárházában" is gondoskodnunk kell a bővítésről.

Nincs ez másként a Windows 2008 és a Windows 2000/2003 tartományok esetén sem. Szerencsére viszont a frissítést nem kézzel kell elvégeznünk, ehhez rendelkezésre áll egy gyári segédprogram, az Adprep.exe (ami a telepítő DVD-n megtalálható, mind a két platformra). A frissítéshez egy speciális jogokat adó csoporttagság is szükséges, konkrétan a Schema Admins biztonsági csoport (amely csak a forest root domainben van) tagjává kell tennünk a bővítést végző felhasználói fiókot, ha még nem az.

További tudnivalók pontokba szedve:

1. Mielőtt elkezdjük a séma frissítését, minimum Windows 2000 natív szinten kell lennie a Windows 2003 tartományunknak (a működési szintekről később még bőven lesz szó).
2. Ha az adott gép lesz az első új DC az erdőben, akkor előzetesen az erdőt is preparálni kell az adprep /forestprep paranccsal. Ekkor a séma frissítését a Schema Master egyedi szerepkörrel ellátott DC-n kell elvégeznünk, ami annyira egyedi, hogy összesen egyetlen egy ilyen gépünk lehet csak az egész erdőben – ez az ún. forest root DC.
3. Ha ez a gép lesz az első új DC a tartományban (de az erdő már elő van készítve), és a tartomány Windows 2003 működési szinten van, akkor az adprep /domainprep parancsot kell használnunk az Infrastructure Master FSMO szerepkört birtokló DC-n a tartomány előkészítéséhez.
4. Ha gond nélkül lemegy minden parancs, és így az erdő és a tartomány preparálás, akkor nem lesz rá szükségünk, de egyébként jó ha tudjuk, hogy az Adprep debug naplófájlok helye megváltozott, immár a következő helyen találjuk: %systemroot%\debug\adprep

E rész végére került extra információ, amellyel még nem találkozhattunk, akárhány éve ütjük-verjük a sémát. Az a speciális helyzet állt elő ugyanis, hogy a Windows 2008 egyik nagy dobásaként számon tartott teljesen új típusú tartományvezérlő, a RODC működik az erdő Windows Server 2003-as szintjén is (igaz egy kisebb szépséghibával, lásd e cikk legvégén). Ha tehát a Windows 2003-as tartományunkban szeretnénk RODC-ket csatasorba állítani, akkor van még egy

teendőnk az Adprep-pel, mivel preparálnunk kell a Windows 2003-as működési szinten lévő erdőt azért is, hogy a RODC replikálhassa a DNS alkalmazáspartíciókat. Viszont ehhez nem kell a Schema Master gép, az erdő bármelyik tartományvezérlőjéről elindíthatjuk az Adprep /rodcprep parancsot, de ehhez is szükséges az Enterprise Admins csoporttagság. További tudnivalók a RODC alkalmazásával kapcsolatban:

- Ha úgy tervezzük, hogy a RODC-nk egyben GC (globális katalógus kiszolgáló) is lesz, akkor az erdő minden egyes tartományában kivétel nélkül futtatnunk kell az Adprep / domainprep parancsot, akár van ezekben új kiadású DC, akár nincs. Ennek a kritériumnak az oka az, hogy így a RODC képes lesz replikálni a globális katalógus adatokat minden tartományból, és így - és csak így - teljes értékű GC-nek számít majd.
- Az első Windows 2008/R2 DC egy meglévő Windows 2003/2008 tartományban semmiképpen nem lehet RODC, ezt a szerepet csak egy második új DC birtokolhatja, mivel az első ahhoz kell, hogy a RODC ezen keresztül érje el a tartományt, és be tudja indítani a speciális replikációt, a jelszószinkront és egyebeket (részleteket lásd a RODC fejezetben).

6.3.2 A MŰKÖDÉSI SZINTEK

A következő lépésben a szintén speciális, működési szintekről lesz szó (a migrációnál már ezt és a sémabővítést is említettük egy kicsit), azért mert az ezzel kapcsolatos teendők is minimum lehetséges, de sok esetben kötelező elemei lesznek az R2 bevezetésének. A most következő áttekintéssel tehát ezen a terhen szeretnék kicsit könnyíteni, sorba állítva a lehetséges forgatókönyveket. Kötelességem szólni arról is, hogy a sémafrissítéshez hasonlóan a működési szinten változtatása is visszavonhatatlan folyamat (általában, lásd következő keret), tehát csak óvatosan!

> A visszavonhatatlanság ténye egészen az R2-ig igaz is volt, de itt már nem, tényleg visszafelé is léphetünk a működési szinttel. Persze bizonyos korlátokkal: 1. Csak egy szinttel vissza (Windows 2008) 2.; feltételezve, hogy nem engedélyeztünk olyan újdonságokat, amelyeket blokkolna a visszaállítás (Ha igen: Disable-ADOptionalFeatures), 3; A Recycle Bin viszont NEM letiltható (azaz ha már megengedtük, nincs visszaút).
> Valamint nincs grafikus felület a visszaállításhoz, ergo marad a Powershell, mégpedig a Set-ADDomainMode, Set-ADForestMode cmdlet-ek.

Nos, most is, mint mindig, szét kell választanunk a témát két részre, a tartományok és az erdő szintjére. Először koncentráljunk a tartományok működési szintjével kapcsolatos okosságokra!

Az összes működési szint listája, szép sorban:

- Windows 2000 mixed (a Windows Server 2003-ban ez az alapértelmezett)

- Windows 2000 natív
- Windows Server 2003 interim[80]
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

R2 tartomány működési szintek

A legfontosabb: az R2 első üzemmód kivételével a többi felállásban képes lesz tartományvezérlőként dolgozni. Tehát az R2 DC egy Windows 2000 mixed módú tartományban semmiképp, viszont efelett a Windows 2000/2003/2008 tartományvezérlőkkel is biztosan egyet fog érteni.

Windows 2000 natív módú tartományok
Tartományvezérlő lehet: W2K, W2K3, WS08, R2
Berakhatunk tehát egy ilyen tartományba is R2 DC-ket, de a tisztán WS08/R2 újdonságok viszont a tartomány ezen állapotában nem használhatóak, hiszen ezen új technológiák alapfeltétele a natív WS08-as tartományi üzemmód. A W2K natív módú tartományok viszont a következő pluszokat adhatják az előző (a Windows 2000 mixed) módhoz képest:

- Az univerzális csoportok biztonsági és terjesztési csoportokként is használhatóak.
- Csoportok általános egymásba ágyazhatósága.
- Biztonsági és terjesztési csoportok közötti konverzió.
- SID history: A felhasználó régi, más tartományban használt SID-jét tartalmazza, melyre tipikusan egy migráció után lesz szükség.

Windows Server 2003 módú tartományok
Tartományvezérlő lehet: W2K3, WS08, R2
Ebben az üzemmódban a Windows 2000 DC-k már nem, a Windows Server 2003-ak viszont csont nélkül használhatóak együtt a Windows Server 2008 tartományvezérlőkkel. A jó pár Windows Server 2008 és R2 újdonság viszont szintén nem működik majd ilyen körülmények között. A W2K3 natív módú tartományok például a következő lehetőségeket biztosítják (az első négy örökölt a Windows 2000 mixed módból, de azért beírtam):

- A Netdom.exe-vel átnevezhetjük a tartományvezérlőt
- A „Users” és a „Computers” tárolók (azaz nem OU-k) átirányítása

[80] Csak ha NT4-ről jöttünk közvetlenül a Windows 2003-ra, mert ilyen egyébként semmilyen más esetben nem fordulhat elő, tehát pl. Windows 2000-ről Windows 2003-ra sem.

- Képes frissíteni a gépek illetve felhasználók viszonylatában a LastLogonTime attribútumot, és replikálni a LastLogonTimeStamp-et a tartományon belül (még ha kissé nehézkesen is, azaz nem túlságosan nagy pontossággal).
- Az Authorization Manager a házirendjeit tárolhatja az AD-ban
- Rendelkezésre áll a Kerberos Secure Delegation az alkalmazások számára a Kerberos hitelesítés kikényszerítésére

Windows Server 2008 módú tartományok
Tartományvezérlő lehet: WS08, R2
Ha itt tartunk, akkor az azt fogja jelenteni, hogy minimum Windows Server 2008 DC-ink vannak (vagy elszúrtuk, de nagyon ☺[81]). Ez a szint azért fontos, mert az ebben a könyvben is említett Windows 2008-as címtárszolgáltatás újdonságok ekkor már elérhetőek, teljes mellszélességgel. A Windows Server 2008 módú tartományok tehát például (a lista nem teljes!) a következő extrákat adják az előző módhoz képest.

- DFS-R replikáció a SYSVOL megosztás számára (kifejezetten kellemes dolog, hiszen ekkor bevethető a DFS-R részeként az RDC algoritmus, amivel könnyedén magas tömörítési hatásfokot is elérhetünk, már csak azért is, mert az RDC a különbségi replikációs módszert preferálja)
- Kerberos AES 128/256 támogatás
- Last Interactive Logon Information, amely megmutatja a felhasználó legutolsó sikeres interaktív belépésének időpontját, az ehhez használt munkaállomást illetve a sikertelen belépések számát is
- Fine-Grained Password Policies, azaz alternatív jelszóházirend

Az R2-vel kapcsolatos tartományi üzemmódnál kicsit variálok, mivel itt szétszedem olyan szintekre is, amelynél még nincs teljes átkapcsolás, csak egy új szerver, vagy aztán az első tartományvezérlő:

- Egy vagy több R2 tagkiszolgáló
    - Offline Domain Join
    - Managed Service Accounts
- Egy vagy több R2 tartományvezérlő
    - Active Directory Administrative Center
    - PowerShell for Active Directory Module
    - Best Practices Analyzer
    - DSRM Password Sync
- R2 tartomány működési szint
    - Authentication Mechanism Assurance
    - Kibővített MSA-SPN management

A tartományok után az erdők működési szintjének WINDOWS SERVER 2008-as szintre emelésével folytatjuk. A lényeg az, hogy mivel az erdő a tartományok „felett”

[81] Ez egyébként nem megy, van ám ellenőrzés.

lévő fogalom, ezért sokkal óvatosabban kell bánnunk az erdő működési szintjének változtatásával.

R2 erdő működési szintek

Először a lista, ez már csak öt elemből áll:

- Windows 2000 (ez az alapértelmezett a Windows Server 2003/2008 esetén)
- Windows Server 2003 interim
- Windows Server 2003 natív (az alapértelmezett az R2 esetén)
- Windows Server 2008
- Windows Server 2008 R2

Az ötből a második kivételével[82] használhatunk R2 tartományvezérlő(ke)t. Nézzük át az idők kezdetétől, hogy mi minden pluszt lehetett korábban elérni egy-egy erdő működési szint emeléssel!

Windows 2000 natív módú erdő
Tartományvezérlő lehet: W2K, W2K3, WS08, R2
Az akkor még újnak számító és előd nélküli címtárszolgáltatás összes alapértelmezett tulajdonságát használhattuk.

Windows 2003 natív módú erdő
Tartományvezérlő lehet: W2K3, WS08, R2
Néhány újdonság (természetesen nem az összes):

- Cross Forest Trust, azaz erdők közötti bizalmi kapcsolat kialakítása, magyarul két erdő összekötése, pl. két cég összeolvadása apropóján. Kétirányú, tranzitív az erdők összes tartománya között, de nem az egyik erdőhöz ugyanígy kapcsolódó harmadik erdő felé.
- Tartomány átnevezés
- Link valued replication, azaz az „finomított” replikáció, amely sávszélesség takarékos, és lehetővé teszi, hogy ne az adott elemet tartalmazó egész tömb replikálódjon, hanem csak a ténylegesen megváltozott elem.
- Séma elemek inaktiválása, azaz olyan osztályok és attribútumok forgalomból kivonása, amelyek sérültek vagy már nem szükségesek. A törlés nem járható út továbbra sem, de legalább a takarítás megoldható, sőt nagy szükség esetén akár visszakaphatjuk a szemetet is, ti. az inaktiválás visszavonása, a deaktiválás is működik.
- A RODC használata

Windows Server 2008 módú erdő
Tartományvezérlő lehet: WS08, R2

[82] Ugye az Interim mód csak egyetlen, nagyon speciális esetben jöhet létre, így nem játszik itt sem.

Kicsit megdöbbentő, de a tartományi szint számtalan újdonságával nagyjából el is fogyott a puskapor, azaz erdőszinten nincs semmilyen extra újdonság. Egyetlen dolgot azért meg kell említeni, ami miatt valószínűleg érdemes is lesz megemelni az erdő működési szintjét, ha ez lehetséges.

A dolog a RODC-val kapcsolatos, de messziről futunk neki. Néhány alkalmazásnál megszokott dolognak számít, hogy a címtárban tárol szenzitív adatokat (jelszavak, jogosultságok, titkosított kulcsok, stb.). Ezzel nincs is gond, sőt praktikusnak is tekinthetjük ezt a módszert, a tartományvezérlőkre amúgyis fokozottan oda kell figyelnünk, és hát valóban ritkán tűnik el egy-egy DC a szerverszobából / teremből.

Viszont ha bekerül majd a képbe egy-egy RODC - ismerve a tulajdonságait: csak olvasható, jelszavakat nem tárol, Server Core-ra is felmegy, stb. - a telephely egy sötét sarkába lerakva, akkor azért kicsit mégis aggódhatunk. Ugyanis egy címtárpéldány azért lesz azon a gépen is, szóval ha történetesen ellopják, azért kibányászható lesz belőle ez-az.

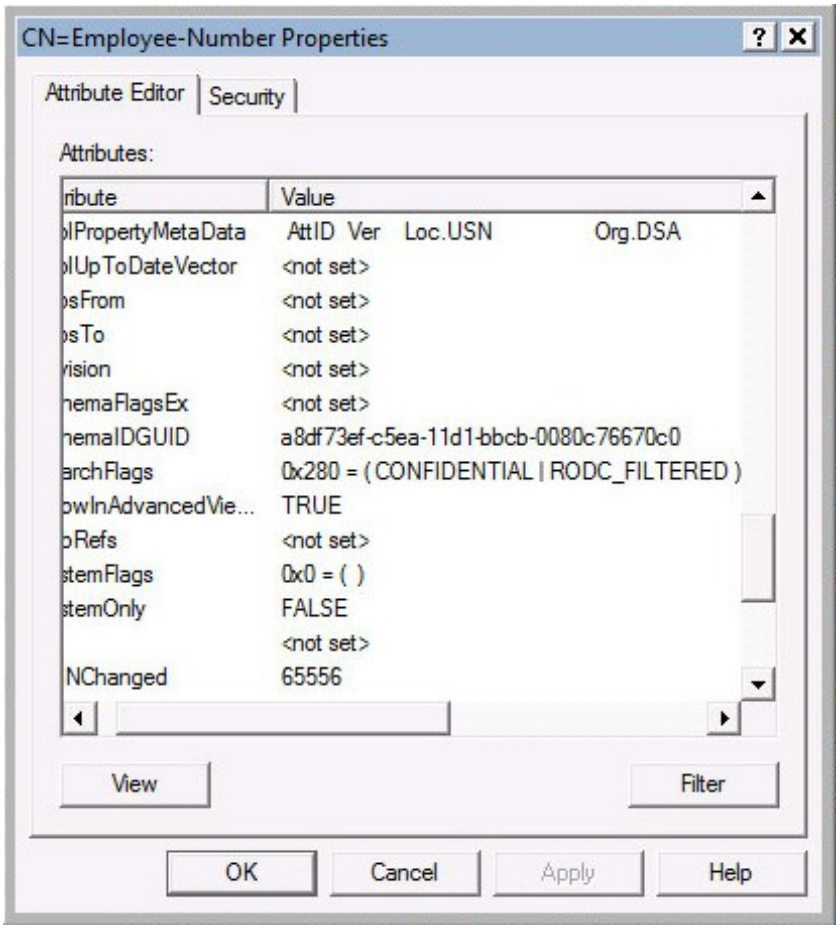
Nos, erre találta ki a Microsoft igen okosan az ún. RODC Filtered Attribute Set (RODC FAS) használatának lehetőségét, amely azt jelenti, hogy a Windows Server 2008 Schema Master DC-n pl. az ldfide-vel vagy az ADSIEdit-tel megnövelhetjük az adott attribútum tulajdonságai között a searchFlags értéket (pl. 0-ról 640-re = CONFIDENTIAL / RODC_FILTERED, lásd kép, bár ott még hexában van). Így aztán ha a tartományvezérlő beleakad ebbe az értékbe, akkor ezt az attribútumot nem fogja replikálni a RODC kérésére. Mármint a Windows Server 2008 GC DC-k, merthogy egy Windows Server 2003 GC DC továbbra is megengedő lesz[83] és csont nélkül hagyja magát megerőszakolni. Ha viszont az erdőnkben már nincs és nem is lehet effajta „régi” DC, akkor a problémát - kicsit közvetve ugyan, de - letudtuk.

> Sőt, a Windows Server 2008-ban már gyárilag meg van jelölve ily módon egy pár attribútum, elsősorban a Credential Roaming (azaz ha több gépen bejelentkezve akarunk azonos tanúsítványt és kulcskészletet használni) és a Bitlocker miatt, konkrétan ezek:
> - ms-PKI-DPAPIMasterKeys
> - ms-PKI-AccountCredentials
> - ms-PKI-RoamingTimeStamp
> - ms-FVE-KeyPackage
> - ms-FVE-RecoveryGuid
> - ms-FVE-RecoveryInformation
> - ms-FVE-RecoveryPassword
> - ms-FVE-VolumeGuid

[83] Kipróbáltam anno ezt is, hiába piszkáljuk meg az említett flag-et a Windows Server 2003 Schema Master-en - nem érti.

- ms-TPM-OwnerInformation

Annyi még lényeges, hogy a jelszavak replikálásával ellentétben itt nincs választási lehetőség egyesével. Akárhány RODC-vel rendelkezünk, a megjelölt attribútumok egyikre sem fognak replikálódni. Vagy mindre fognak, ha nem jelöljük meg.



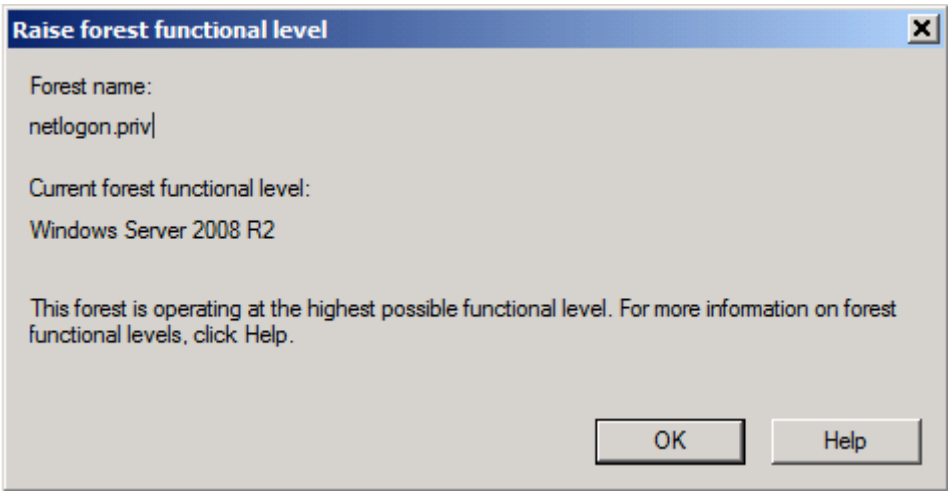
6.25 ÁBRA A MEGVARIÁLT EMPLOYEE-NUMBER ATTRIBÚTUMON SZÉPEN LÁTSZIK A VÁLTOZÁS

Ha már itt tartunk, azért említsük meg, hogy a FAS mellett/helyett van még egy lehetőségünk, ez pedig a védeni kívánt attribútum searchFlags értékének feljavítása a „CONFIDENTIAL" szintre (ennek 128 a decimális értéke, ez az előző esetben ugye automatikusan benne van a 640-ben, látszik is az előző képen). Ezt a Windows Server 2003 SP1 óta lehetséges művelni, van is hozzá egy fárasztó KB cikk[84] is.

Gyakorlatilag e változtatás az Authenticated Users csoport Read jogát veszi le (ergo egy akármilyen jöttment RODC-jét is), csakhogy - állítólag - az a gond lehet ezzel, hogy az említett alkalmazások esetleg nem veszik majd ezt jónéven.

[84] http://support.microsoft.com/kb/922836

R2 módú erdő
Tartományvezérlő lehet: R2
A Windows Server 2008-hoz hasonlóan megint csak a puskapor teljes mértékű elfogyásáról van szó (nézzük csak meg az R2 tartományi szintnél, hogy mennyi lehetőség van!), mivel egyetlen újdonságunk van ezen a szinten, de az mondjuk nagyon szimpatikus: ez a már megismert Recycle Bin.



6.26 ÁBRA ITT A VÉGE, FUSS EL VÉLE!

6.4 TELEPÍTSÜNK VÉGRE!

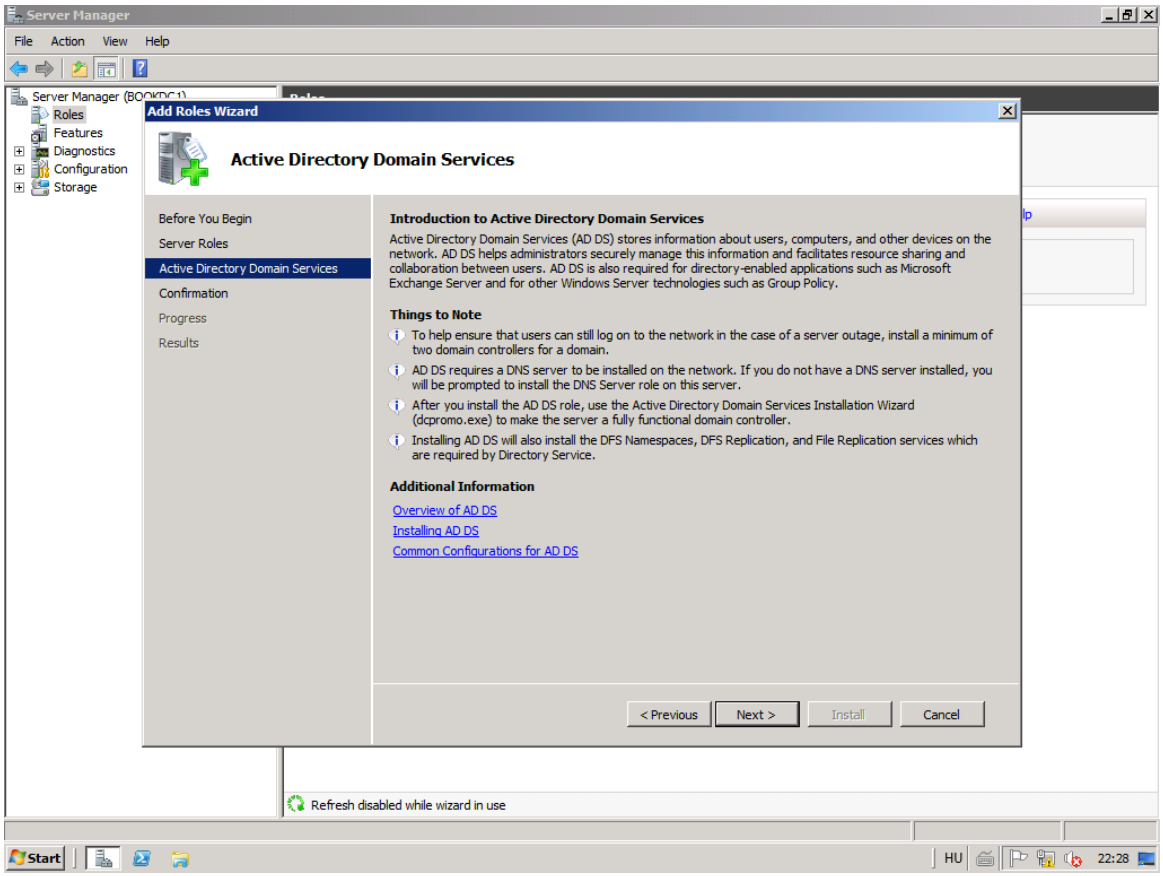
Most egy képes beszámoló kezdődik az AD telepítésről, azért, mert menet közben sokkal könnyebb lesz elmagyarázni az újdonságokat. Most rögtön hadd jegyezzem meg, hogy lépésről lépésre bemutatok mindent, azonban nem magyarázom el, hogy a névkonvenció miért lényeges, vagy azt, hogy pl. mi az a globális katalógus, meg a DNS szerver, de azért, mert mindezt már leírtuk egyszer („Rendszerfelügyelet rendszergazdáknak” című könyv), és már 2x belinkeltem.

Viszont azért arról beszéljünk, hogy az AD telepítés és eltávolítás mindig is a dcpromo.exe-vel kezdődött és végződött! De a Windows Server 2008 óta már nem feltétlenül, illetve egyáltalán nem. Ködös, ugye? Direkt csinálom ☺.

Szóval ha most a dcpromo-t futtatjuk, akkor először felteszi az AD-hoz szükséges bináris állományokat, majd elkezdi a telepítést. De ha nem így akarjuk, van más mód is, emlékezzünk vissza, a Server Manager-ben is van AD DS szerepkör. De ha ezt telepítjük, az nem azt jelenti majd, hogy máris tartományvezérlő lett a gépünk, csak annyit, hogy a bináris állományok fent vannak, jöhet a dcpromo.

És ha egy visszaléptetésről van szó? Nos ezt viszont két lépésben muszáj elvégeznünk: 1.; dcpromo > eltávolítás ; majd 2.; Server Manager uninstall AD DS[85].

Ennyi bevezetés elég lesz, jöjjön a lényeg!



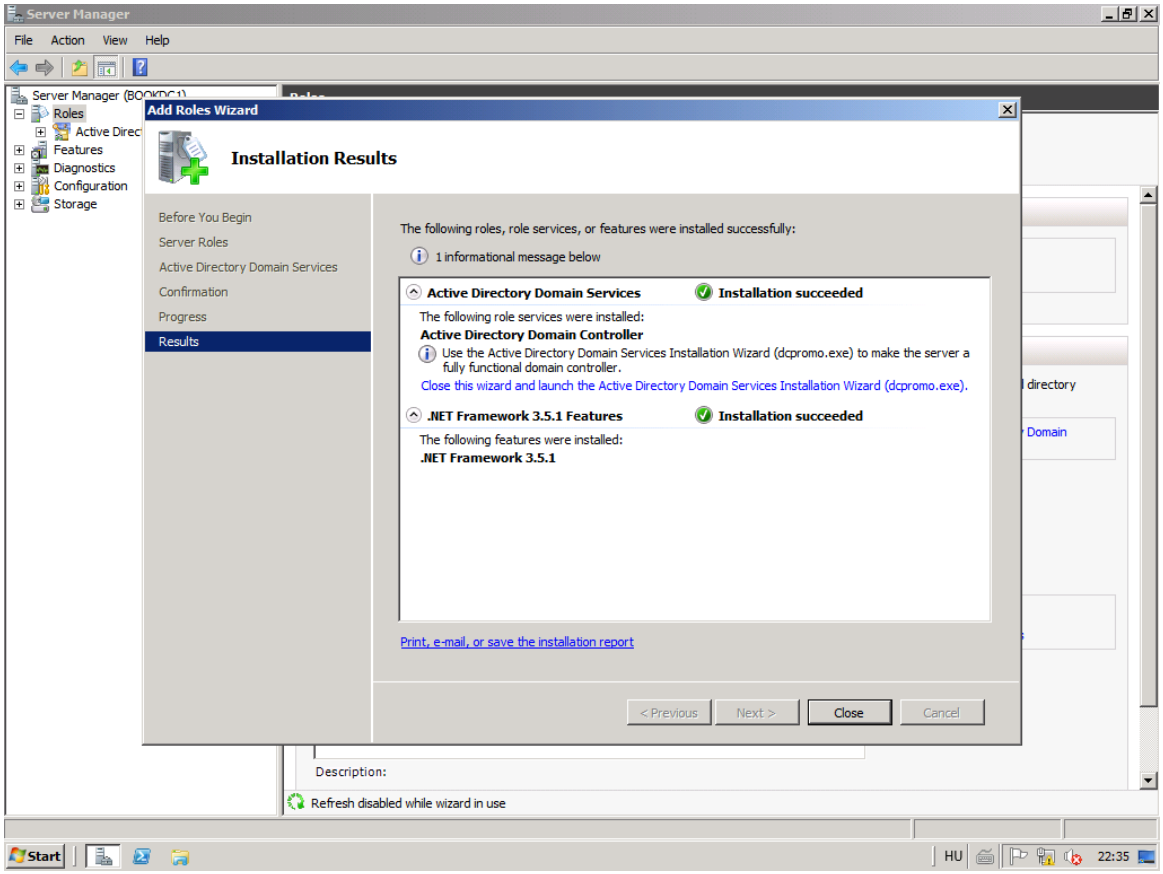
6.27 ÁBRA KEZDŐDIK, APA, KEZDŐDIK!

Az alapszintű instrukciókból már itt kapunk egy csokrot:

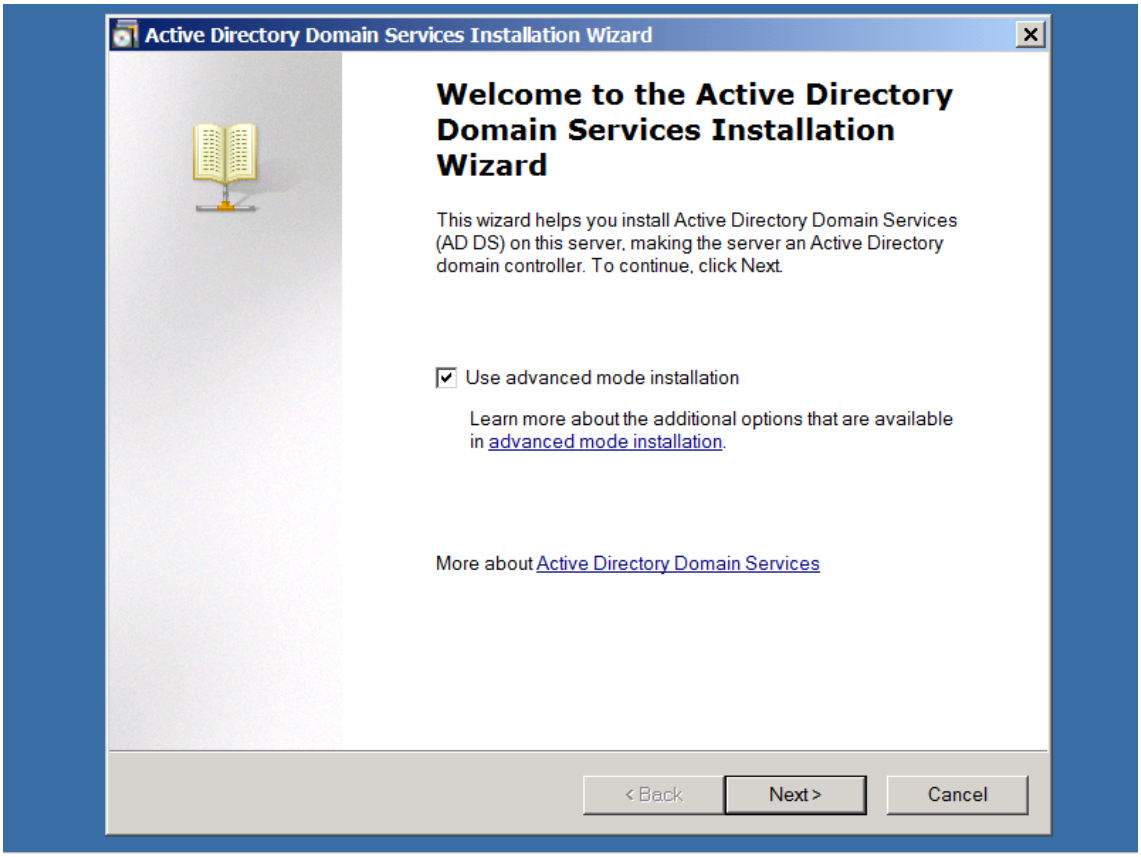
- Legyen minimum 2 DC-d („*Egy DC nem DC*”, már jeleztem korábban)
- A DNS szerver muszájfaktor (majd feltesszük menet közben)
- 2 lépcsős telepítés (pár sorral nézzünk vissza)
- További elemek is felkerülnek automatikusan a rendszerre, pl. a DFS/R (ez ugye 2 db dolog), illetve a File Replication szolgáltatás, plusz a .Net Framework 3.51.

Ha felértünk a telepítés első lépcsőfokára, akkor indíthatjuk a dcpromo-t, az innováció azonban csodálatos, a Server Manager szumma képernyőjéről egy kék színű linkkel is, azaz nem muszáj a Start/Run szakaszban gépelgetnünk ☺.

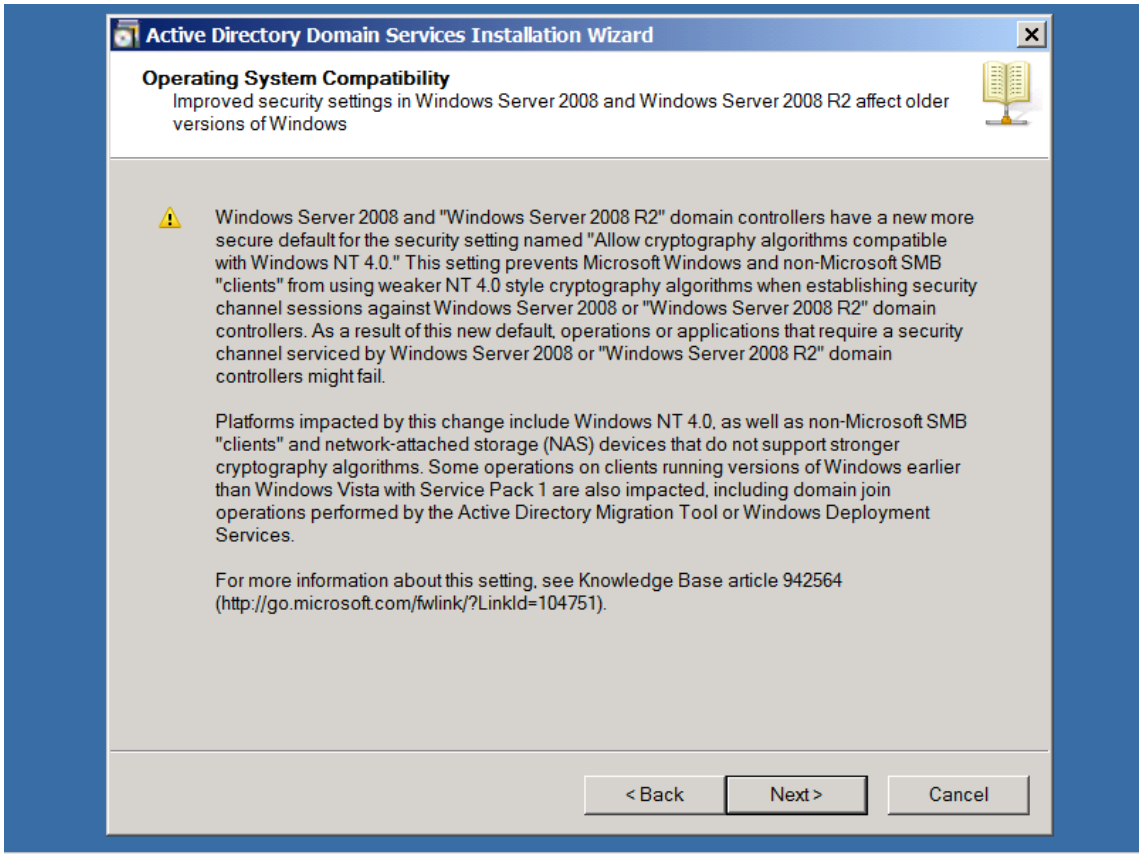
[85] Hány, de hány olyan egykori tartományvezérlőt láttam már, ahol ez az utóbbi lépés nem történt meg!



6.28 ÁBRA EDDIG KIRÁLY



6.29 ÁBRA ÁLTALÁBAN SZÜKSÉG IS VAN AZ „ADVANCED" MÓDRA, ÉS KÜLÖNBEN IS

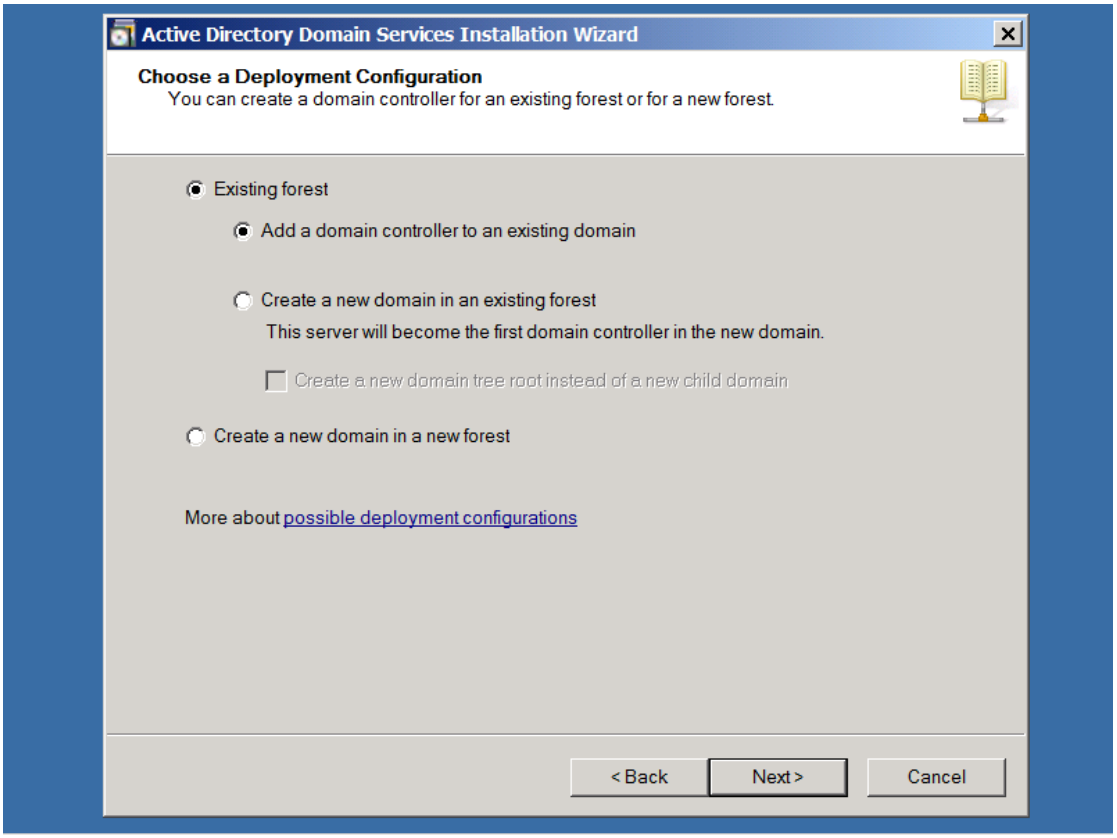


6.30 ÁBRA KOMOLY FIGYELMEZTETÉS

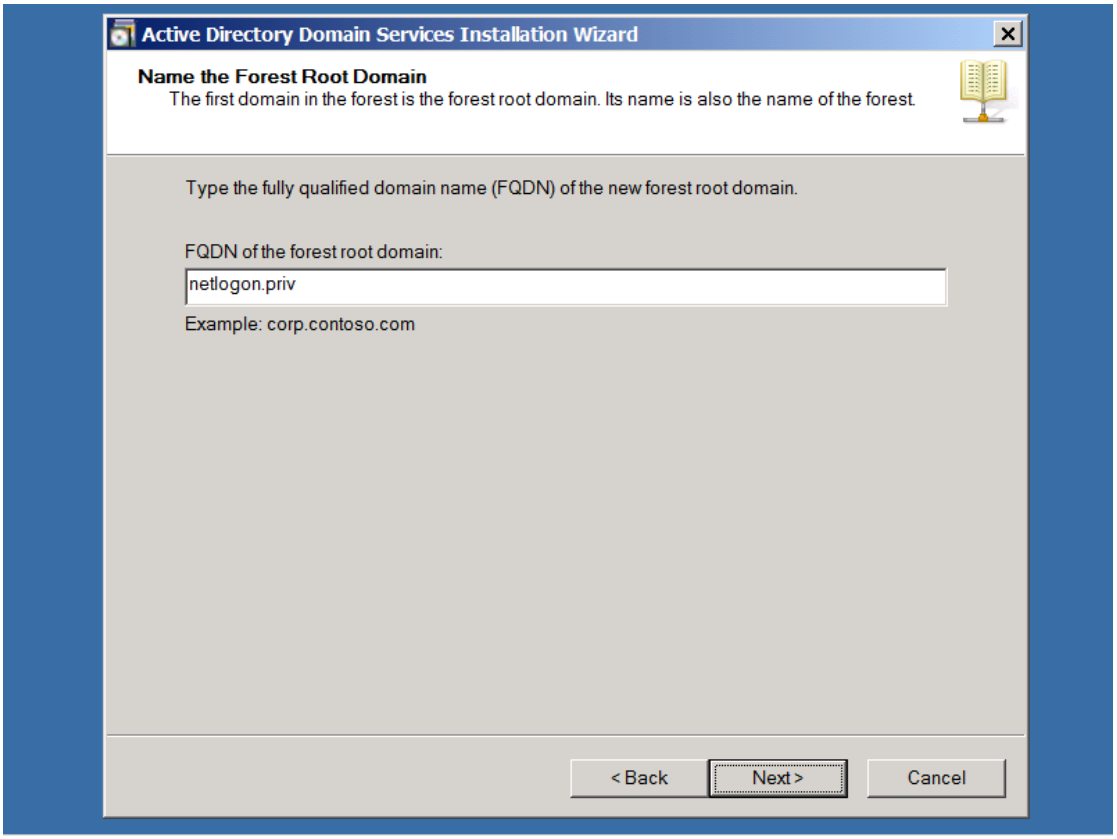
Itt azért kevés a képaláírás, ezért kicsit kifejtem. A Windows Server 2008-tól kezdve a gyári tartományvezérlői házirendben (ami tehát egyből működni fog) jó pár a hálózati biztonsággal kapcsolatos opció engedélyezetté vált[86]. Ezek közül itt egyről van szó, amely hatása viszont a Windows 2000 előtti klienseket kizárja a tartományba belépés lehetőségétől (értelemszerűen akkor is, ha eddig működtek, tehát nemcsak a beléptetéssel, a belépéssel is gond lesz), de pl. egy NT tartomány és az R2-es tartomány közötti megbízhatósági (trust) kapcsolatoknak is vége.

Ráadásul külső, nem tartománytagként működő eszközökkel (pl. NAS-ok, egyéb SAMBA SMB kliensek, vagy más, IP alapon elérhető hálózati tárolók) is lehetnek elérési problémák, sőt még a Vista SP1 előtti szoftveres komponenseket is említ ez a figyelmeztető üzenet. A megoldás a lábjegyzetben lévő KB cikkben benne van, ha muszáj, akkor gyengítenünk kell ezeken a biztonsági opciókon.

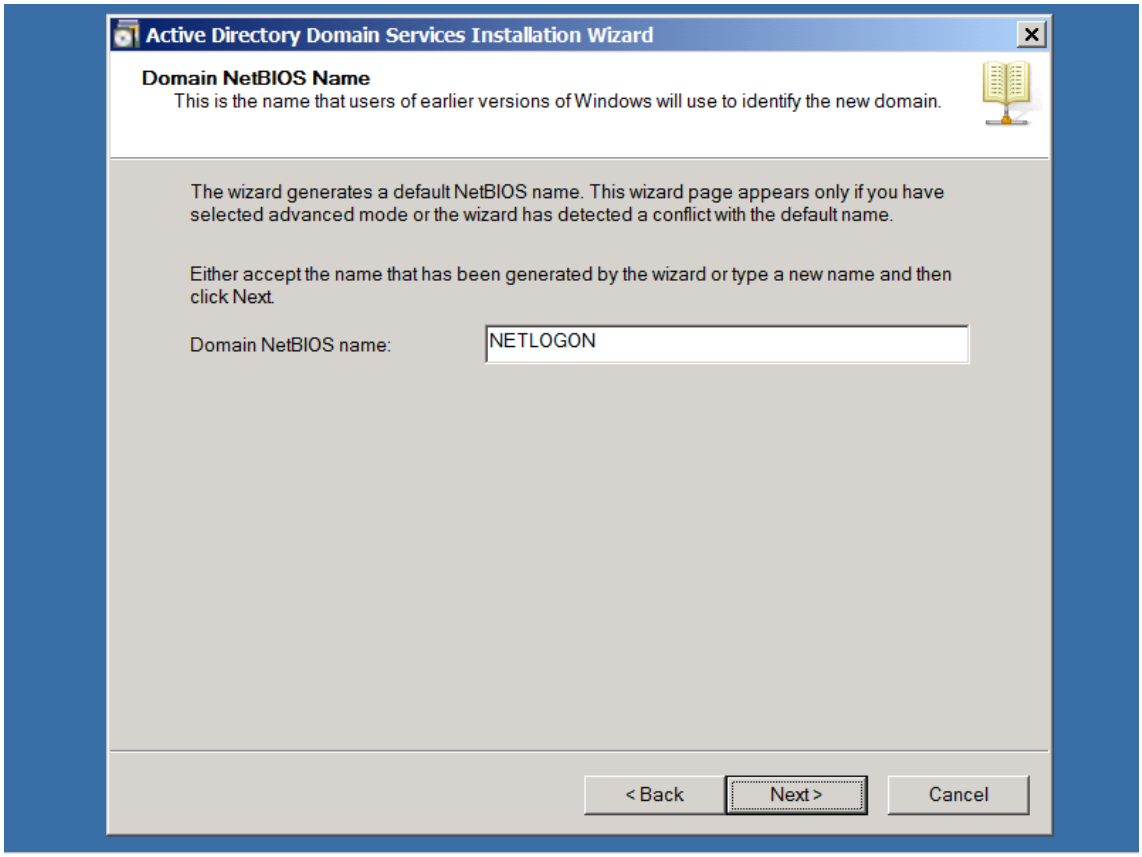
[86] http://support.microsoft.com/kb/942564



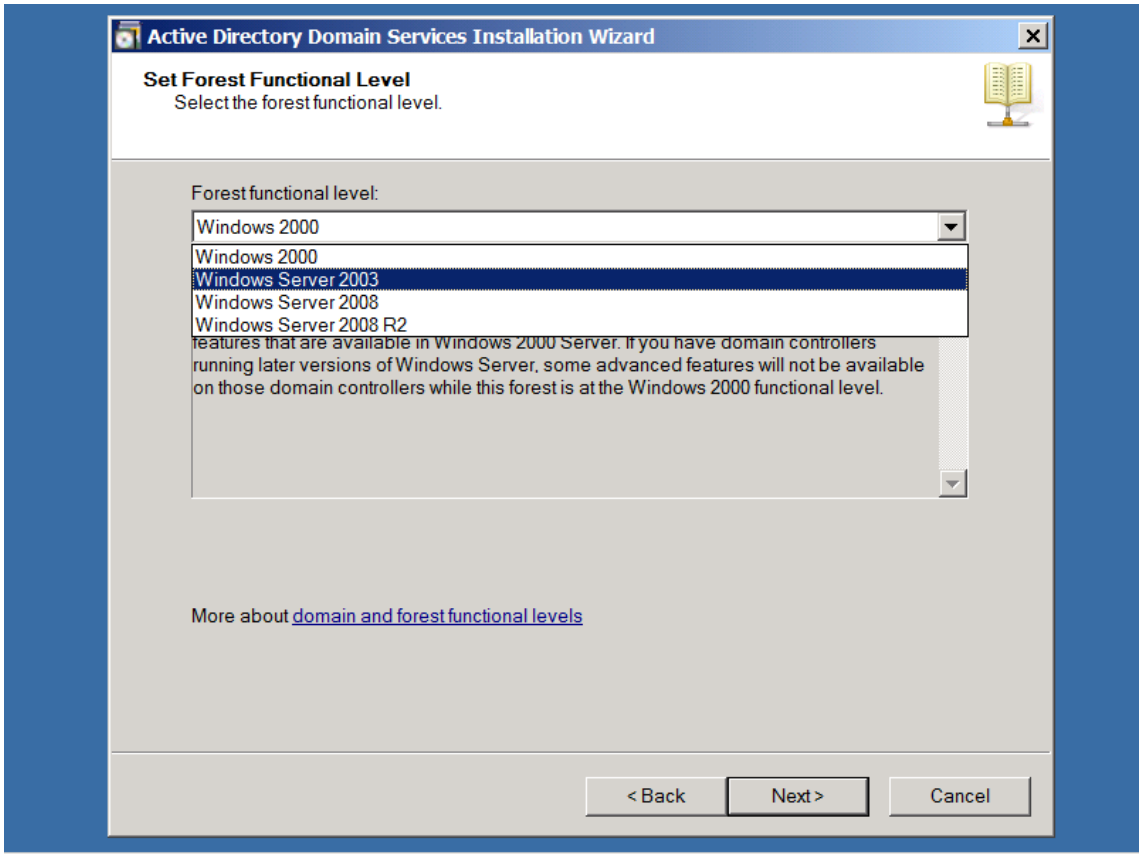
6.31 ÁBRA MEGLÉVŐ VAGY ÚJ, EZ ITT A KÉRDÉS? ÉN ÚJAT KREÁLOK, CSAK AZÉRT VAN MÁS A KÉPEN, HOGY LEHESSEN LÁTNI A TÖBBI OPCIÓT IS.



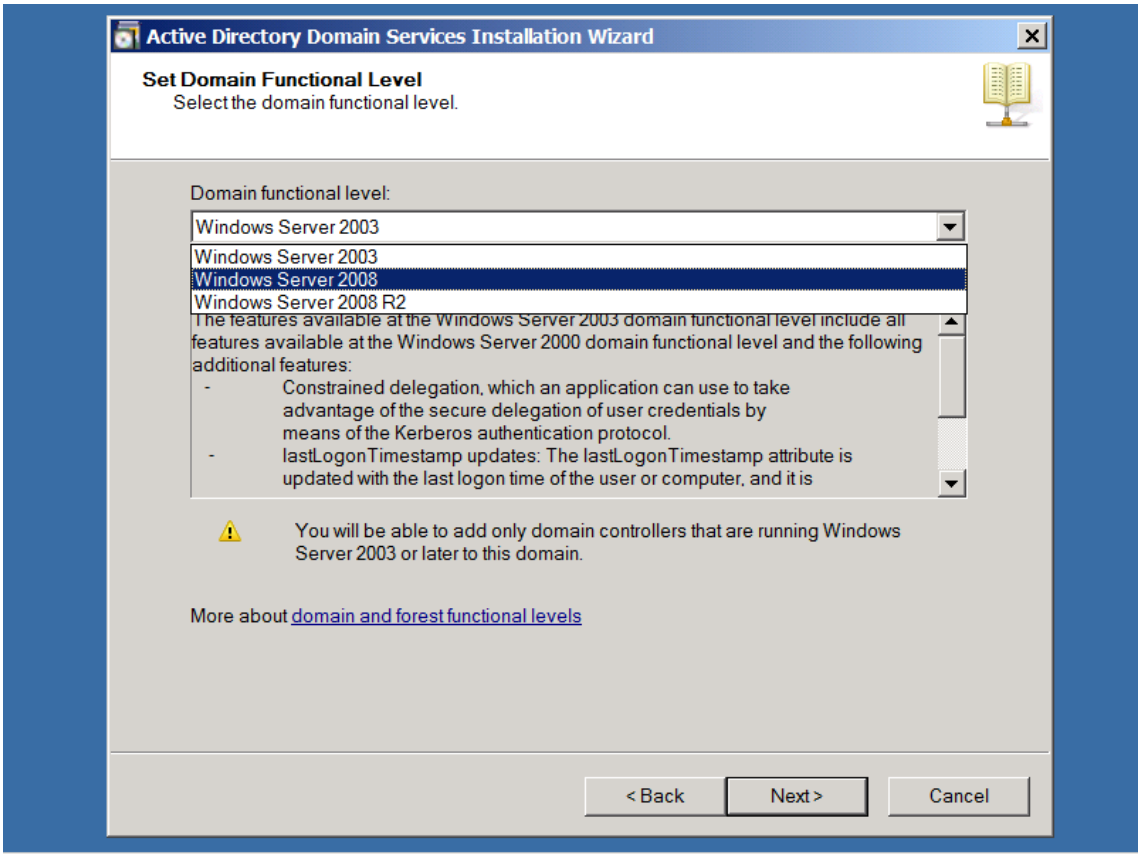
6.32 ÁBRA A TARTOMÁNY TELJES DNS NEVÉNEK KIVÁLASZTÁSA FONTOS, AZ AJÁNLÁS SZERINT NE HASZNÁLJUNK PUBLIKUS VÉGZŐDÉST (BÁR EZ IS MEGOLDHATÓ), DE A .LOCAL, A .PRIV, STB. RENDBEN VAN



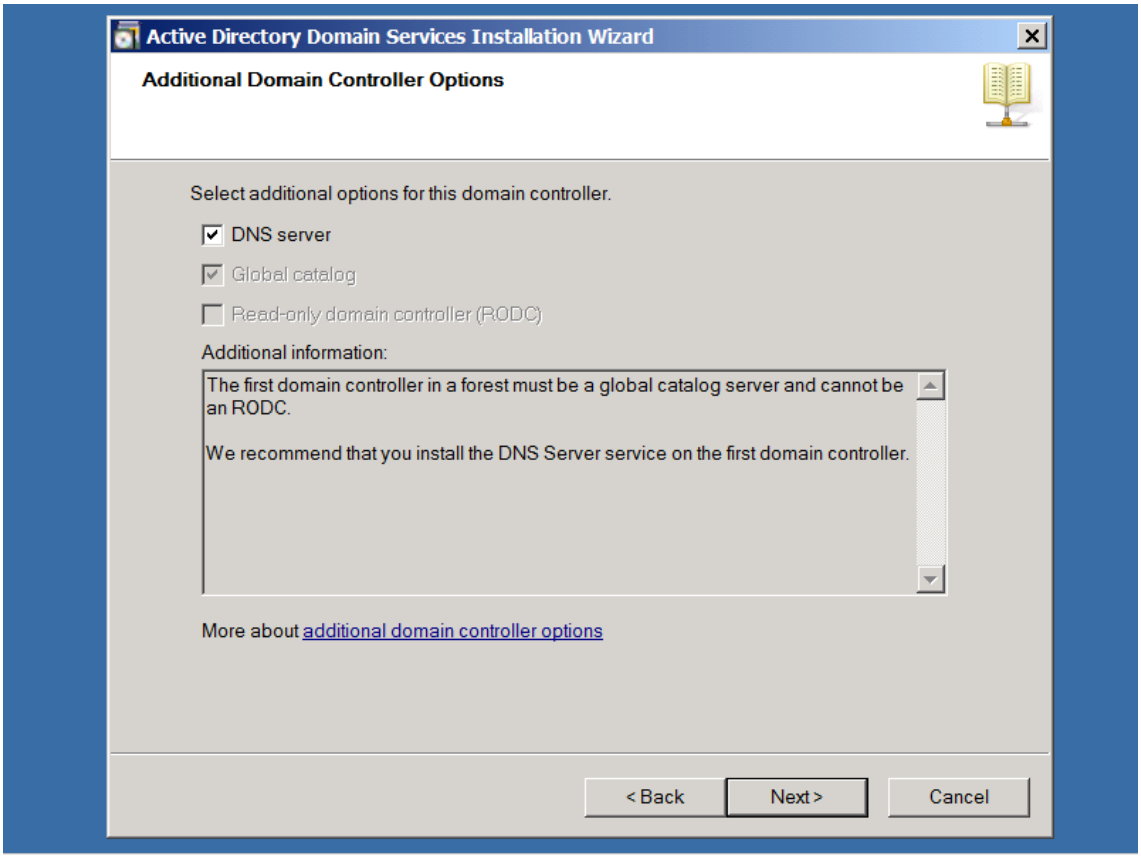
6.33 ÁBRA A KOMPATIBILITÁS OKÁN EGY NETBIOS NÉV IS KELL, EZT ALAPBÓL CSONKOLÁSSAL KÉPZI A TELEPÍTŐ



6.34 ÁBRA ERDŐ MŰKÖDÉSI SZINTEK, DE EZT MÁR KIBESZÉLTÜK, ÚJ TELEPÍTÉS, ERGO INTERIM NINCS



6.35 ÁBRA UA. A TARTOMÁNYNÁL (MIVEL AZ ERDŐ 2003-AS LESZ, EZÉRT CSAK 3 LEHETŐSÉG VAN)

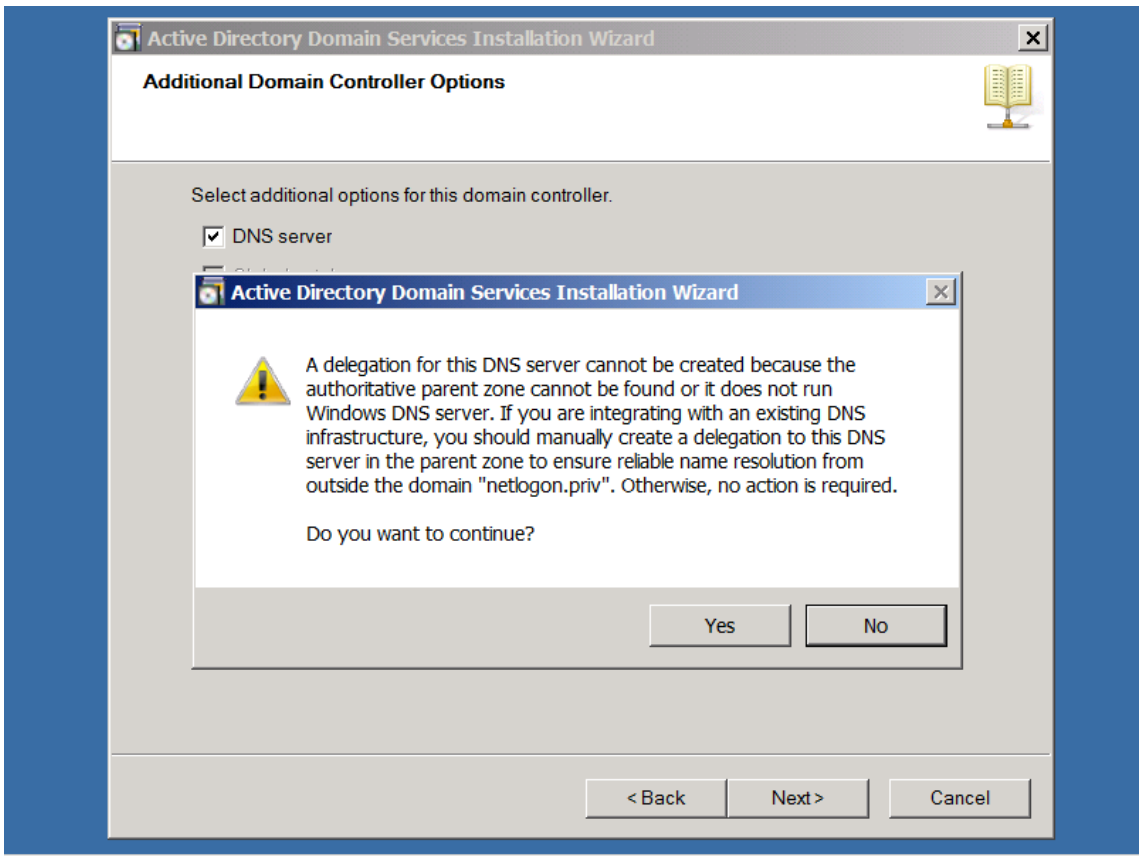


6.36 ÁBRA 3 A KISLÁNY

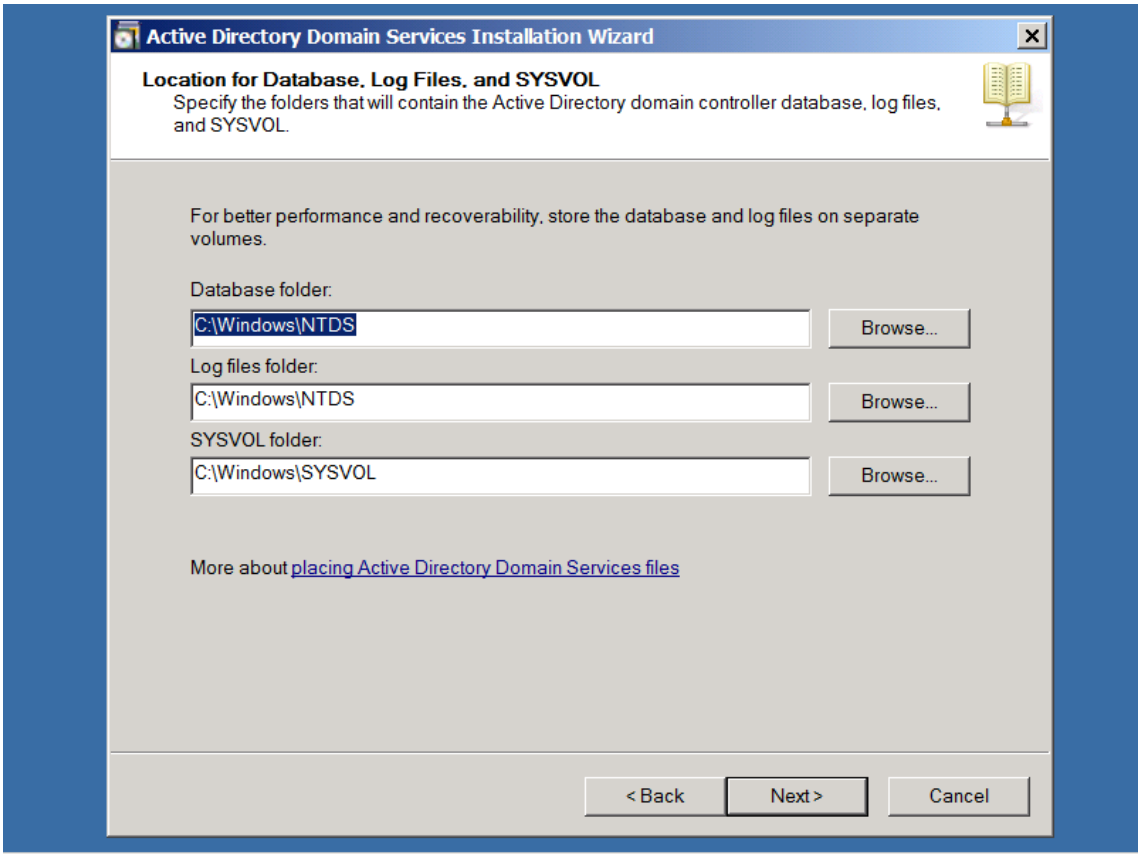
Újra álljunk meg, muszáj magyarázni kicsit. A képen három opció van, de kettő szürke. A globális katalógus azért, mert mivel ez az első DC, azaz a forest root DC, muszáj, hogy globális katalógus legyen. A RODC meg azért, mert az első (új) DC nem lehet RODC, kell neki előtte egy másik, ami a replikációs partnere lesz. A DNS rendben van, az kell.

Egyébként, ha RODC telepítést végzünk, akkor egy kicsit más lesz innentől a telepítő, de erről már volt szó korábban.

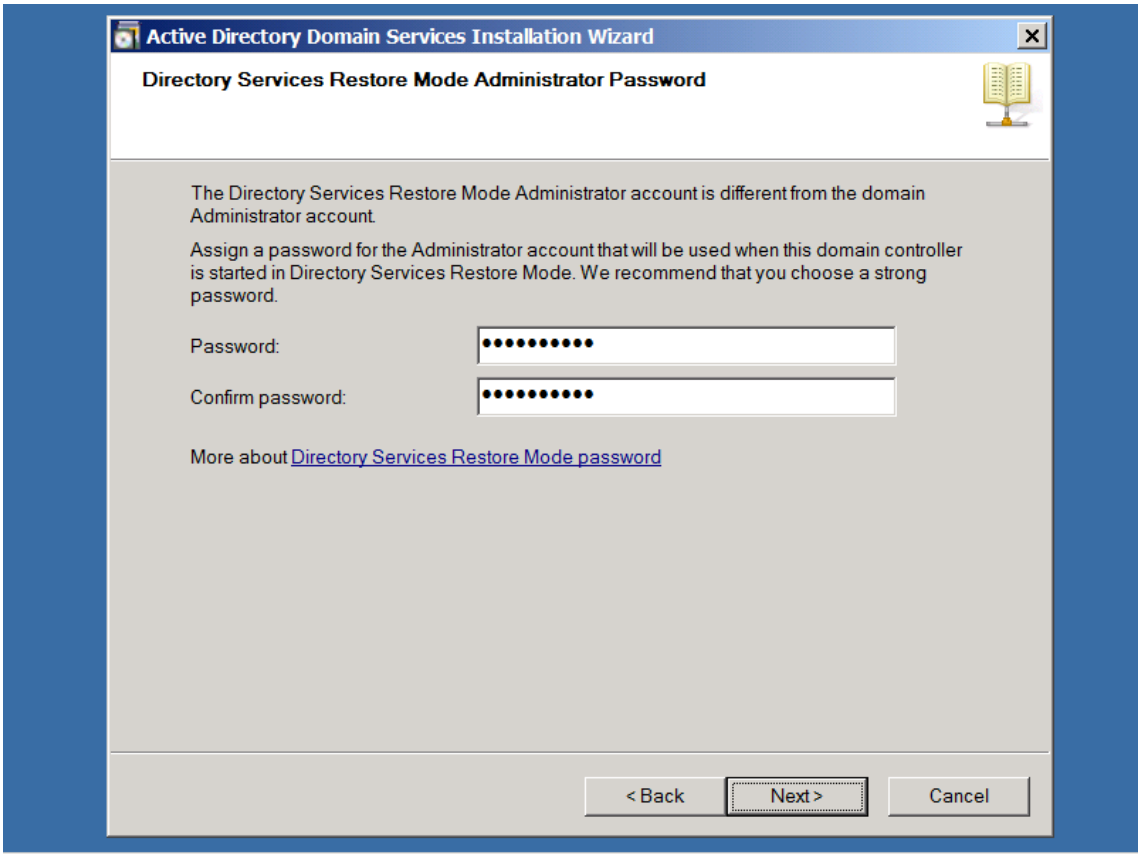
Szaladjunk csak előre, mert rögtön jön ezután egy ellenőrzés és egy figyelmeztetés, amit ha értünk, akkor nem fogunk izzadó kézzel rögtön bepánikolni. Arról van szó, hogy a DNS zóna ellenőrzésekor a telepítő sikít, hogy nem tud delegálást végezni, mert nem találja a netlogon.priv zóna autoritatív szülő zónáját. Persze hogy nem találja, mivel nincs ilyen ☺, ez csak akkor lenne fontos üzenet, ha egy olyan tartományt kreálunk, amely a DNS név (és így a zónanév) alapján egy másik tartomány alá kerülne, pl. cegled.netlogon.priv. De még ekkor sem lenne katasztrófa, mert tovább engedne, csak jelezné hogy akkor csináld meg kézzel a szülő zónában utólag a delegálást, és menni fog. Szóval hagyjuk ezt figyelmen kívül és menjünk tovább!



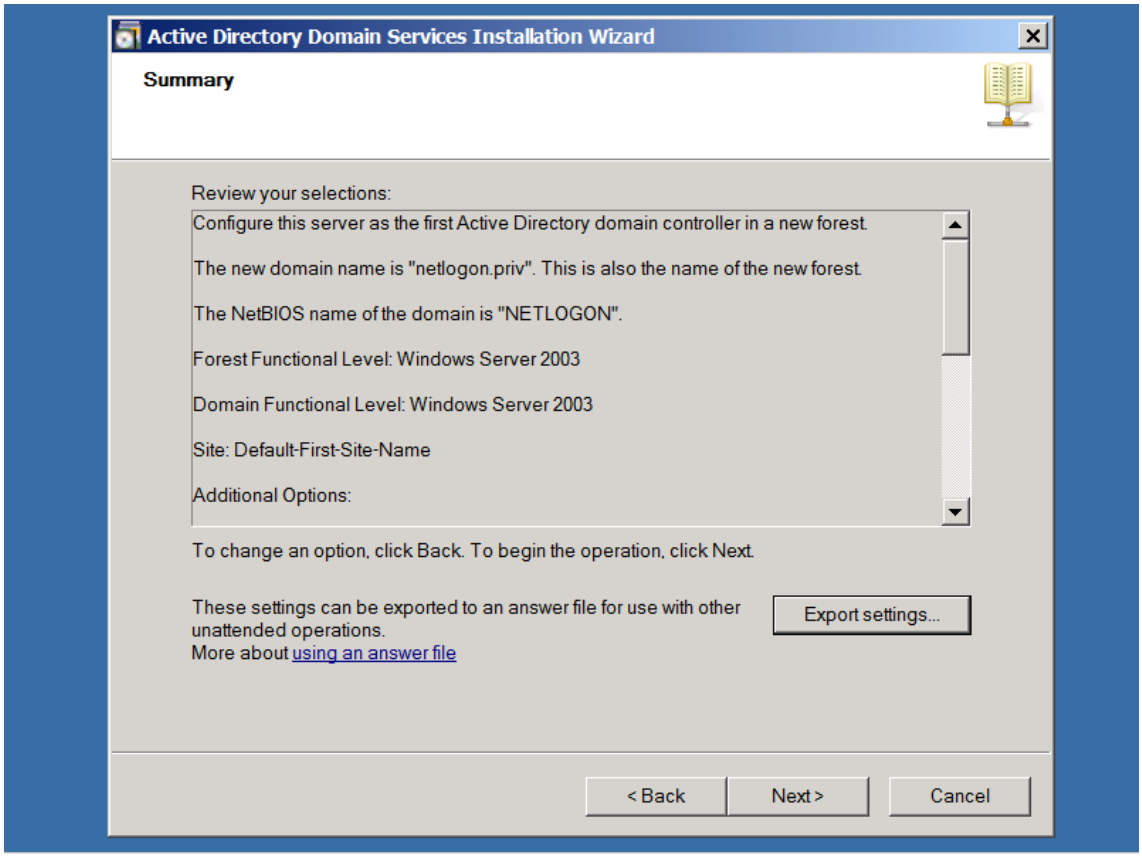
6.37 ÁBRA DNS ZÓNA DELEGÁLÁSI PROBLÉMA, VAGY NEM PROBLÉMA



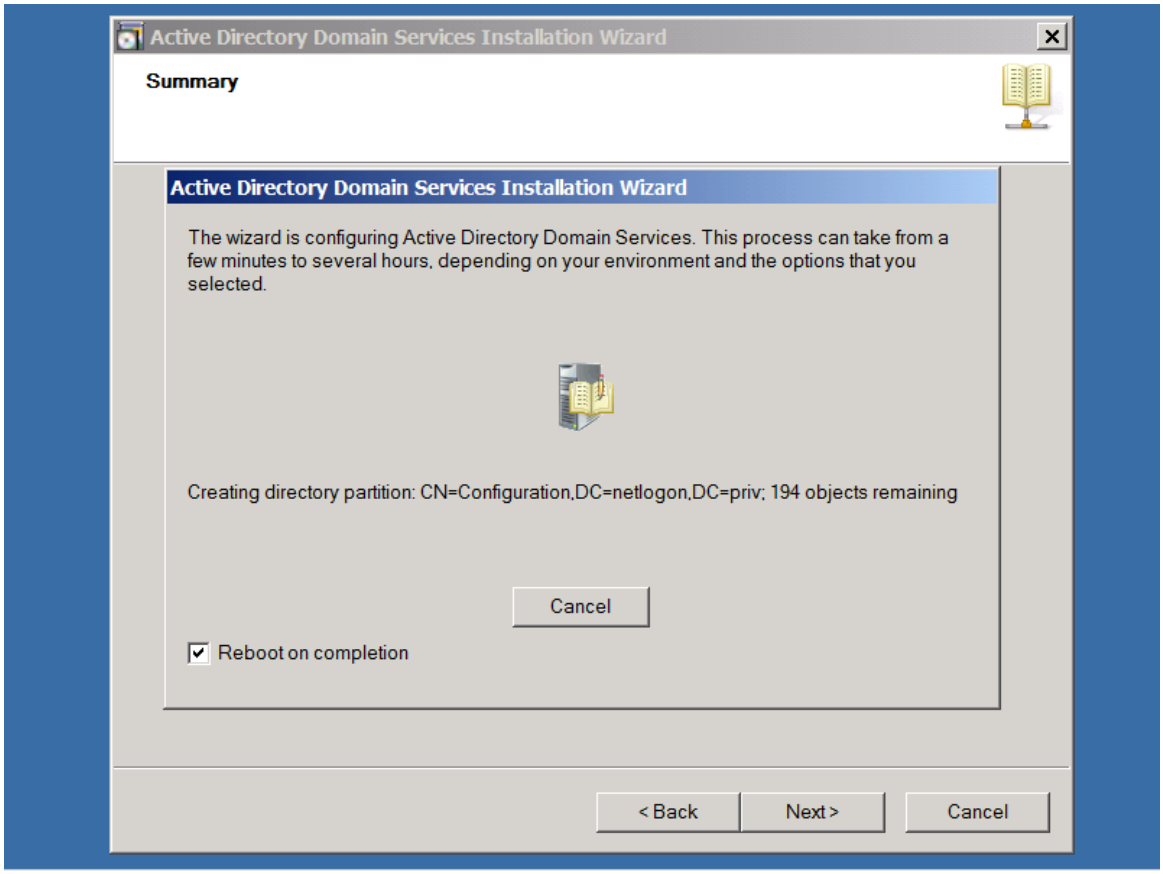
6.38 ÁBRA RUTIN FELADAT, 95%-BAN JÓ AZ ALAPÉRTELMEZETT HELY



6.39 ÁBRA EZ EGY ÜBERFONTOS LÉPÉS, VISZONT KIBESZÉLTÜK MÁR



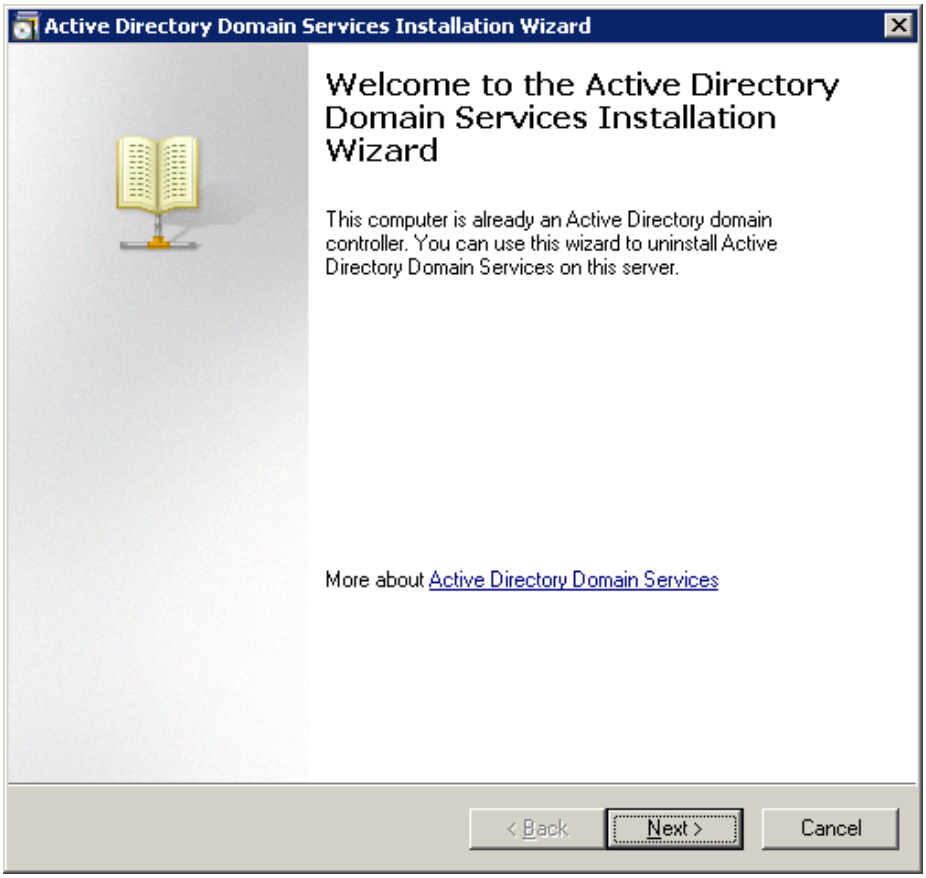
6.40 ÁBRA A SZUMMA ÉS AZ EXPORT SETTINGS, AMI MAJD A CSENDES AD TELEPÍTÉSHEZ KELL (LÁSD 10. FEJEZET)



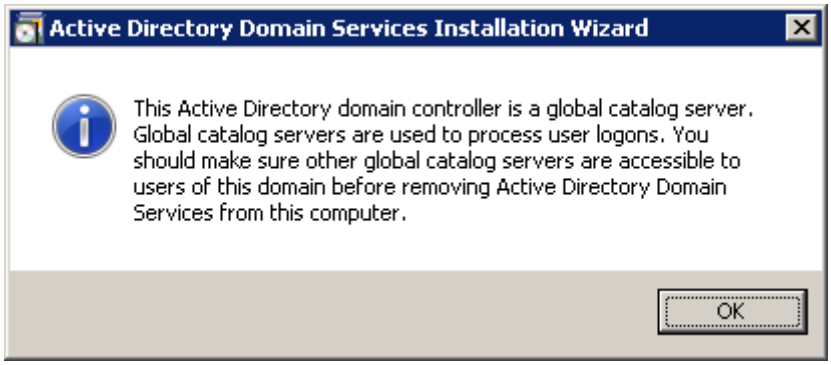
6.41 ÁBRA AZ IGAZI MUNKA MOST KEZDŐDIK, DE EZ MÁR NEM A MI SARUNK

A sikeres előléptetés és az igényelt automatikus újraindítás után (bal alsó sarok) a bejelentkező képernyőn már csak és kizárólag a tartományba léphetünk be, a helyi felhasználói adatbázisba már nem, viszont az eddigi Administrator jelszót kell használnunk.

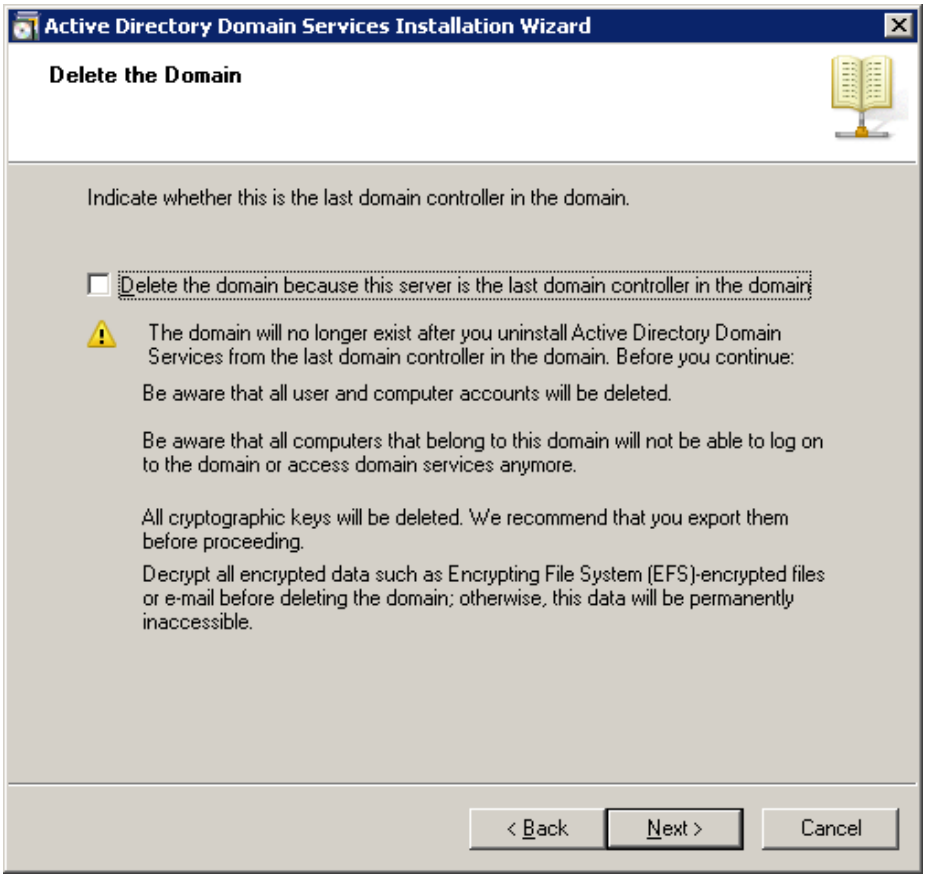
No és ha eltávolítunk? Tegyük meg most. Egy második DC eltávolításáról lesz szó, ami egy 2008 R2-es DC, és az elsődleges is az.



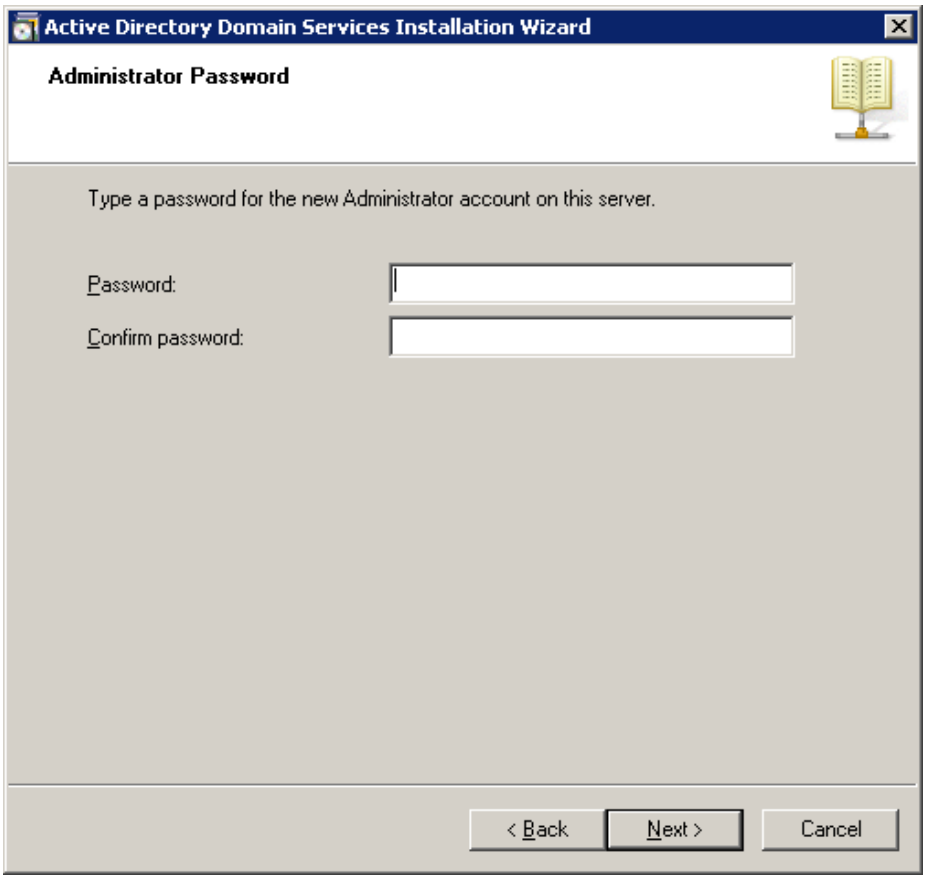
6.42 ÁBRA NEMSOKÁRA VÉGE LESZ



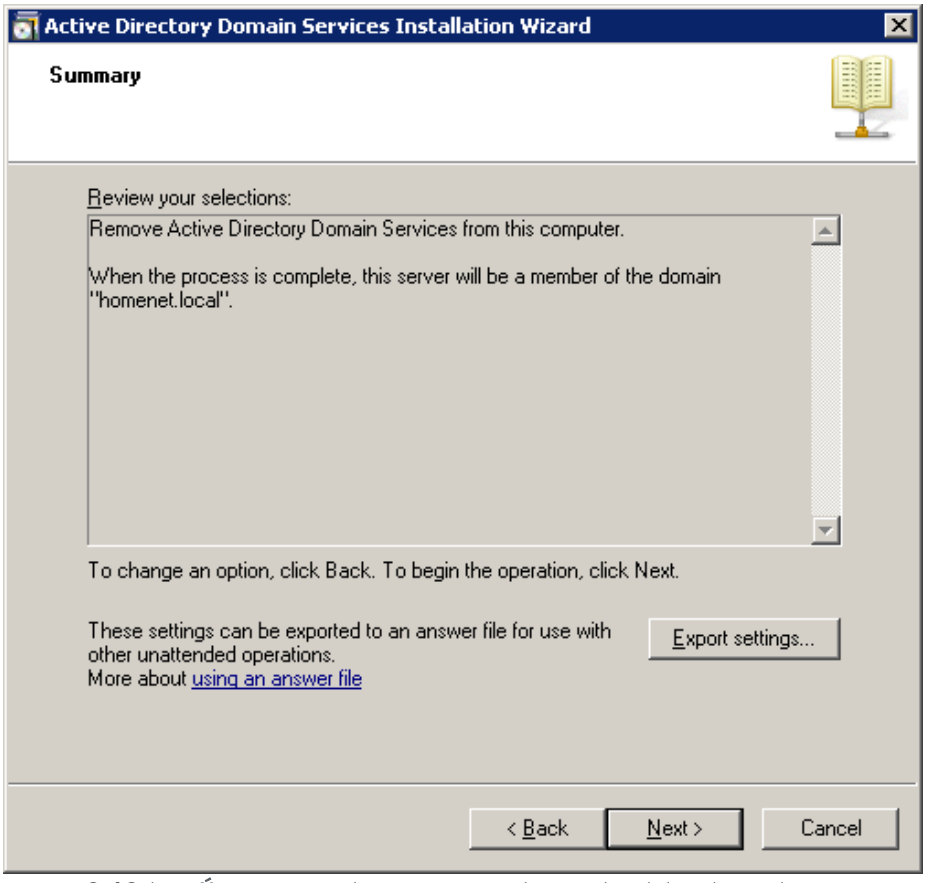
6.43 ÁBRA MIVEL EZ EGY GC, RÖGTÖN JELZI IS, HOGY AZ, DE HA LÚD, LEGYEN KÖVÉR!



6.44 ÁBRA EZT CSAK AKKOR, HA TÉNYLEG EZ AZ UTOLSÓ DC, KÜLÖNBEN NAGY BAJ LESZ ☺



6.45 ÁBRA MIVEL ÚJRA LESZ HELYI FELHASZNÁLÓI ADATBÁZIS, HELYI ADMIN JELSZÓ IS KELL



6.46 ÁBRA ÚJRA SZUMMA, ÚJRA EXPORT OPCIÓ AZ ELTÁVOLÍTÁSI VÁLASZFÁJLHOZ

A legeslegvégén hadd mondjak el egy fontos dolgot: az összes panelen működik a CTRL+C, ergo ha pl. egy hibába futunk vele, könnyű lesz kimásolni és a kedvenc keresőnkbe beírni.

6.5 KEDVENCÜNK A CSOPORTHÁZIREND

Rengeteg alkalommal kapok olyan - akár egészen összetett - szakmai kérdéseket amelyekre egyetlen szóval, azaz brutális egyszerűséggel tudok válaszolni: *Csoportházirend*. Felettébb idegesítő szokásom ez, viszont általában nem tréfálok, a tapasztalatom alapján tényleg számos problémát megoldhatunk a házirend opciókkal, és sok-sok időt és energiát meg tudunk spórolni az energikus Csoportházirend használattal.

Legfontosabb előnyei az egy helyről történő, központi kezelés és a hatókör, azaz akár az összes számítógépre és felhasználóra érvényesíthető beállítások. A központosítás mellett egy másik lényeges érv (csúnya szóval) az implementálhatóság, azaz képesek vagyunk-e fájdalmas átszervezés nélkül ráhúzni a szervezetünkre egy komplex, de azért igény esetén egyedivé is tehető beállítás gyűjteményt? Szerencsére igen, ennek több biztosítéka is van, például a címtárszolgáltatáshoz hangolt működés, és a közösen használt hierarchia.

Így aztán akár öt, akár ötezer gépről vagy felhasználóról van szó, ha van tartományunk (legyen ☺), telephelyünk, stb., a Csoportházirend adu ászként a kezünkben van, csak fel kell fordítani. Használhatjuk sokféleképpen, átfogó megoldásként vagy kiegészítő eszközként, a fókusz lehet az operációs rendszer vagy a rendszerkomponensek vagy éppen az egyéb kiszolgáló termékek, de gyárthatunk egyedi sablonokat, azaz testreszabott beállításcsomagokat is. No és persze ne feledkezzünk meg a munkaállomások és a felhasználók környezetének kialakításáról, illetve bizonyos opciók kikényszerítéséről és/vagy elrejtéséről – hiszen ez az a terület, ahol az idővel és az energiával valószínűleg a legtöbbet tudunk spórolni ☺.

6.47 ÁBRA EZ A LEGJOBB KÉPEM A CSOPORTHÁZIRENDRŐL

A Csoportházirend evolúciója a Windows 2000 Server / Professional párossal kezdődött (ami előtte volt, arról inkább hallgassunk). E két OS viszonyában kb. 630 beállítás állt a rendelkezésünkre, ami megdöbbentően nagy mennyiségnek bizonyult akkoriban. Azóta viszont minden OS váltáskor illetve szinte minden szervizcsomag esetén növekedés volt tapasztalható, amely következik egyrészt az egyre „okosabb” opciók kiötléséből, másrészt a szaporodó új komponensek lehetőségeinek lefedéséből. Ma egy Windows 7 és egy R2 esetén a tartományban használható házirend beállítások száma 3300 körüli, szóval bátran mondhatjuk, hogy eléggé aprólékosan szabályozható.

A *„fejlődés folyamatos”* kijelentés közhelynek számít ugyan, de azért igaz. Gondolkodjunk logikusan: a Csoportházirend a kliensekben megtalálható komponensek és szolgáltatások lehetőségeinek a szabályzását jelenti. Ha újabb és

újabb elemek jelennek meg egy újabb operációs rendszerben, ezeket célszerű, majdhogynem kötelező lekövetni a házirend opciók között is. Ez pontosan így volt eddig is, sőt egy-egy OS szervizcsomagja vagy akár egy-egy új Office verzió kapcsán is. Ez mindenféle szempontból irdatlanul, áttekinthetetlenül sok, de szerencsére a bővülő opciókon kívül - jó ideje először - jó pár kellemes és kényelmes változást is tapasztalhatunk a működéssel, a kezeléssel, illetve a felügyelettel kapcsolatban egyaránt. Nézzük ezeket most sorban!

6.5.1 A Central Store

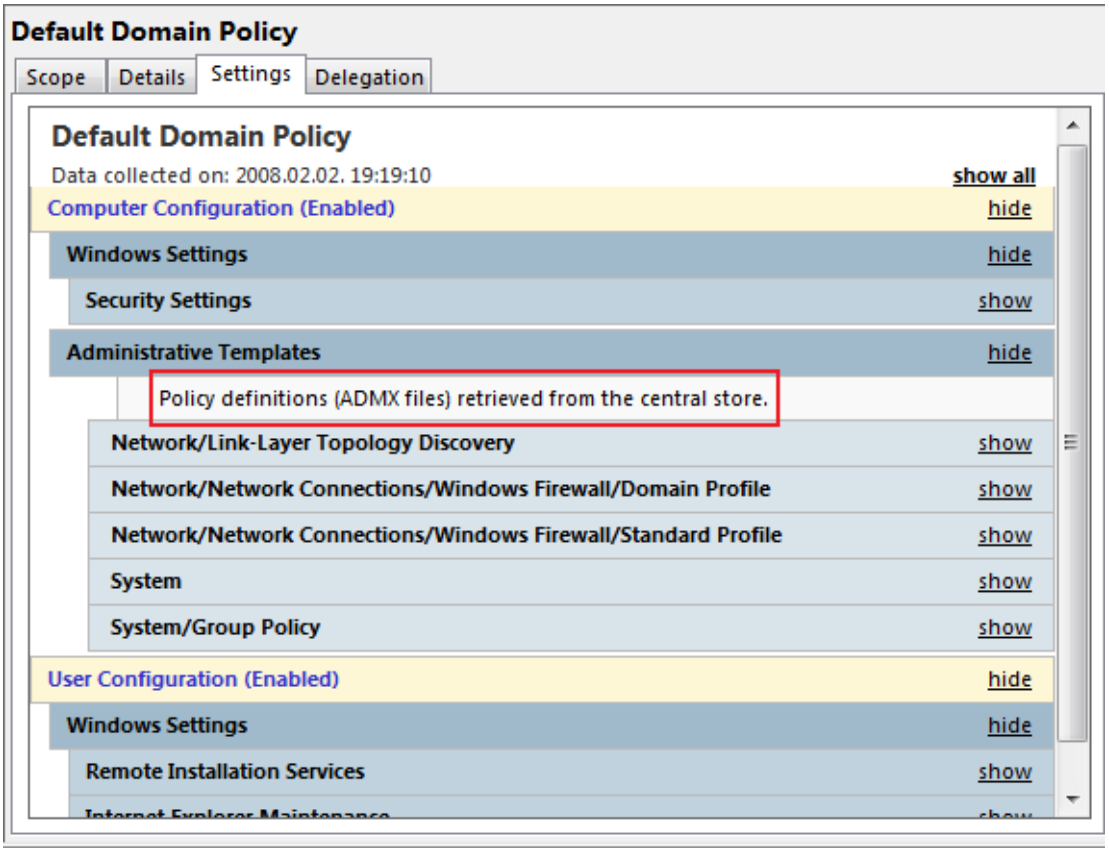
Messziről kell elkezdenünk, mivel a Central Store kialakításának az egyik előzménye a Windows Server 2008-ban és a Vistában debütált új házirend sablon formátum, az .admx és a hozzá passzoló nyelvi sablonok, azaz az .adml fájlok megjelenése. A hagyományos, már az NT-kben is megtalálható .adm formátumú sablonok finoman szólva számtalan hiányossággal küzdenek, ezek egyike a SYSVOL mappa túlterhelése. Azaz ha tartományban létrehozunk egy új csoportházirend objektumot, akkor, ha esik, ha fúj, a GPO mappájába az alapértelmezett .adm fájlok, azaz az Administrative Templates szakasz sablonjai automatikusan bemásolódnak. Ez összesen 4-5 fájlt jelent, a Windows Server 2003 SP2 esetén, kb. 4 Mbyte méretben, teljesen üres állapotban. Gondoljunk bele, többtíz esetleg még több GPO esetén (akkor is, ha egyetlen beállítást teszünk meg) számolnunk kell az újabb 4 Mbyte-tal. Replikáció, telephelyek, alacsony sávszélesség, mondjam tovább? Pazarlás, az biztos. Nevet is adtak ennek a jelenségnek, ez az ún. *SYSVOL Bloat*.

Nos a Vistától kezdődően a gyári sablonok összmérete nem, a registry alapú működés szintén nem, ellenben a sablon formátuma és mennyisége megváltozott. 132 darab (ez a szám a Windows 7-nél már jóval magasabb) XML alapú, tartalmában a nyelvi elnevezésektől teljesen elválasztott .admx fájlunk van a Windows\PolicyDefinitions mappában minden egyes kliensen illetve a szervereken is. Plusz ugyanebben a mappában lehetnek még további mappák is, a nyelvi fájloknak (.adml), amelyekből értelemszerűen szintén 132 db van. Ezek elnevezése nem tetszőleges, a mappa neve kötelezően csak az adott nyelvre egyértelműen utaló rövidített változat lehet, pl. En-US, hu-HU, stb..

Nos, el is érkeztünk végre a lényeghez, ha vesszük a bátorságot, és ezt az egész szerkezetet (a PolicyDefinitions mappát) bemásoljuk a tartományunk PDC FSMO-val rendelkező DC-jére, a SYSVOL mappába, akkor nincs sablon többszörözés, nincs pazarlás, kisebb a replikációs forgalom, mindenki örül. Konkrétan a következő helyre kell másolnunk ezt a nevezetes mappát:

SYSVOL\sajat.domain\Policies

A másolásba vegyük be a tartományunkban lévő összes nyelvű legfrissebb kliens és szerver saját .adml állományait is az említett mappákon keresztül. Ha majd frissíteni kell, akkor pedig csak felülírjuk és kész. Innentől kezdve az újabb OS-ek automatikusan észreveszik majd, hogy van központi tároló, és nem is használják majd a helyben letett sablonfájlokat egyáltalán.



6.48 ÁBRA VAN CENTRAL STORE-UNK (A KÉP EGYÉBKÉNT MÉG EGY WINDOWS 2003-AS TARTOMÁNYBAN KÉSZÜLT)

A Central Store kialakításához a kézi másolás is működik és támogatott[87], de ha ez bármilyen elképzelhetetlen okból nem megy, van hozzá egy segédeszköz is (Central Store Creator Utility), amely egy Group Policy MVP kolléga blogjáról letölthető[88].

Egyetlen megjegyzést fűznék még hozzá a sablonváltozáshoz. Ha ugyanis rendelkezünk saját .adm sablonokkal, amelyeket szeretnénk a jövőben is használni, és nem vagyunk XML guruk, akkor nekünk találták ki az ADMX Migrator segédprogramot, amiről anno jómagam is írtam egy TechNet cikket[89].

87 http://support.microsoft.com/kb/929841

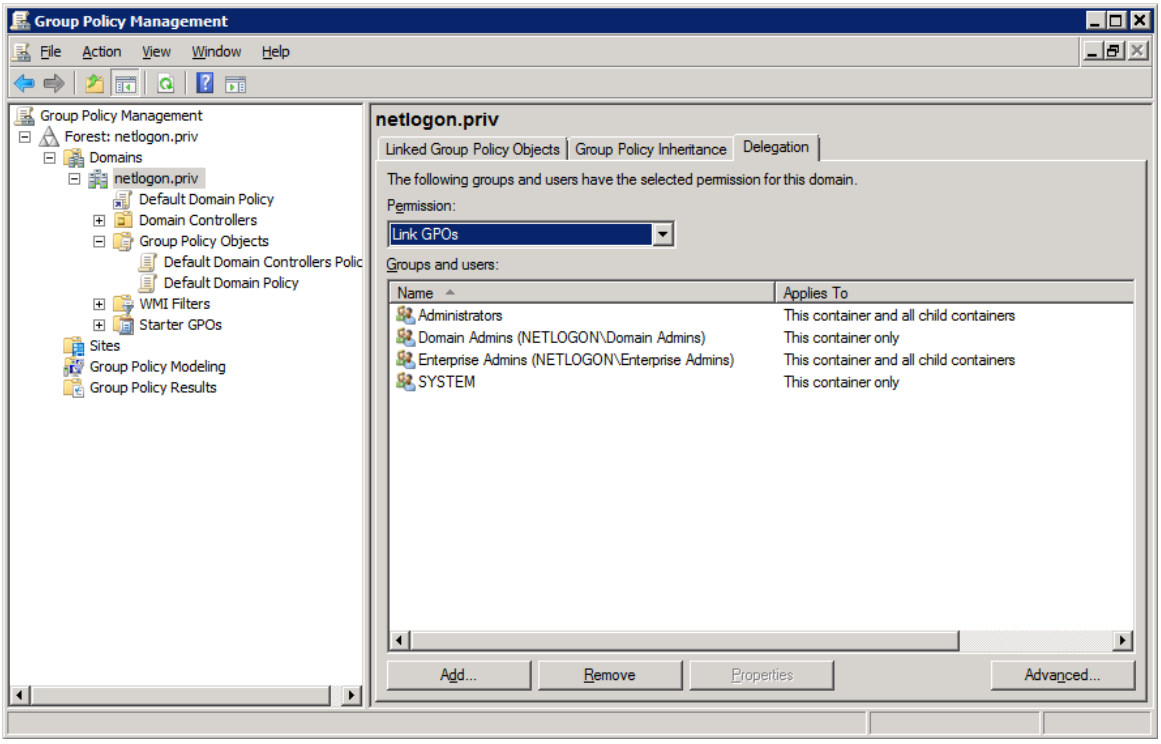
88 http://www.gpoguy.com/FreeTools/FreeToolsLibrary/tabid/67/agentType/View/PropertyID/88/Default.aspx

89 http://technetklub.hu/blogs/windowsvista/archive/2010/08/18/admx-migration-tool.aspx

6.5.2 A RÉGI-ÚJ GPMC

A lassan öt éve publikus Vistában már megtalálhattuk a Group Policy Management Console nevezetű MMC-t, azaz már csak az igazán régi motorosok emlékeznek arra, amikor még külön le kellett tölteni és telepíteni minden gépre ezt a csomagot, ha a nagyon egyszerű alapértelmezett GP Object Editor (gpedit.msc) nem bizonyult elégnek (nem bizonyult).

Ma már viszont integrált, az R2-ben elsődlegesen tehát ezt a keretprogramot használjuk, igaz itt is telepíteni kell a Server Manager-rel – a modularitás elveinek megfelelően (leszámítva a forest root DC-t, amelyre mindig felkerül automatikusan). Kliens oldalon ellenben kicsit cifrább a helyzet, mert a Vista még tartalmazta, a Vista SP1-ből azóta viszont kikerült. Ellenben az RSAT minden esetben tartalmazza, tehát ha a rendszergazda a saját gépére ezt a csomagot felrakja, akkor az összes többi felügyeleti eszköz mellett az új GPMC-t is használhatja.

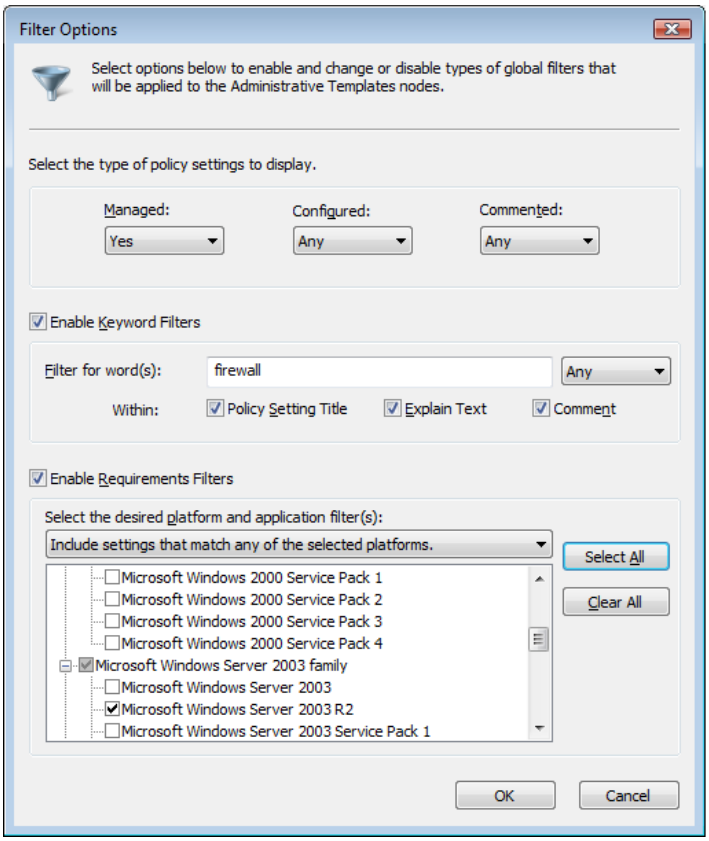


6.49 ÁBRA A GPMC

6.5.3 SZŰRÉS, KOMMENTEK ÉS AZ „ALL SETTINGS” NÉZET

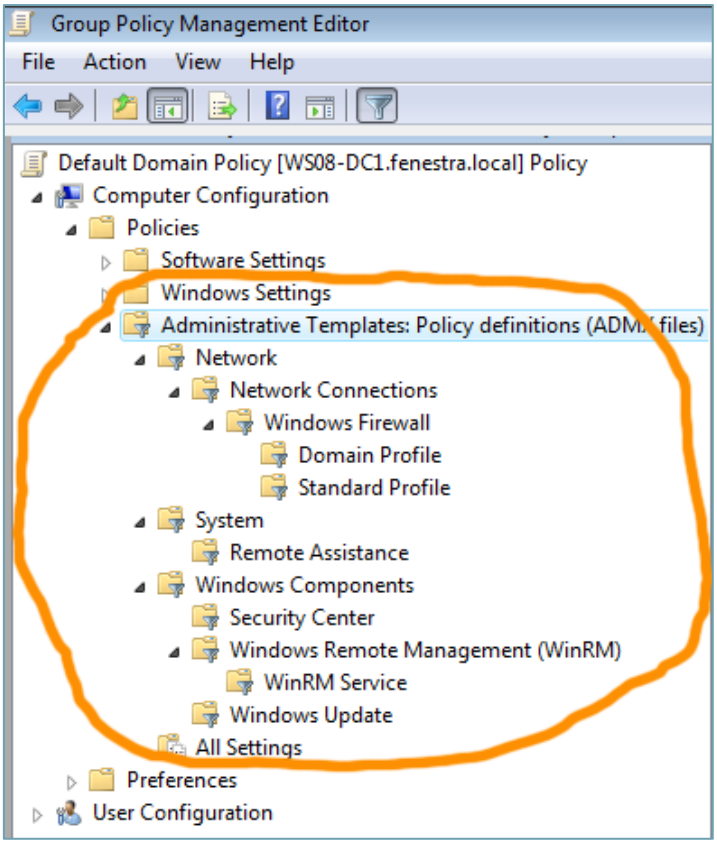
Nos tehát, melyek azok az előnyök, amelyek miatt megéri ilyen bonyolult módon előkészíteni és körbejárni a GPMC használatát? Például a keresés vagy inkább szűrés. Sok éve és sok mindenre használom a Csoportházirendet, de azért van, hogy egy ismerős opciót percekig keresek feldúltan, de az idevágó MCP tanfolyamokon – a kezdeti Csoportházirend kábulat után - a hallgatók első és teljesen logikus kérdése is mindig ezzel kapcsolatos.

No és ez persze egyre és egyre rosszabb, mivel az opciók száma folyamatosan nő. Még akkor is, ha a szerkezet most már nagyon részletes, azaz egy-egy csoportházirend objektumban, az Administrative Templates-en belül a „System” és a „Windows Components” alatt sok és értelmesen elnevezett ágra bomlik a tartalom. De ez nem elég, jó párszor előfordul, hogy egy-egy komponenssel kapcsolatos beállítások eltérő helyeken is megtalálhatóak, és pont amiatt az egyetlen más helyen megtalálható plusz beállítás miatt nem működik a jól kitalált felhasználó „kínzó” elképzelésünk ☺.



6.50 ÁBRA SZŰRÉS, NAGYON ALAPOSAN

Szóval, ha minden egyes opciót szeretnék látni, ami például a „firewall”-lal kapcsolatos, akkor az új GMPC-ben rá tudunk keresni erre (az Administrative Templates szakaszon belül), azaz kiszűrhetjük ezeket az opciókat egy egyéni nézetbe (jobb gomb: „Filter Options”). Ilyenkor csak azok a tárolók látszanak a bal oldali keretben, amelyek azokat az opciókat tartalmazzák, melyben szerepel a keresett szó (illetve az „All Settings” alatt megtaláljuk az összeset, egy listában).



6.51 ÁBRA A SZŰRÉS EREDMÉNYE A BAL OLDALI KERETBEN

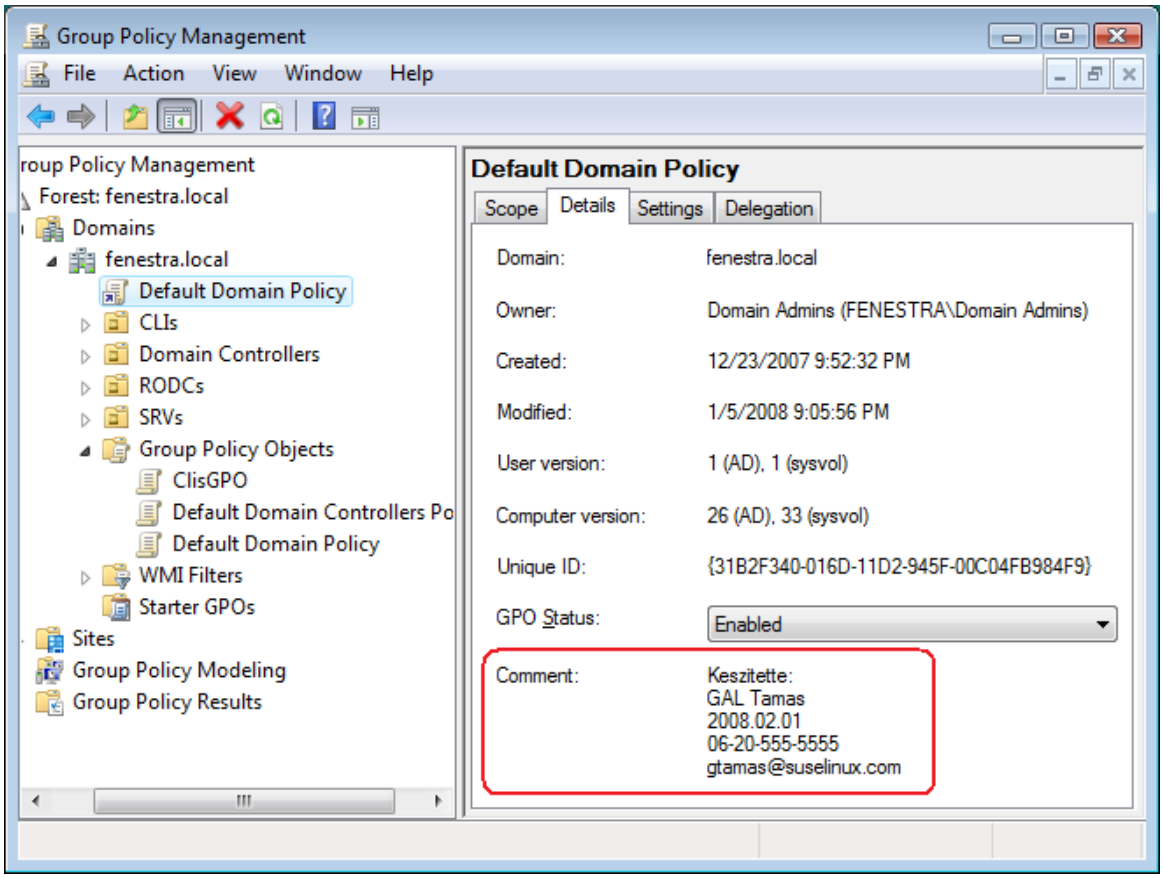
A Filtering panelt (legelső kép) jobban megvizsgálva találhatunk jó pár érdekességet. Szűkíthetjük a keresést az „igazi”, azaz a menedzselhető opciókra, vagy mondhatjuk azt is, hogy csak azok a beállítások érdekelnek bennünket, amelyekhez már korábban hozzányúltunk, de szűrési opció lehet a felhasználói megjegyzések megléte is (erről majd később). Ha kulcsszót írunk be, akkor nemcsak az adott beállítás szövegében, hanem a gyári magyarázatok, illetve a felhasználói megjegyzésekben is kereshetünk (ezek miatt látszik annyiféle találat a második képen a „firewall” szóra).

Ráadásul tovább szűkíthetünk egy terjedelmes listából az operációs rendszer, a szervizcsomag vagy akár a különböző komponensek kiválasztásával. Szóval a Windows 2000 óta várjuk a keresés/szűrés lehetőségét a Csoportházirendben, rengeteg ideje nélkülözzük már ezt a lehetőséget, de most végre megkaptuk – ráadásul eléggé kimerítő módon.

A keresés, szűrés, rendezés témaköréhez tartozik még két újdonság is. Az egyik a korábban már említett felhasználói megjegyzések bevitelének lehetősége. Minden egyes opcióhoz szabadon fűzhetünk hozzá megjegyzéseket, ami elsőre nem tűnik valami nagyon fontos lehetőségnek, pedig az. Ha például többen hangoljuk a Csoportházirendet, akkor ha lelkiismeretesen végezzük ezt, azaz kommentezünk rendesen, akkor mindig tudni fogjuk, hogy ki és miért állította be az adott opciót. De tegyük a szívünkre a kezünket: ha csak egyedül konfigurálunk, akkor is emlékszünk

arra, hogy egy februári ködös péntek estén, három évvel ezelőtt miért állítottuk be ezt vagy azt? Én nem szoktam, ezért aztán néha vad fejtörésbe kezdek – ami így talán nem lesz szükséges.[90]

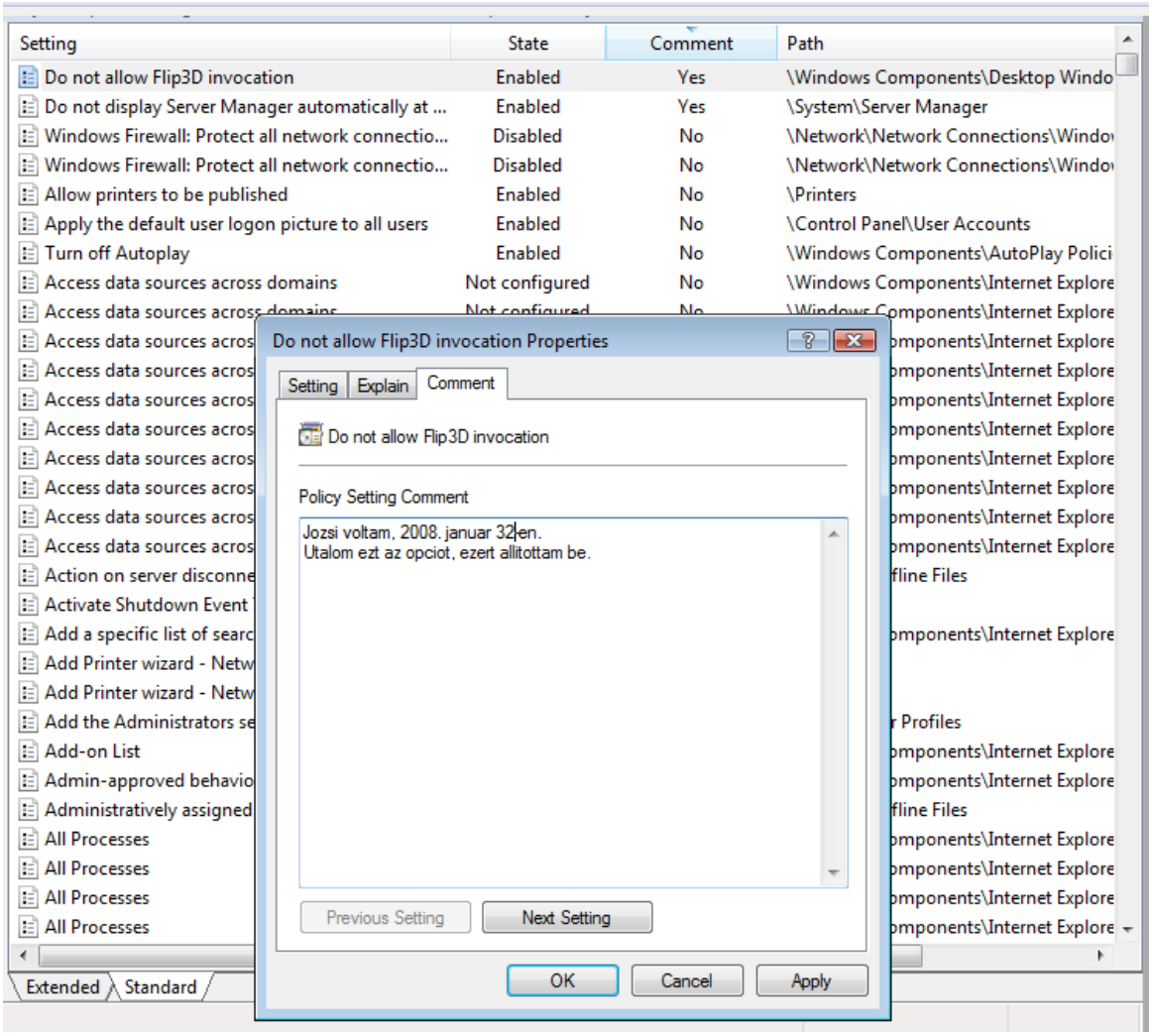
Egyébként az Administrative Templates szakaszon kívül még egyetlen helyen használhatjuk ezt a lehetőséget, az adott házirend objektum tulajdonságai között, ami szintén hasznos lehet egy-egy nagyobb szervezetben. Arról már ne is beszéljünk, hogy az előbbi kommentek .cmtx, az utóbbi pedig .cmt formátumban (Notepad-del szerkeszthetően) megtalálhatóak az adott GPO mappájában, a SYSVOL-on belül!



6.52 ÁBRA KÖNNYŰ ELIGAZODNI A GPO-K KÖZÖTT IS

Egy másik lehetőség az összes létező opció egyetlen listába zsúfolása (All Settings). Ez szintén egy Administrative Templates hatókörű művelet, külön a gépek, illetve külön a felhasználók esetén. Ilyenkor a gépek esetén 1648, a felhasználóknál pedig 1454 db opciót a jobb oldali keretben láthatunk, alapesetben ABC sorrendben, de van lehetőség rendezni az opció állapota, az esetleges kommentek vagy az elérési útvonal szerint. Ráadásul nem egy passzív listát kapunk, hanem bármelyik elemre kattintva rögvest szerkeszthetjük is az opciót (korábban elfelejtettem jelezni, hogy ez a szűrés esetén is ugyanígy van).

[90] A közös emlékezést segítheti a Microsoft Desktop Optimization Pack „Advanced Group Policy Management” eszköze, amely még jóváhagyási folyamatokat is tartalmaz egy-egy GPO változáshoz (a lektor megjegyzése).
http://technet.microsoft.com/en-us/library/ee532079.aspx



6.53 ÁBRA ALL SETTINGS NÉZET, KOMMENTEK SZERINT RENDEZVE, ÉS EGY FONTOS MEGJEGYZÉS AZ ADOTT BEÁLLÍTÁSON

Az Explain text, azaz a gyári „magyarázó” szöveg kibővítése is ehhez a témához tartozik még, sok-sok helyen újraírták, értelmesebbé és használhatóbbá tették ezeket a magyarázó szövegeket, ergo érdemes időnként megnézni.

> És egy megjegyzés: ha valamivel ezekben nem értünk egyet, hibát találunk benne, vagy jobbat tudunk írni, akkor a Group Policy Team szívesen fogadja az alternatívákat a gptext@microsoft.com e-mail címen.

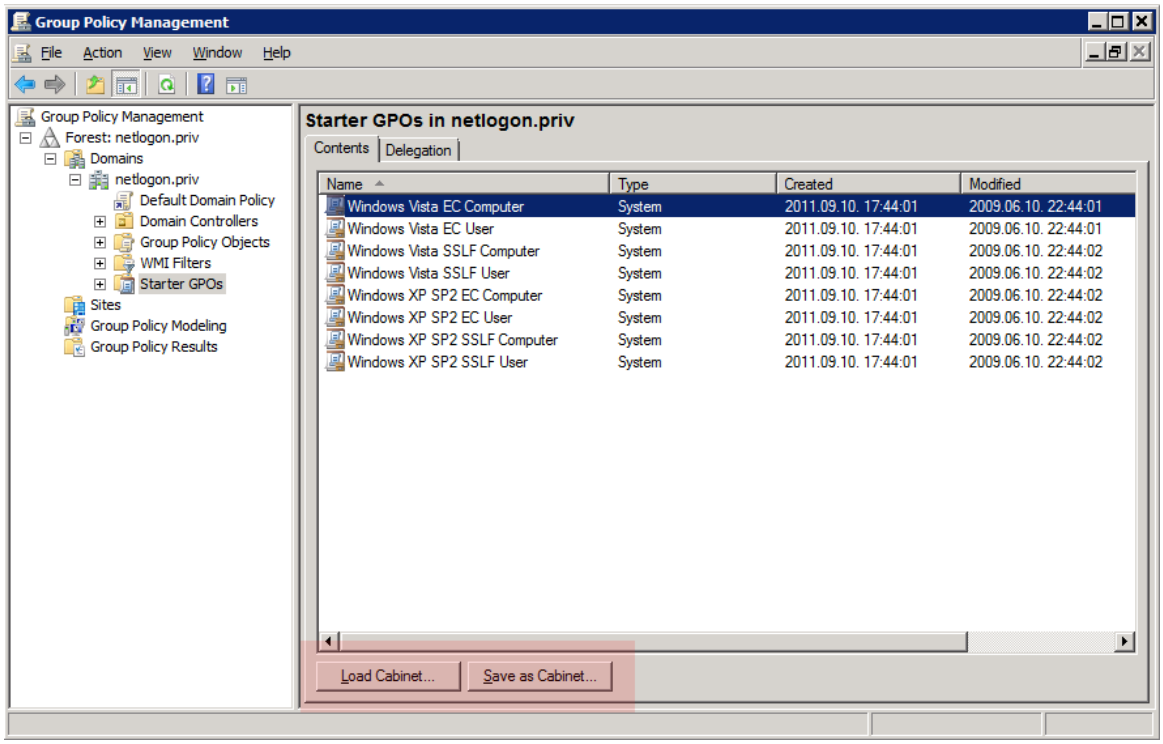
6.5.4 STARTER GPO-K

Képzeljük el, hogy szükségünk van 5 darab GPO-ra, amelyben egyenként 100-100 opciót fogunk beállítani! A 100-ból 50 ugyanaz lesz (mert mondjuk ezek a céges alapkövetelmények), a maradék 50-nek viszont teljesen eltérőnek kell lennie. Mit csinálunk? Régóta vannak már sablonjaink (lásd: Security Templates MMC) a Csoportházirendhez, de ezek tipikusan biztonsági sablonok, az Administrative Templates szakaszra nem vonatkoznak, nekünk pedig kifejezetten a gépek és a

felhasználók környezetével és a komponensekkel kapcsolatos konkrét beállításokra lenne szükségünk...

Nos, a Windows Server 2008-tól kezdve használhatjuk erre a célra az ún. Starter GPO-kat. Ezek is egyfajta sablonok, amelyeket nekünk kell előzetesen, és egyszer elkészíteni (a rendszerrel egy darab sem érkezik, ez is egy eltérés a biztonsági sablonokkal összehasonlítva). Az új GPMC-ben külön menüpontot kapott a Starter GPO szakasz, és ha elvándorolunk ide, akkor első lépésben engedélyeznünk kell a Starter GPO mappa létrehozását (Create Starter GPOs Folder gomb, a SYSVOL-on belül ugyanúgy létrejönnek majd a GUID-dal jelölt mappák ehhez is).

Ezután vagy használjuk az alaphelyzet szerint itt szereplő[91] 8 darab GPO közül az egyiket, vagy elkezdhetjük létrehozni az első sablont, amelyben láthatóan nincs is más, mint a két Administrative Templates szakasz (azért ne becsüljük le ezt a jelenleg több mint 3000 opciót tartalmazó részt ☺). Ha megtesszük a szükséges alapbeállításokat, és bezárjuk az új sablonunkat, akkor egy új GPO készítése előtt akár választhatunk is ezen sablonok közül kiindulópontként egyet, és máris lesz mondjuk - a példa szerinti helyzetben - 50 beállításunk.



6.54 ÁBRA A STARTER GPO FELHASZNÁLÁSA

Szeretném a figyelmet felhívni a piros keretben szereplő két nyomógombra. Szerepük fontos, mivel a hordozhatóságot szolgálja, azaz ha egy Starter GPO-t elmentünk .cab formátumba, akkor egy másik rendszerben is elérhetővé tudjuk tenni a „Load

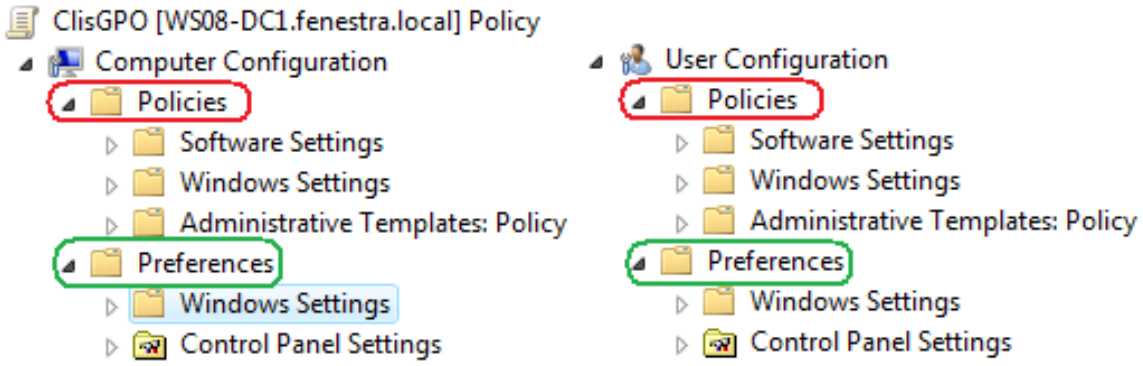
[91] A Windows Server 2008-ban ne keressük ezeket, mert ez egy R2-es újdonság.

Cabinet" paranccsal. Ezek ismeretében szimpla ügy lesz felszerelni magunkat néhány hasznos Starter GPO-val.

6.5.5 Group Policy Preferences

2006 őszén a Microsoft megvásárolta a Desktop Standard nevű céget, melynek volt egy remek alkalmazása ami lehet, hogy néhány Olvasónak még ismerős: ez volt a PolicyMaker. Nos, ezt az alkalmazást jelentősen átírták és testre szabták, majd teljesen beépítették a Windows Server 2008-ba (és az RSAT-ba is), és Group Policy Preferences néven fut azóta is.
Annyira fontos és annyira más, hogy a GPO-kban egy teljesen külön főágat kapott. Még akkor is így van ez, ha összesen kb. 90-100 opciót tartalmaz csak (de ez igazából sokkal több, mert egy-egy ponton akár 30-40 dolgot is állíthatunk), tehát mennyiség szempontjából nem összemérhető a hagyományos házirendekkel. De más szempontból sem összemérhető, ugyanis a hatása nem kötelező a felhasználókra nézve, hanem csak ajánlásnak számít, azaz a felhasználó, ha akarja, megváltoztathatja az általunk előre definiált beállítást.

Természetesen ugyanúgy központilag hangoljuk, és ugyanúgy frissülhet is (a kliensen 90-120 percenként), ráadásul külön-külön van itt is gép/felhasználó hatókör (bár a hasonlóság az opciók típusa és értelme között azért jóval kisebb, mint az alap házirendeknél). Amit még meg kell jegyeznünk, hogy ha egy hagyományos házirend opció és egy Preferences opció „összeakad", akkor mindig a hagyományos „nyer", de ez logikus is.



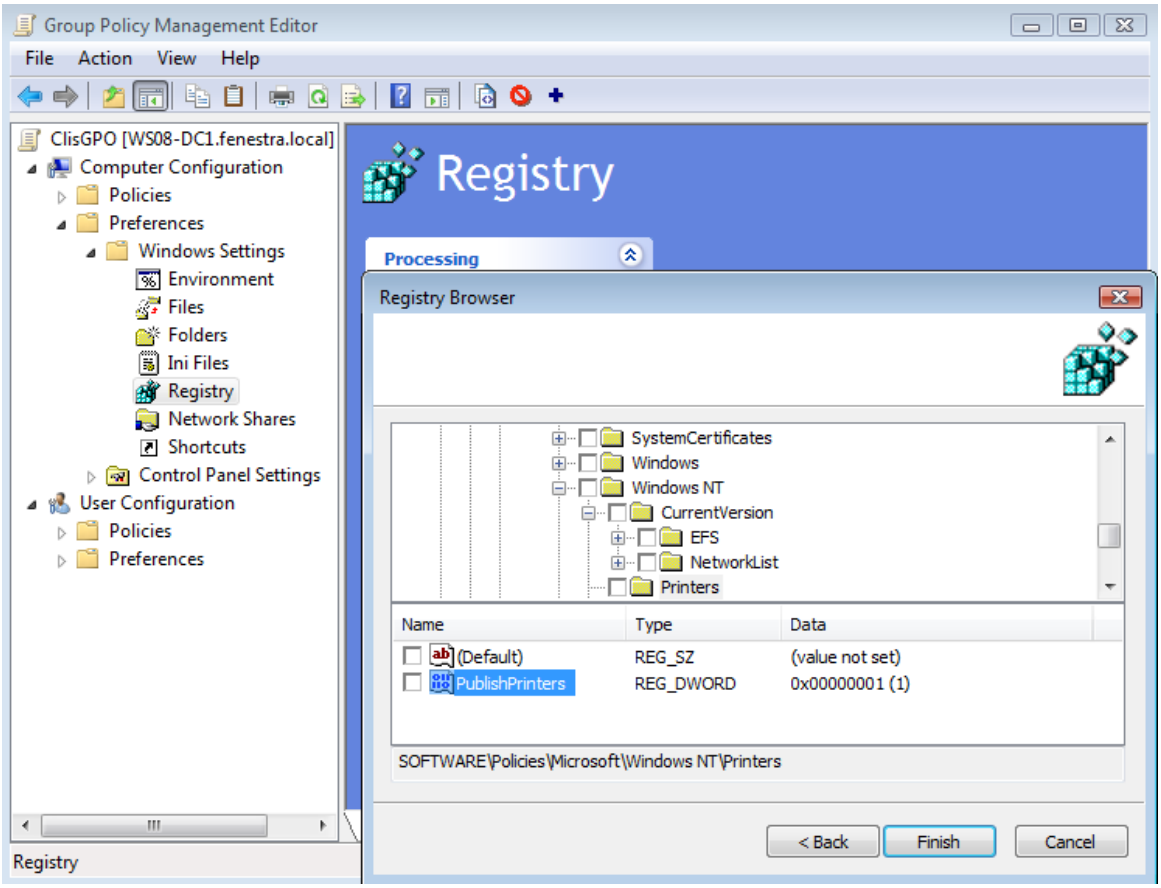
6.55 ábra Policies és Preferences 2x is egy-egy GPO-n belül

A GPP rengeteg olyan kellemes lehetőséget ad a rendszergazdák kezébe, amely eddig kimaradt a hagyományos házirendekből, beszéljünk tehát tételesen ezekről, először a számítógépekre vonatkozó opciók közül a „Windows Settings" körben:

- Environment szakasz: Létrehozhatunk, módosíthatunk, kicserélhetünk és törölhetünk környezeti változókat.
- Files és Folders: Létrehozhatunk, módosíthatunk, frissíthetünk és törölhetünk fájlokat és mappákat! Mindkét szakaszban számos lehetőség van a létrehozás

után a mappák és fájlok tulajdonságainak megváltoztatására is, valamint pl. törlés esetén is válogathatunk a lehetőségekből.

- INI Files: Létrehozhatunk, módosíthatunk, kicserélhetünk és törölhetünk .ini fájlokat, némi befolyással a szerkezetre is.
- Registry: Szintén minden alapművelet elvégezhető a registry esetén is, sokféle érték típust érintve – szemben a régi sablonok fapados lehetőségeivel. Sőt, elindíthatunk egy varázslót is, mellyel csatlakozhatunk a távoli géphez, így „élesben" tudunk a registry értékein változtatni (ehhez persze a távoli gépen futnia kell a Remote Registry szerviznek, a Vistán ez már nem alapértelmezett).

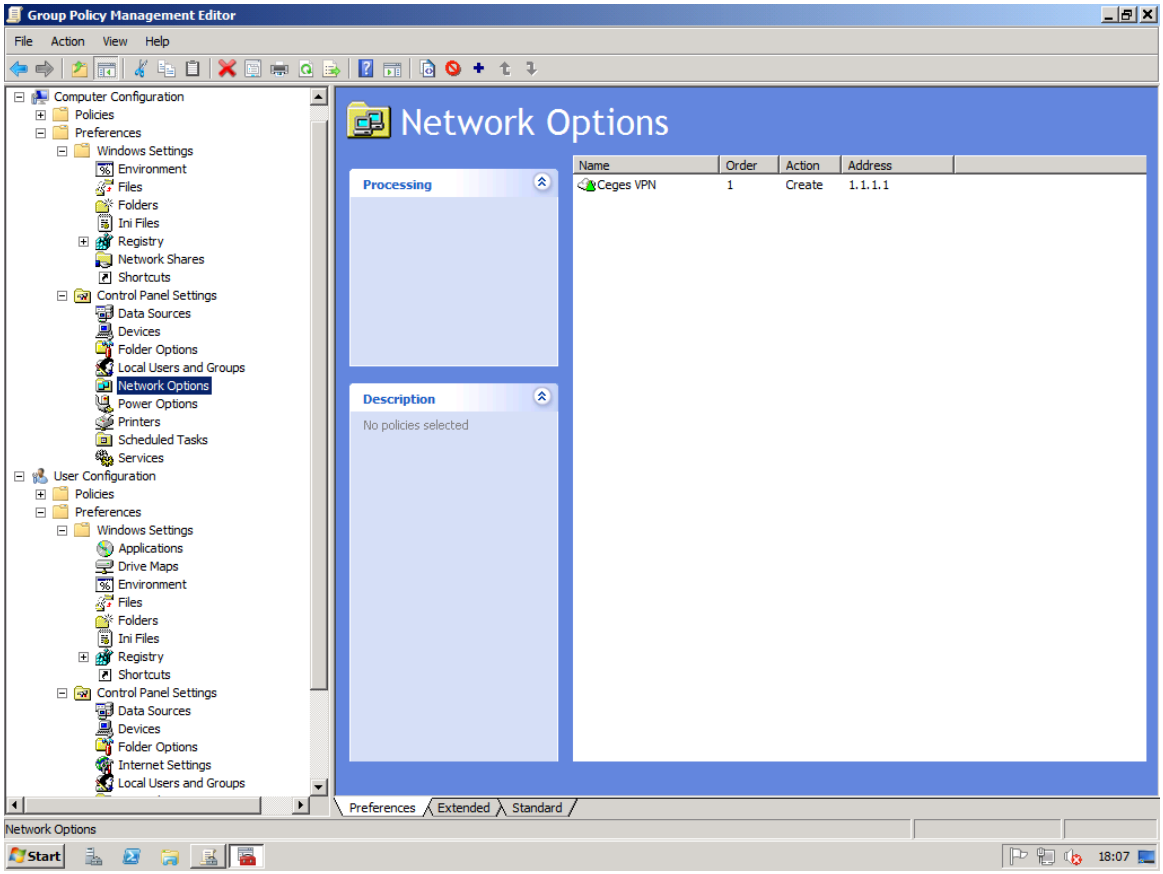


6.56 ÁBRA MŰKÖDIK A KLIENSHEZ KAPCSOLÓDÓ ÉLES REGISTRY VARÁZSLÓ

- Network Shares: Létrehozhatunk hálózati megosztásokat is, minden egyes a klasszikus módon is elérhető jellemzőjével együtt, sőt az Access-based Enumeration (magyarul: csak azt látja a felhasználó, amihez van jogosultsága) opciók is elérhetőek.
- Shortcuts: szintén elérhető minden alapművelet a parancsikonokkal kapcsolatban is.

Van folytatás is még a gépek házirendjénél, és ez a Control Panel kör, ahol a következő szakaszok találhatóak meg.

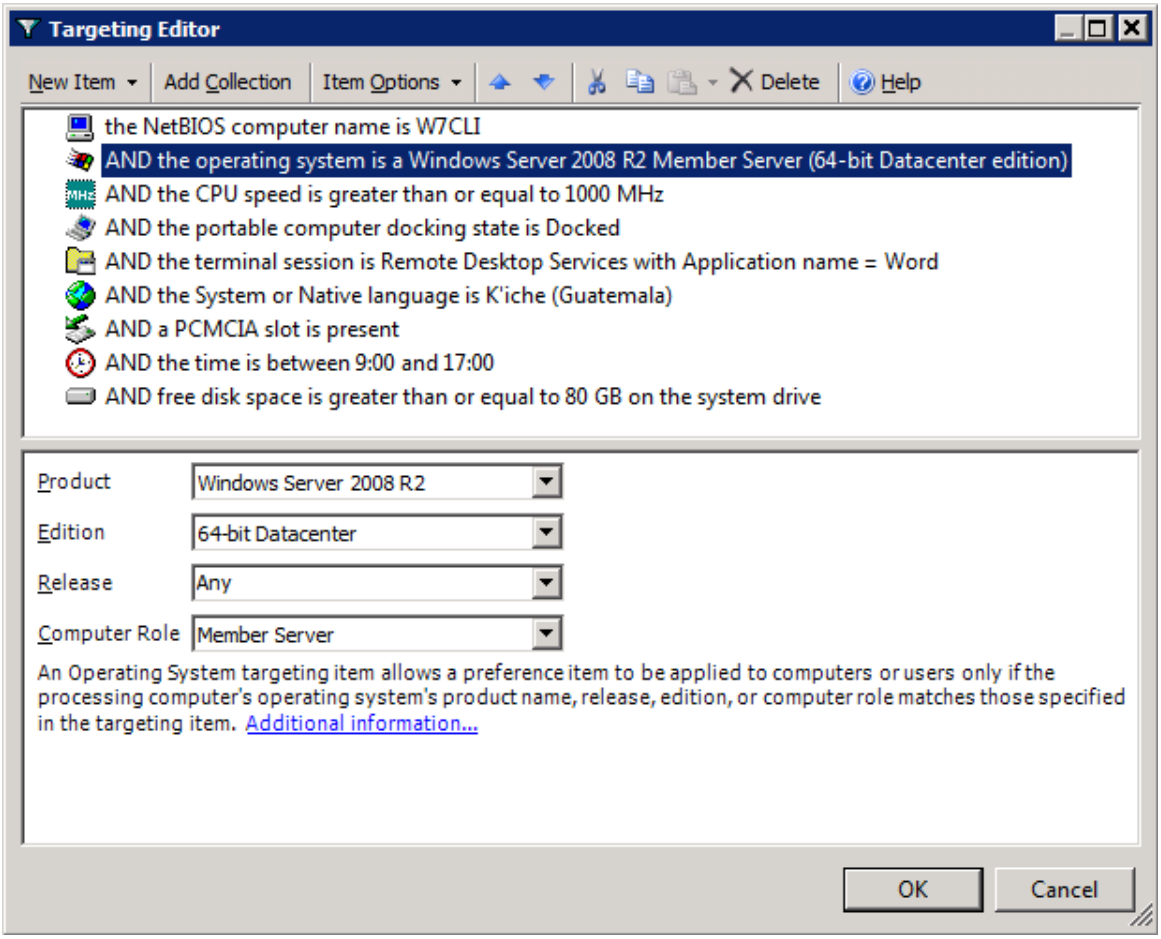
- Data Sources: Létrehozhatunk, módosíthatunk, frissíthetünk és törölhetünk DSN-eket és adatforrásokat is konfigurálhatjuk, ugyanúgy mint az ODBC panelen a Vezérlőpultban.
- Devices: engedélyezhetünk vagy tilthatunk eszközmeghajtókat a class ID-jük alapján, nagyjából hasonlóan, mint az eredeti (Vista) házirendben.
- Folder Options: kicsit más, mint fent, a fájltípusok, a fájl-összerendelések körét szélesíthetjük vagy szűkíthetjük.
- Local Users and Groups: minden (!), amit egyébként tudunk művelni a helyi felhasználókkal és/vagy a csoportokkal. Persze először létre kell hozni ezeket, bár az Administrator és a Guest felhasználókat alapértelmezés szerint is tudjuk kezelni így.
- Network Options: Hihetetlen, de igaz: innen indulva képesek leszünk minden részletre kiterjedő VPN és DUN kapcsolatokat létrehozni a kliensen. Mindenre gondoltak, eldönthetjük, hogy egy vagy az összes felhasználónál jelenik majd meg a kapcsolat, elérhetőek a tárcsázási, a hitelesítési és egyéb opciók is. Ha van már azon a gépen VPN kapcsolatunk, amelyiken konfiguráljuk a GPP-t, azt például importálhatjuk, elképesztő...
- Power Options: Itt gyárthatunk opciókat és sémákat az energiaellátás opciókörben (csak Windows XP esetén).
- Printers: TCP/IP és lokális (!) nyomtatókat hozhatunk létre. LPT/USB/COM portokat, IP címet és minden más nyomtató tulajdonságot is konfigurálhatunk itt.
- Scheduled Tasks: Létrehozhatunk, módosíthatunk, frissíthetünk és törölhetünk időzített feladatokat.
- Services: A rendszerszolgáltatásokat illetően is számos lehetőségünk van, igaz, ez nem sokban különbözik a szimpla házirend esetén ismerős opcióktól.



6.57 ÁBRA KIBONTOTT GPP ÁGAK ÉS EGY MOST KONFIGURÁLT VPN KAPCSOLAT

Ezek mellett a felhasználókra is van egy-egy „Windows Settings” és egy „Control Panel” szakasz, de ennek (néhány esetben szintén szenzációs) részleteitől már megkímélem a kedves Olvasót, nézzük meg önszorgalomból, megéri.

Attól viszont nem kímélek meg senkit, hogy bemutassak még egy fontos komponenst, az ún. „Target Editor”-t, amelyet minden beállításnál megtalálunk (a Common fülről érhető el > „Item level targeting” fül > „Targeting” gomb), és amellyel egyszerűen és látványosan szűkíthetjük a beállított opciónk hatókörét. A következő képhez értelmetlen feltételeket szedtem össze, a lényeg nem is ez, hanem a sokszínűség, még legalább háromszor ennyi lehetőség van, amit nagyon egyszerűen összepakolhatunk egy közös feltételrendszerré (szóval nem kell a WMI-vel kínlódnunk). Ami lemaradt a képről, pedig különösen fontos, az a csoportokra illetve az egyéni felhasználókra történő szűrés lehetősége.



6.58 ÁBRA SZERFELETT GRANULÁRIS ÉS IDIÓTA FELTÉTELEK – CSOPORTBA SZEDVE

Már csak egyetlen fontos kérdés maradt hátra a GPP-vel kapcsolatban: mely klienseken fog működni alapértelmezés szerint, és mi lesz a többivel?
A válasz nem olyan rossz, mint amire számíthatnánk: Windows 2008-on csont nélkül, a Vista RTM, XPSP2 és Windows Server 2003 SP1/SP2 esetén egy letölthető ún. Client-Side Extension (CSE) segítségével működik a GPP. A Vista SP1 óta viszont gyárilag beépített a kliens.

6.5.6 TOVÁBBI R2-ES ÚJDONSÁGOK

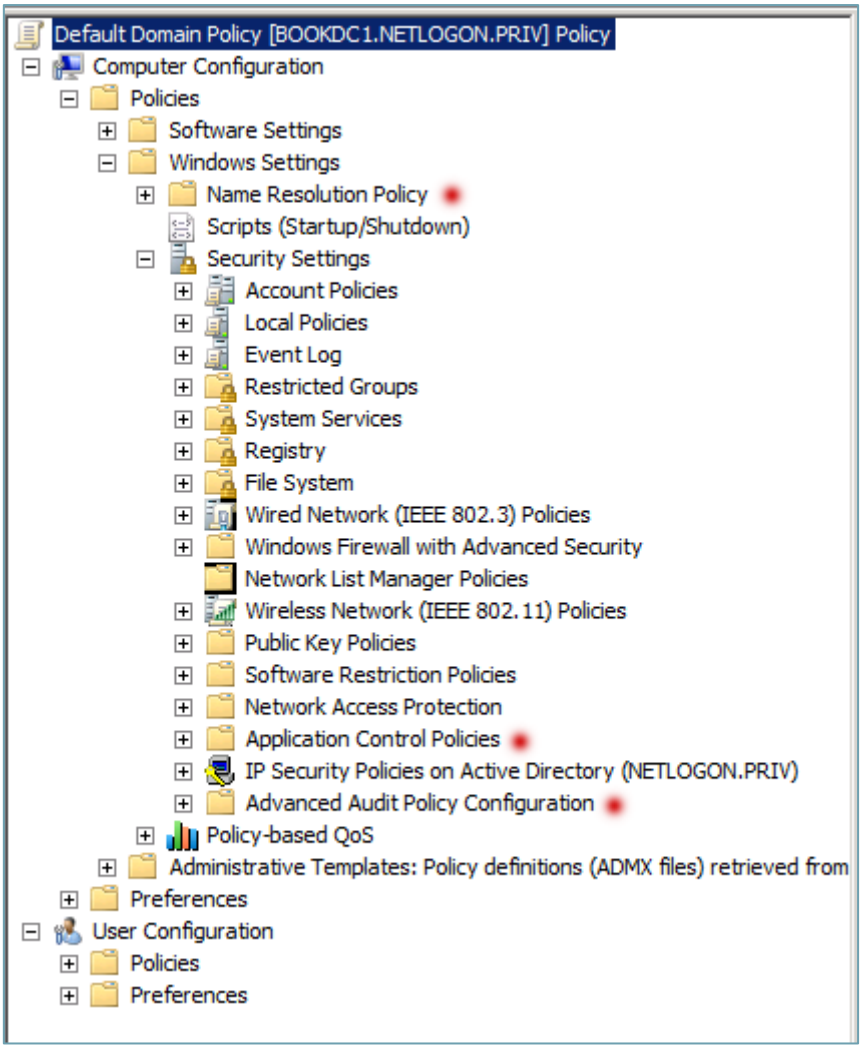
Néhány dolog megújult, több mint 300 [92] opció bekerült (IE8, Bitlocker/ToGo, Power, Taskbar, Security, WLAN, PKI, NAP, NRPT, AppLocker, DNSSec, DirectAccess, Biometric Framework), és lett 1-2 komoly és fontos újdonság is, de azért mindezt csak egy szűk felsorolás formájában fogom most ismertetni:

- Windows PowerShell Cmdlets for Group Policy
    - Ahogyan nagyon sok egyéb területen, a csoportházirendben is megjelent a PowerShell szkriptek segítségével történő menedzsment lehetősége. GPO-k létrehozása, törlése, mentése, átnevezése, valamint

[92] Ez a plusz 300 benne van az általam korábban emlegetett 3300-ban.

a direkt írás és olvasás a GPO-kban, Logon / logoff, startup / shutdown PS szkriptek mind-mind egyszerű feladattá vált.

- Group Policy Preferences
    - A Windows Server 2008-ban bemutatkozó GPP (Group Policy Preferences) szolgáltatásai ismét bővültek néhány elemmel, ezeket sem fogjuk kihagyni az áttekintésből.
- System Starter Group Policy Objects
    - Beállításokkal feltöltött 8 darab Starter GPO, bevált Microsoft ajánlások alapján
- GPP
    - Több kisebb javítás a „Targeting”-en, némi UI ráncfelvarrás és rengeteg új lehetőség a Windows 7-hez (energiaellátás, „Inmediate Task”, IE8, stb.)
- AppLocker
    - Talán ez a funkció az R2-es verzió legnagyobb Csoportházirend újdonsága, ami a jól ismert és bonyolultsága miatt kevés alkalommal használt Software Restrictions Policy új változata (az SRP azért továbbra is megvan), amely Windows 7 és Windows Server 2008 R2 alatt, az alkalmazások egyszerű, központi tiltásával/engedélyezésével könnyíti majd meg az életünket.



6.59 ÁBRA A PIROS PONTOSOK TELJESEN ÚJAK

És most, hogy végre elértünk a Csoportházirend szekció végére, különösebb kommentek nélkül megosztanék 1-2 üzemeltetési tanácsot, mert tanács az aztán tényleg kell ehhez az eszközhöz:

- Mindenképpen teszteld le a beállítások hatását!
- Először a GPO-kat csináld meg, és csak eztán kerüljenek be a kliensek a hatókörükbe!
- A GPO gyártás/szerkesztés ugyanarról az OS verzióról történjen!
- A jó cél a kevés GPO, sok és logikailag összefüggő beállítással!
- Óvatosan a „kényszerítés” és a „blokkolás” lehetőségekkel!
- Az adminoknak mindig tiltás (Deny) legyen a végrehajtáson!
- Használd bátran a parancssort és a GPMC extrákat!
- Kommentálás, dokumentálás, mentés!
- Próbáld meg a felhasználók tudomására hozni a „miért” magyarázatát! [93]

[93] Opcionális ☺

7 KIEMELT SZOLGÁLTATÁSOK

Mármint úgy értem, hogy az *általam* kiemelt szolgáltatások ☺. Ezek azok a nagyobb komponensek, melyeket nehéz beskatulyázni, mert több szerepkörrel és szolgáltatással is együtt dolgoznak. Viszont közös jellemzőjük, hogy ingyenesen elérhetőek, azaz az operációs rendszer részei, és az is, hogy igencsak innovatív megoldás mind, valamint még az is, hogy a bevezetésük vagy a működésük megértése nem egyszerű feladat – dehát nekünk muszáj szeretni a kihívásokat.

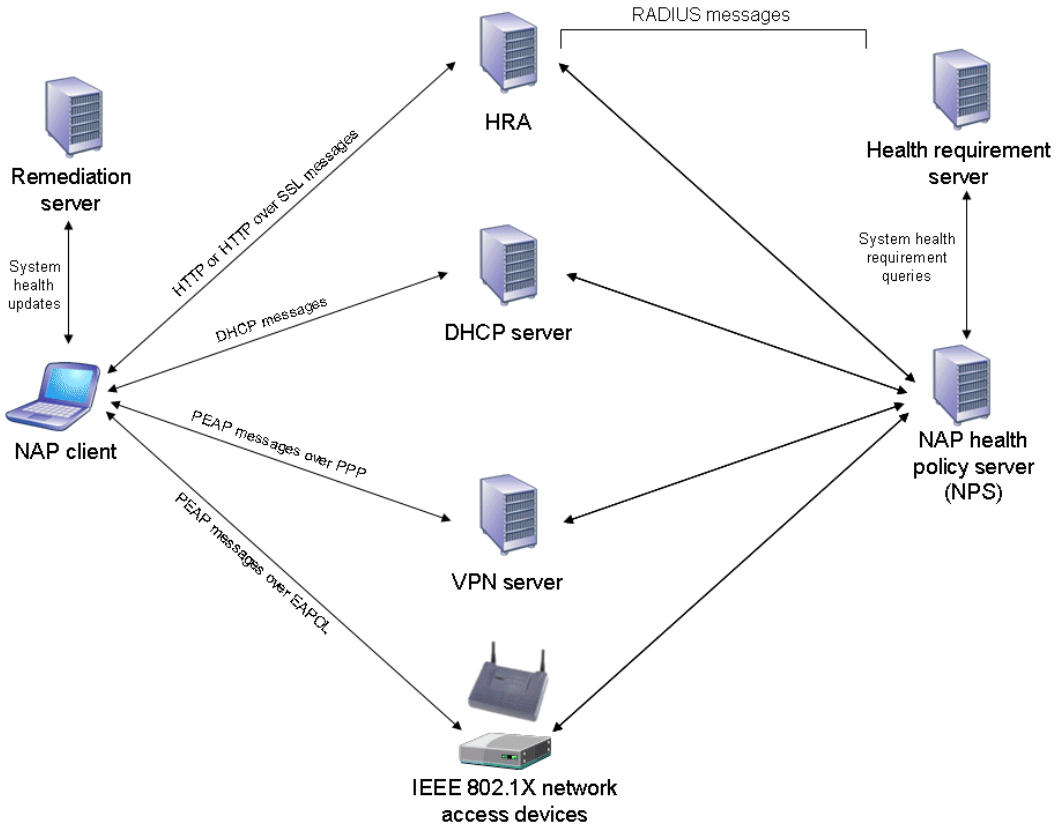
7.1 A KARANTÉNUNK, A NAP

A NAP, azaz a Network Access Protection valószínűleg a Windows Server 2008 legnagyobb – biztonsággal kapcsolatos – „dobása". A legtöbb szervezet esetén ugyanis jelentős igény mutatkozik egy olyan megoldásra, amely már a fizikai hálózat szintjén elválasztja az alkalmi csatlakozású vagy kevésbé megbízható, illetve kevésbé felügyelhető számítógépeket a belső hálózatba tartozó kliensektől és szerverektől. Tartományi környezetben ugyan van néhány eszközünk a biztonsági határok felállítására, a központi felügyeletre és a renitens gépek „móresre tanítására", de sok esetben még ez is kevésnek bizonyul, vagy éppen nem alkalmazható.

Viszont a fizikai vagy a távoli hozzáférés szintjén egyáltalán nem rendelkezünk ezekkel az eszközökkel, ugyanakkor nagyon sok esetben nem tagadhatjuk meg teljesen a hozzáférést a hálózatra szükségszerűen jogosan kapcsolódó (nem tartományi) gépektől sem. Erre a láthatóan nehezen megoldható helyzetre nyújthat gyógyírt a NAP, azaz egy olyan szerver–kliens megoldás, amely a védett hálózatunkban alapértelmezés szerint még az IP-kapcsolatot sem engedi meg, és amely csak egy alapos, az üzemeltetők által részletesen hangolható „*vizsga*" sikeres teljesítése esetén adja meg a hozzáférést a belső hálózathoz kapcsolódni szándékozó gépeknek. De a NAP nemcsak az ellenőrzést oldja meg, hanem az elutasított gépek lelőhelyének, azaz a karanténnak a vezérlését és az automatikus állapotjavításhoz szükséges folyamatokat is képes kézben tartani.
A NAP célja tehát tömören az, hogy a routerek, switchek, a vezeték nélküli hozzáférési pontok, a szoftveres és az appliance (hardverbe épített célszoftver, például egy Forefront TMG) rendszerek segítségével érvényesítse a végpontokon a biztonsági elvárásainkat. Mindezt úgy éri el, hogy lekérdezi a hálózatra csatlakozó eszközök „egészségi" állapotát (bekapcsolt tűzfal, Windows Update kliens, vírus/spyware-irtó állapota, sőt külső gyártótól származó sablonok[94], stb.), majd ezt összehasonlítja az általunk előre definiált szabálycsomaggal, és az eredmény alapján dönt a hálózati hozzáférés engedélyezéséről. Ha a folyamat negatív eredménnyel zárul, a

[94] Mára (2011) rengeteg külső gyártó is támogatja, százas nagyságrendben (http://www.microsoft.com/en-us/server-cloud/windows-server/network-access-protection-nap.aspx).

kapcsolódni szándékozó kliens nem jut be a védett hálózatba, hanem lehetőséget kap biztonsági állapotának „szintre hozására”, azaz csatlakozhat a publikus szegmensen működő „*patikaszerverekhez*[95]”, pl. egy WSUS-hoz/SCCM-hez vagy a vírusirtó- szignatúrákat tároló szerverhez, majd a szükséges korrekció után (ami lehet automatikus is, lásd auto-remediation[96]) végrehajthat egy újabb kapcsolódási kísérletet, és ha „egészséges”, akkor beengedjük a hálózatba[97].



7.1 ÁBRA AZ ÖSSZES KAPCSOLÓDÁSI KÖZEG

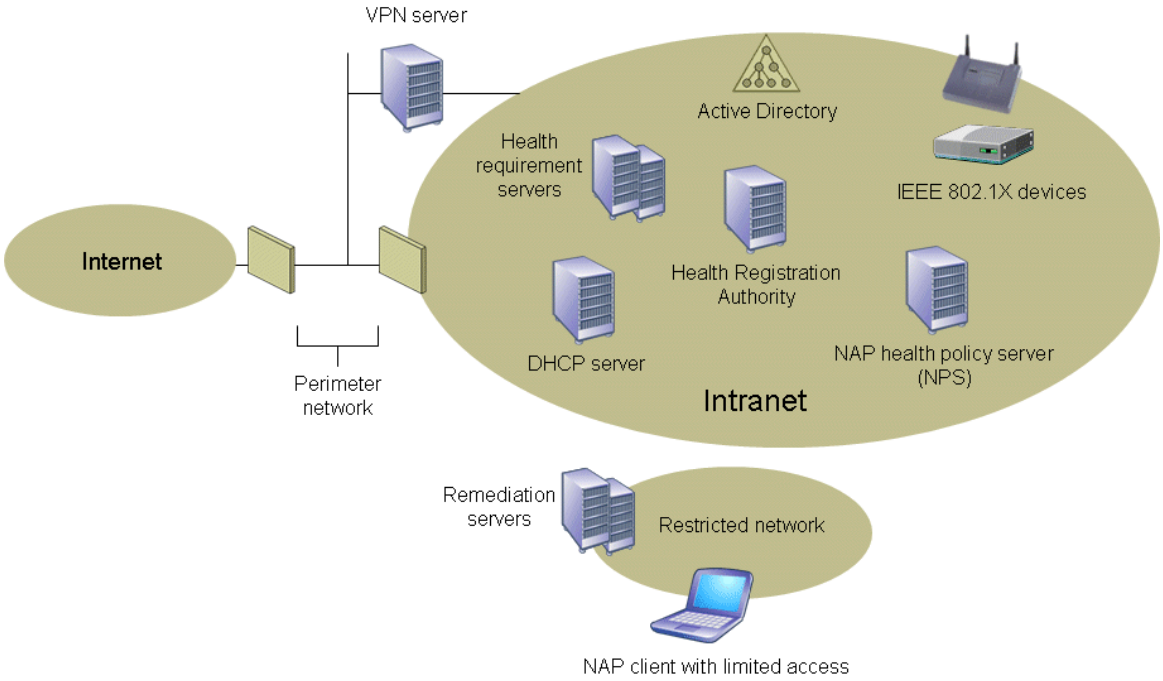
A korrektség kedvéért említsük meg a NAP egyetlen előzményének tekinthető – már a Windows Server 2003-ban és az ISA 2004/2006 kiszolgálókban is jelenlévő – VPN-karantén megoldást, de csak azért, hogy kiderüljön: mélységében és használhatóságában egyaránt nagyon különbözik a NAP-tól. A legjobb példa erre a beléptető közeg, ugyanis a VPN karantén értelemszerűen csak a VPN kapcsolatok esetén volt használható, míg a NAP a vezetékes, a vezeték nélküli és a RAS/VPN kapcsolatok esetén is, illetve a kapcsolódás típusa alapján a DHCP-, IPSec- vagy éppen az RDP kliensekre is alkalmazható.

[95] Fóti Marcell szenzációs elnevezése.
[96] Magyarul bekapcsolja a kikapcsolt tűzfalat.
[97] Ha sokáig nem viselkedik „rendesen”, akkor viszont a karanténból is kikerülhet (mivel konfigurálható az itt tölthető időtartam), azaz meg is szakítható a kapcsolat.

Fontos azt is tudni, hogy az első NAP kiszolgáló a Windows Server 2008 volt, kliensoldalon viszont a Vista már tartalmazza a megfelelő összetevőket, de egy jó ideje már elérhető az XP SP2-re telepíthető NAP kliens is, de sokkal logikusabb (más okokból is nyilván) XP SP3 használata, mivel ez is gyárilag tartalmazza a NAP kliens alkalmazást. Ha van a gépünkön NAP kliens, és működik a NAP infrastruktúra is, akkor viszont az ellenőrzése folyamatos, tehát dinamikusan változhat a számítógépünk elhelyezése, azaz ha a feltételeket nem teljesíti a gépünk, egyből a karanténban találhatja magát. Ezek után tisztázzunk egy-két ismeretlen fogalmat, illetve további elemet, amelyek a NAP hierarchia részei a kliensoldalon:

- System Health Agent (SHA): Feladata a kliens rendszer alkalmasságának ellenőrzése, majd ennek az információnak a jelentése.
- Enforcement Client: A kliens kapcsolódási metódusát jelöli. Minden hálózati hozzáférési típushoz (lásd később) egy-egy külön NAP EC áll a rendelkezésre. Ha például a klienseink a DHCP-vel kapcsolódnának a NAP kiszolgálóhoz, akkor ezt kell engedélyeznünk.
- NAP ügynök: Az EC-k és az SHA közötti információcsere bonyolítója.

És persze ne felejtsük: ha nincs ügynök a gépen, vagy ha nem működik, vagy nincs elindítva egy NAP EC sem, akkor *nem* a karanténban vannak a gépek, hanem nincs semmilyen kontroll és mindent szabad[98]!



7.2 ÁBRA KOMPONENSHEGYEK

7.1.1 ÖSSZETEVŐK

[98] De ne ijedjünk meg: Csoportházirend! ☺

Ha szándékunkban áll a NAP bevezetése, akkor számoljunk azzal is, hogy több kiszolgáló-szerepkör is felkerül majd a kiszolgálónkra, illetve jó pár külső szerepkört össze is kell konfigurálnunk a NAP-pal. Nézzük az összes kapcsolódó elem listáját:

- Network Policy Server (NPS): Már volt róla szó korábban, gyakorlatilag a Microsoft legújabb RADIUS szerver implementációja[99]. Az NPS talán a legfontosabb eszközünk, mivel gyakorlatilag minden fogadó komponenssel tartja kapcsolatot, és a kezében van a döntés a beengedésről, vagy az elutasításról. Ezenkívül a Connection és a Network Policy gyűjtőkben lévő szabályok segítségével:
    - Központilag képesek leszünk felügyelni a vezeték nélküli hozzáférési pontokat, a VPN szervereket, a dial-up szervereket és például a 802.1x szabvánnyal dolgozó hálózati eszközöket is.
    - Az egészségi állapot előírások SHV (System Health Validator) ellenőrző csomagok formájában kerülhetnek fel az NPS szerverre.
    - A kliensek „egészségi” állapotát felmérő és az eredményt tároló csomagok (Statements of Health – SoH) is kézbesíthetőek az NPS-en keresztül.
    - A korlátlan és a korlátozott hozzáférések kritériumait is leírhatjuk (Health Policy), és persze a NAP EC-knek megfelelően több szabályzat is létezhet.
- Health Registration Authority (HRA): Egy olyan NAP komponensről van szó, amely csak az IPSec típusú kapcsolódáskor (lásd később) szükséges. A kliens egy – a megfelelt állapotát bizonyító – tanúsítványt kaphat ettől a kiszolgálótól az SoH kérés kiküldése után, és ezzel építi majd fel az IPSec kapcsolatot.
- Host Credential Authorization Protocol: A Cisco hasonló (NAC, Network Admission Control) rendszere felé kapcsolatot teremtő komponens.
- RRAS: Szintén felkerül a szerverre ez a régi jó ismerős is, amely a sokféle kapcsolódási lehetőségért, illetve hálózati technológiáért felel (VPN, DUP, LAN-to-LAN, LAN-to- WAN, NAT stb.) , de a NAP-hoz csak közvetve kapcsolódik.
- IIS7 + PKI infrastruktúra. Szintén kötelező elemek, már a telepítő varázslóban is konfigurálhatunk egy saját CA-t (persze ha már létezik, akkor használni is tudja a megfelelő szervertanúsítványt).
- És végül, de egyáltalán nem utolsósorban az Active Directory, ami az előírt egészségi információk lelőhelye lesz.

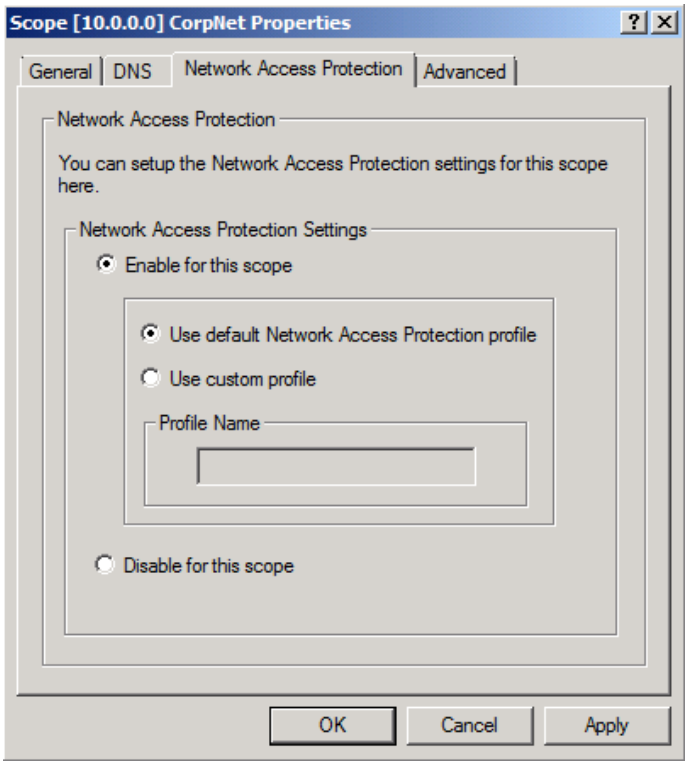
És most jöjjenek a részben már emlegetett kapcsolódási lehetőségek, amelyből öt áll rendelkezésre, azaz ezek azok a „közegek” amelyekből kapcsolódva egy kliens állapotát a NAP képes vizsgálni, majd dönteni a sorsáról.

7.1.2 A KAPCSOLÓDÁSI LEHETŐSÉGEK

[99] Az NPS-t persze használhatjuk RADIUS kliensként is, és ezen a területen is, pl. egy telephelyes, több NAP kiszolgálós infrastruktúrában.

1. DHCP kiszolgálón keresztüli kapcsolódás

Nem tökéletes módszer[100], hiszen arról van szó, hogy elutasítás esetén egy nem kifogástalanul megfelelő IP konfigurációt fog kapni a kliens - de ha a felhasználó fogja magát és beállítja (beállíthatja?) statikusra a TCP/IP jellemzőket, már ki is kerülte a NAP-ot. Mivel a kommunikációhoz egy értelmes IP címre azért szükség van, így csak egy speciális DHCP User Class konfiguráció részeként pl. egy rossz default gateway-t kaphat elutasítás esetén a kliens.



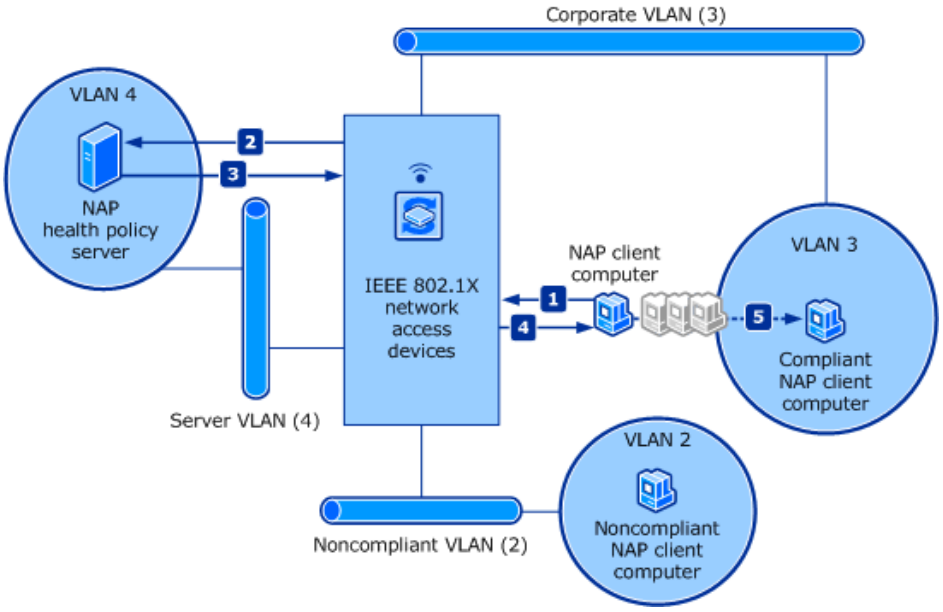
7.3 ÁBRA A NAP DHCP SZKOPÓNKÉNT ENGEDÉLYEZHETŐ

2. 802.1x Vezetékes (Wired) és vezeték nélküli (Wireless) kapcsolódások

Korrektebb megoldás, mint az előző, vezetékes és vezeték nélküli eszközök segítségével, viszont ezekkel a hardver eszközökkel szemben elvárás, hogy a hozzájuk forduló kliens egészségi állapotát képesek legyenek fogadni és továbbküldeni az NPS felé. Negatív válasz esetén viszont a hardver eszköz tipikusan egy a belső hálótól eltérő, attól függetlenített VLAN-ba irányítja majd a gépeket. De persze gondoskodunk kell arról, hogy a patikaszerverekkel is legyen kapcsolata ennek a VLAN-nak.[101]

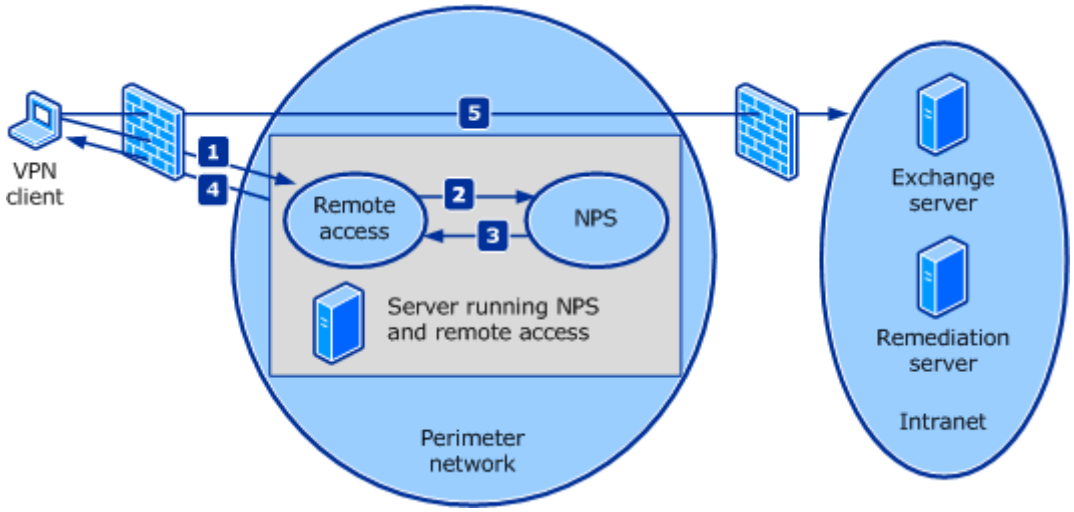
[100] Viszont a DHCP mindig kéznél van, és ha erre is használjuk, akkor már ez is hatalmas előrelépésnek számít.

[101] Nehezíti ezt a szituációt, hogy vagy a hálózatos kollégákkal kell egyeztetni (nem mindig sikeres az ilyen kezdeményezés), vagy magunknak kell érteni ezekhez az eszközökhöz (a lektor megjegyzése).



7.4 ÁBRA SZÁMTALAN VLAN

3. VPN alapú hálózati hozzáférés



7.5 ÁBRA KÉT TŰZ(FAL) KÖZÖTT

A NAP VPN támogatása szemben a korábbi VPN karantén megoldással széleskörű, és könnyen konfigurálható, és nehezebben kikerülhető. Könnyedén előírhatjuk az egészségi állapotot, amit a kapcsolódó kliensen lévő ügynök folyamatosan figyel. Tipikusan a kapcsolódó gép egy tartományi gép lesz, így az automatikus javítás sem lehet probléma, és a kapcsolódás ideje alatt folyamatosan ellenőrzés alatt marad a kliens.

Az új fejlesztésű VPN tunnel protokollok mind NAP kompatibilisek, de a következő részben ismertetésre kerülő DirectAccess elérés esetén is folyamatosan ellenőrzés alatt maradhat a kapcsolódó munkaállomás. És persze ne feledjük, ha pl. egy

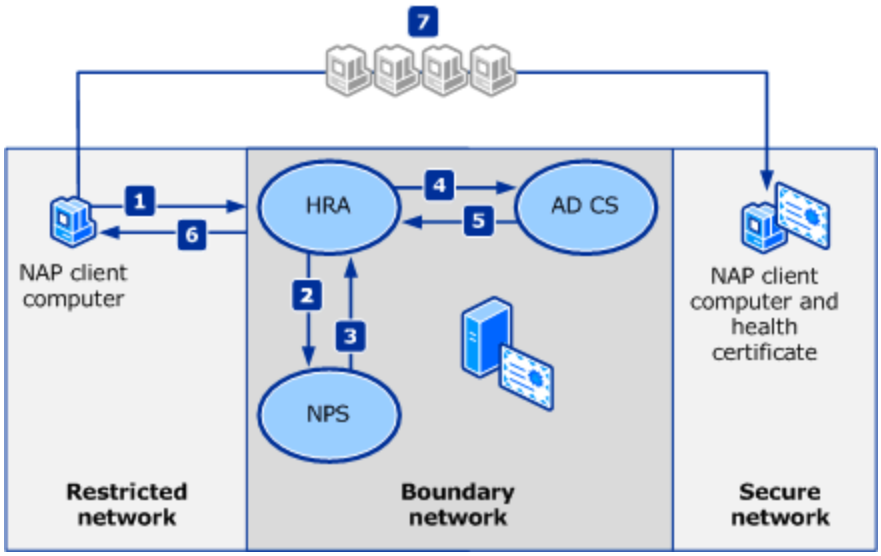
Forefront TMG 2010 „adja” a VPN szerver funkciót, akkor sem csorbul a NAP kompatibilitás!

4. RDP over HTTPS (Remote Desktop Gateway)
Egy későbbi fejezetben alaposan ki fogom fejteni az egyik kedvenc témaköröm, a TS/RDS részeként megjelenő Remote Desktop Gateway feladatait, de most csak annyit, hogy az RDP kapcsolatok HTTPS tunnelbe bújtatása, illetve a kapcsolatfüggő biztonsági szabályok alkalmazása mellett, a kívülről, a kliensektől érkező NAP kéréseket is képes továbbítani. Viszont a NAP ebben az egy kapcsolódási területben nem képes a karantén kezelésre. Tehát megvizsgálhatjuk a kapcsolódó gép egészségi állapotát, azonban ha az nem teljesíti az előírt feltételeket, akkor itt nem létesül karantén hálózat, ahonnan képes megjavítani magát a gép - viszont a tiltás kiválóan működik.

5. HRA: IPSec alapú védett hálózati forgalom
Talán a legbiztosabb védelmet ez a megoldás képes nyújtani a nem megfelelően konfigurált gépekkel szemben. A megfelelő rendszer felépítéséhez alkalmaznunk kell a domain izoláció fogalmát, melynek lényege, hogy a belső hálózatban futó szenzitív információkat tartalmazó kiszolgálónkhoz IPSec alapú szabályokat hozunk létre. Az IPSec alkalmazásával nem csupán a hálózati forgalom titkosítását és az adatintegritás védelmét nyerjük, de egyúttal azt is szabályozhatjuk, hogy csak azok a kliensek legyenek képesek kommunikálni a kiszolgálói rendszerrel, akik teljesítik az előírt egészségállapot feltételrendszert.

Az IPSec alapú kommunikációs csatorna kiépítésének első lépése a két fél kölcsönös hitelesítése. A hagyományos IPSec esetében a hitelesítéshez alkalmazható a megosztott titok (preshared key), a Kerberos alapú jegyrendszer és a megbízható, CA által kibocsátott tanúsítvány. A NAP esetében viszont kicsit tekertek a fejlesztők az alap logikán. Itt mindkét félnek egy speciális OID (Object Identifier) mezővel ellátott tanúsítvány sablonból kiállított tanúsítványra van szüksége, amit nem igényelhetnek közvetlenül. Ilyen tanúsítványt a Health Registration Authority (HRA) Windows Server 2008-as szerepkört ellátó kiszolgáló állít ki az előírt egészségi állapotot teljesítő gépek számára.

Ha egy gép nem teljesíti az előírt feltételeket, akkor nem kaphat ilyen tanúsítványt, ha pedig korábban teljesítette azt, de valamilyen oknál fogva menet közben attól eltért, akkor a korábban kibocsátott tanúsítványt a kliensen futó nap ügynök eldobja, ezzel megszakad a védett kiszolgálóval felépített IPSec csatorna.



7.6 ÁBRA EGY SIKERES KAPCSOLÓDÁS TANÚSÍTVÁNY ÉS AZ IPSEC SEGÍTSÉGÉVEL

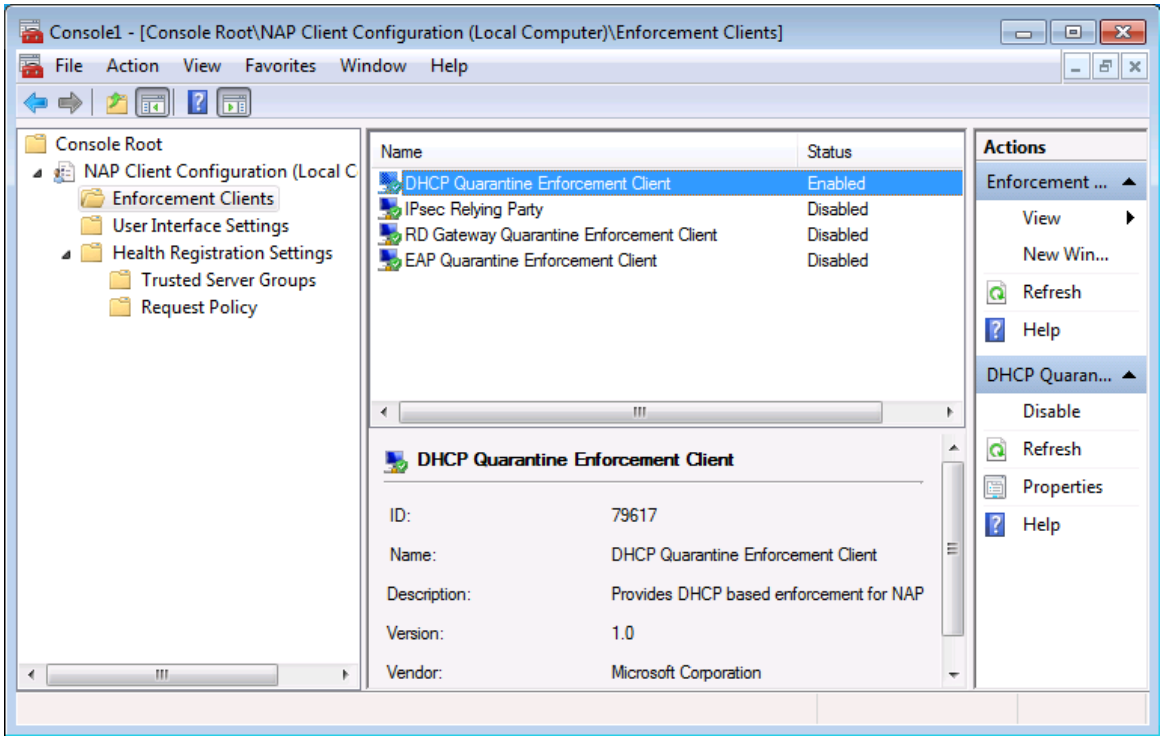
Végül címszavakban nézzük meg, hogy mi történik egy működő NAP rendszerben, amikor a kliens DHCP-vel szeretne kapcsolódni.

1. A kliensünk a szokásos módon IP-beállításokat kér a DHCP-kiszolgálótól. Ha a kliens rendelkezik az SoH-val, akkor ezt a DHCP-kérelem már tartalmazza. A DHCP-szerver az SoH-t továbbítja az NPS kiszolgálónknak, az pedig kideríti, hogy érvényes-e.

1.1. „A" eset: Ha igen, a DHCP-kiszolgáló ellátja a klienst a komplett IP-konfigurációval, a kliens pedig korlátlan hozzáférést kap a hálózathoz, és vége a folyamatnak.

1.2. „B eset": Ha nem, akkor a DHCP olyan IP-paramétereket ad át a kliensnek, amelyek csak a korlátozott hálózathoz biztosítanak hozzáférést (lásd korábban).

2. Ha a kliensnek nincs SoH-ja, akkor nem megfelelő, és ugyanaz történik, mint az előző pont „B" esetében, és jöhet a következő pont.
3. A kliens NAP ügynöke frissítési kérelmet küld a nyitott vagy elérhető hálózaton lévő patikaszervernek.
4. A patikaszerver ellátja a klienst a megfelelő javításokkal, és a kliens SoH-ja is aktualizálódik.
5. Ismételt kérelem indul a DHCP-szerver felé, amely viszont már tartalmazza az új SoH-t – azaz kezdődhet elölről a vizsgálat, az ideális 1.1 pont felé haladva.

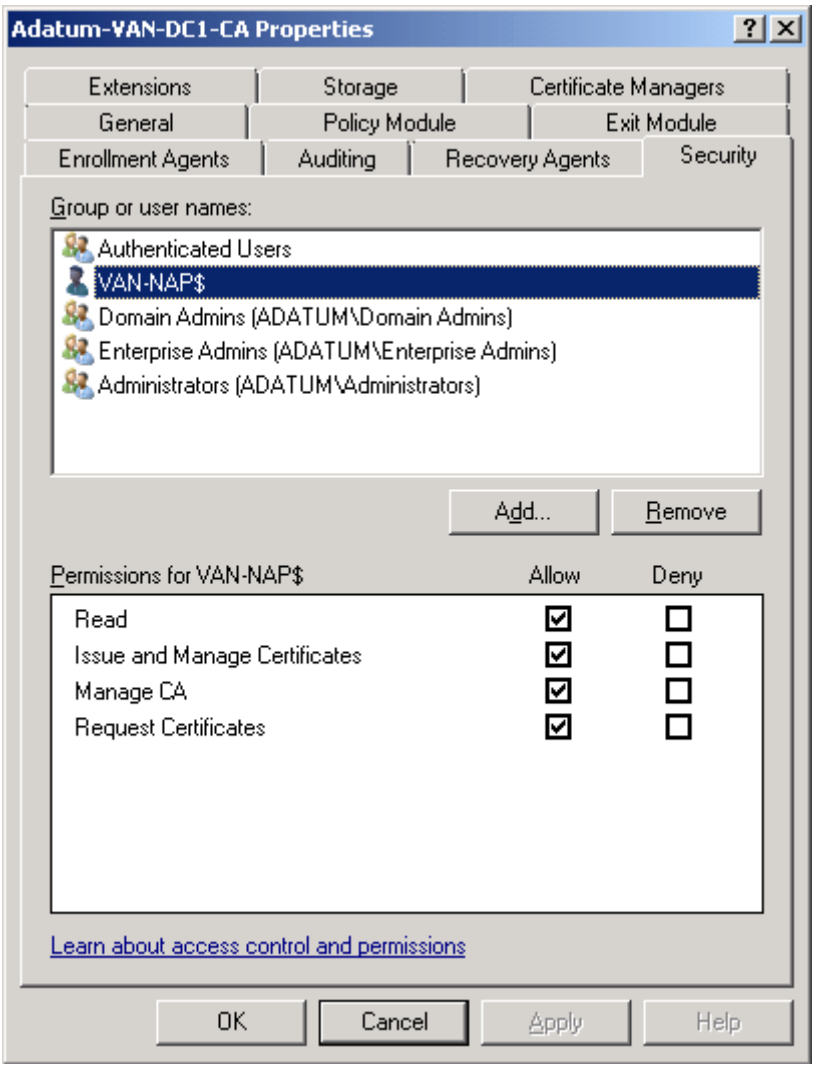


7.7 ÁBRA EGY NAP KLIENS ÉS AZ EC-K, BEKAPCSOLT DHCP EC-VEL

De nézzük meg - gyorsított üzemmódban - azt is, hogy hogyan konfigurálunk be egy IPSec EC-vel működő NAP-ot! A feladat kicsit elrugaszkodik a könyv alaptémájától, de legalább egy reális cél: egy VPN szerverként (is) működő Forefront TMG vagy UAG szerveren keresztül működjön a NAP, a tartományi - tipikusan hordozható - gépeink számára, amikor *nem* a belső hálózatban vannak.

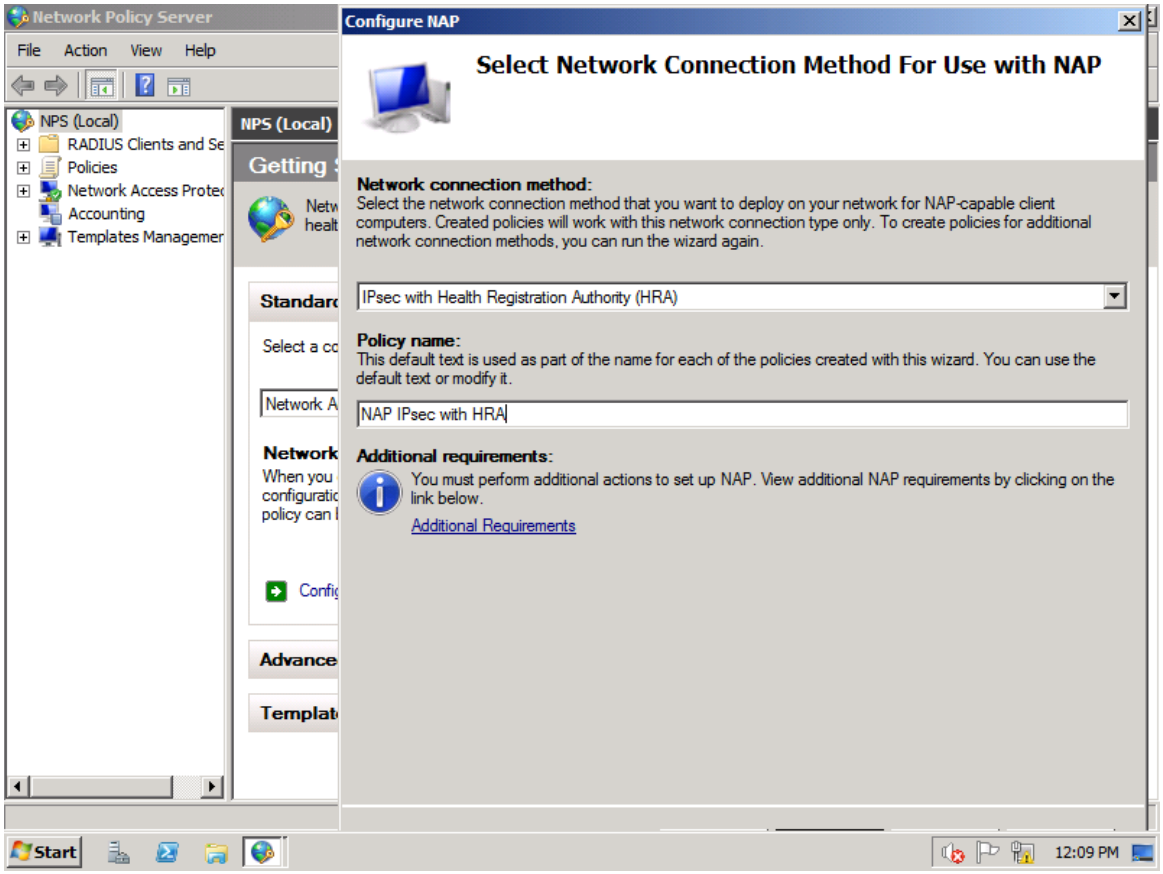
1. Állítsuk be a tanúsítványkiadónkat (Certificate Authority) úgy, hogy képes legyen egy megfelelő egészségi tanúsítványt kiadni a NAP kliens kérése esetén!
   a) Ehhez egy „Workstation Authentication” tanúsítvány kell majd, tehát másoljunk le egy ilyen sablont a CA „Certificates Templates” konzolban (Windows Server 2003 Server, Enterprise Edition típus).
   b) A neve lényegtelen, ellenben az Extension > Application Policies > Edit alatt vegyük fel a „System Health Authentication” policy-t, mivel ennek az OID-ja azonosítja majd a tanúsítványt egy NAP egészségi tanúsítványként.
   c) Engedélyezzük a sablont (Certificate Templates > New > Certificate Templates to Issue), majd a CA gyökerén adjunk meg minden jogot a leendő NAP szerverünk számítógép fiókjának (lásd következő kép). Erre azért van szükség, hogy a NAP kiszolgáló képes legyen kiadni egy tanúsítványt az egészséges kliens nevében.
   d) Egy bonyolult parancs jön: „Certutil –setreg policy\EditFlags +EDITF_ATTRIBUTEENDDATE” – ez azért kell hogy a HRA számára a leendő kérésben specifikálható legyen az érvényességi periódus.
   e) Ezek után a CA újraindítása kötelező.

f) A leendő NAP szerveren kérjünk egy „Computer” típusú tanúsítványt a kiszolgálónak (elvileg itt már látni fogjuk a NAP klienseknek szóló sablont is, de nem ez kell most).



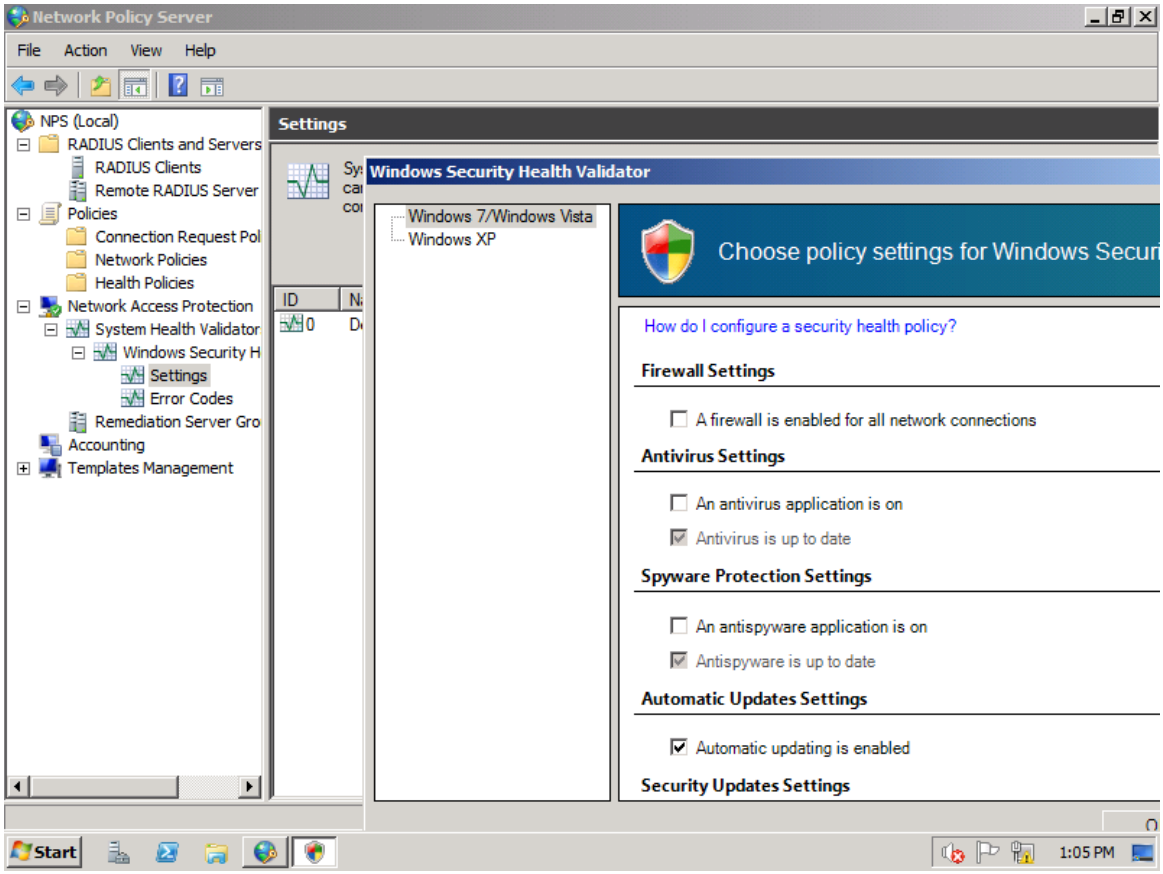
7.8 ÁBRA A NAP SZERVER JOGAI ERŐSEK LESZNEK ITT

2. A NAP szerepkör telepítése a következő lépés, azaz rakjuk fel az NPS es a „Health Registration Authority” komponenseket. A telepítés közben válasszuk ki a CA szerverünket, mint „Existing Remote CA”-t, majd az előbb elkészített tanúsítványt is.
3. Indítsuk el az NPS-t, majd a főképernyőről a „Configure NAP” pontot! Ha IPSec alapon szeretnénk a NAP-ot, akkor válasszuk a következő képen is szereplő „IPSec with HRA” metódust.
4. A RADIUS kliens(eke)t meghatározó lépésen simán átugorhatunk, mivel a mi esetünkben a helyi HRA lesz majd a RADIUS kliens. A következő, „Machine Groups” ablakban a felhasználói érvényességi kört adjuk meg. Ha nem adunk meg semmit, akkor minden felhasználóra érvényes lesz ez a házirend.



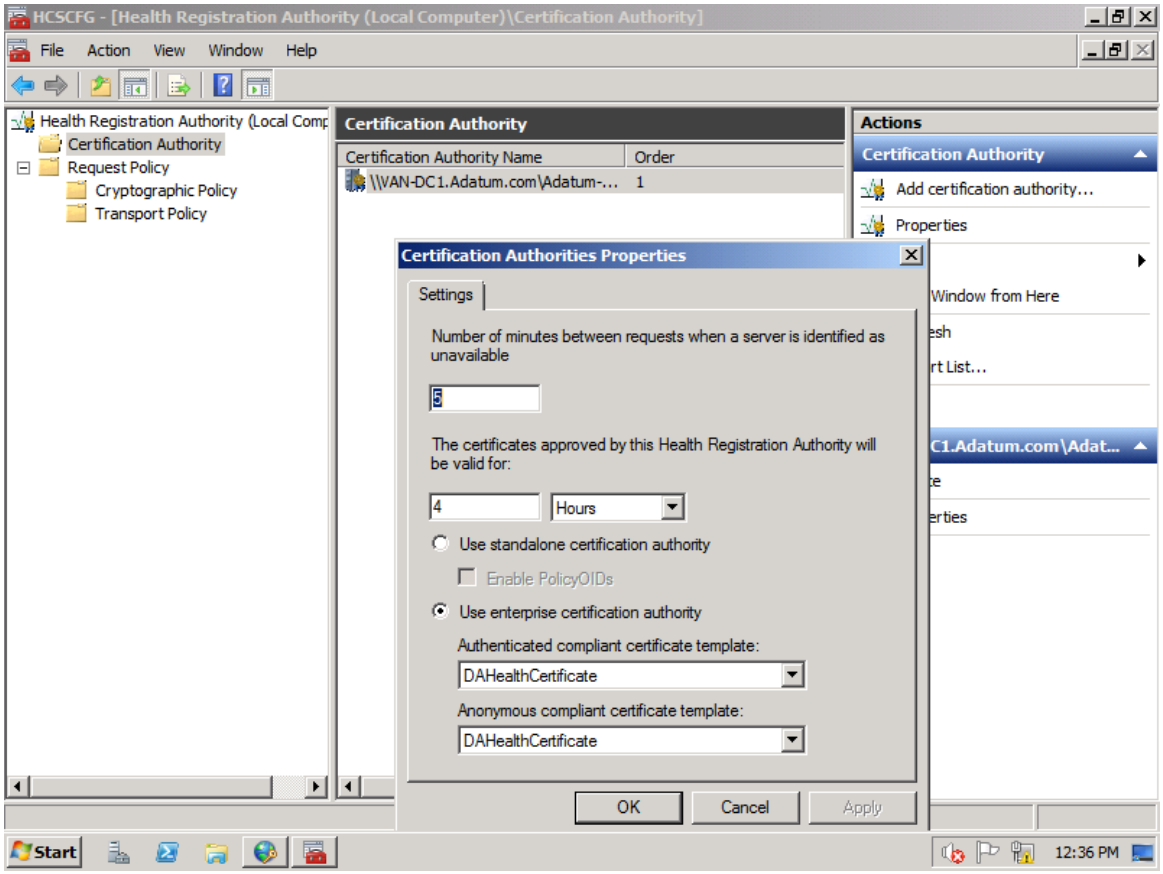
7.9 ÁBRA ÍGY INDUL A NAP VARÁZSLÓ

5. Ezután egy SHV megadása következik. Ha nem telepítettünk egy külsőt (pl. a Forefront vírusirtóhoz is van ilyen), akkor marad a gyári a Windows SHV (mindjárt ránézünk a beállításaira). Itt láthatunk még egy fontos opciót is, ami az „auto-remediation”-ra, azaz az automatikus gyógyításra vonatkozik. Ha ezt megengedjük, akkor pl. a kikapcsolt MIcrosoft Update kliens vagy a tűzfal bekapcsolja majd „magát” a kliensen.
6. Ezek után jön az összegzés és ez a rész készen is van, viszont az egész művelet még egyáltalán nem, ezért ugorjunk át a Network Access Protection pontra és keressük meg a Windows SHV beállításait (7.10 ábra). Nos, itt fogjuk a csatlakozási feltételeket beállítani! Az ábrán is látható, hogy én csak annyit követeltem meg most, hogy a Microsoft Update kliens legyen mindig bekapcsolva.



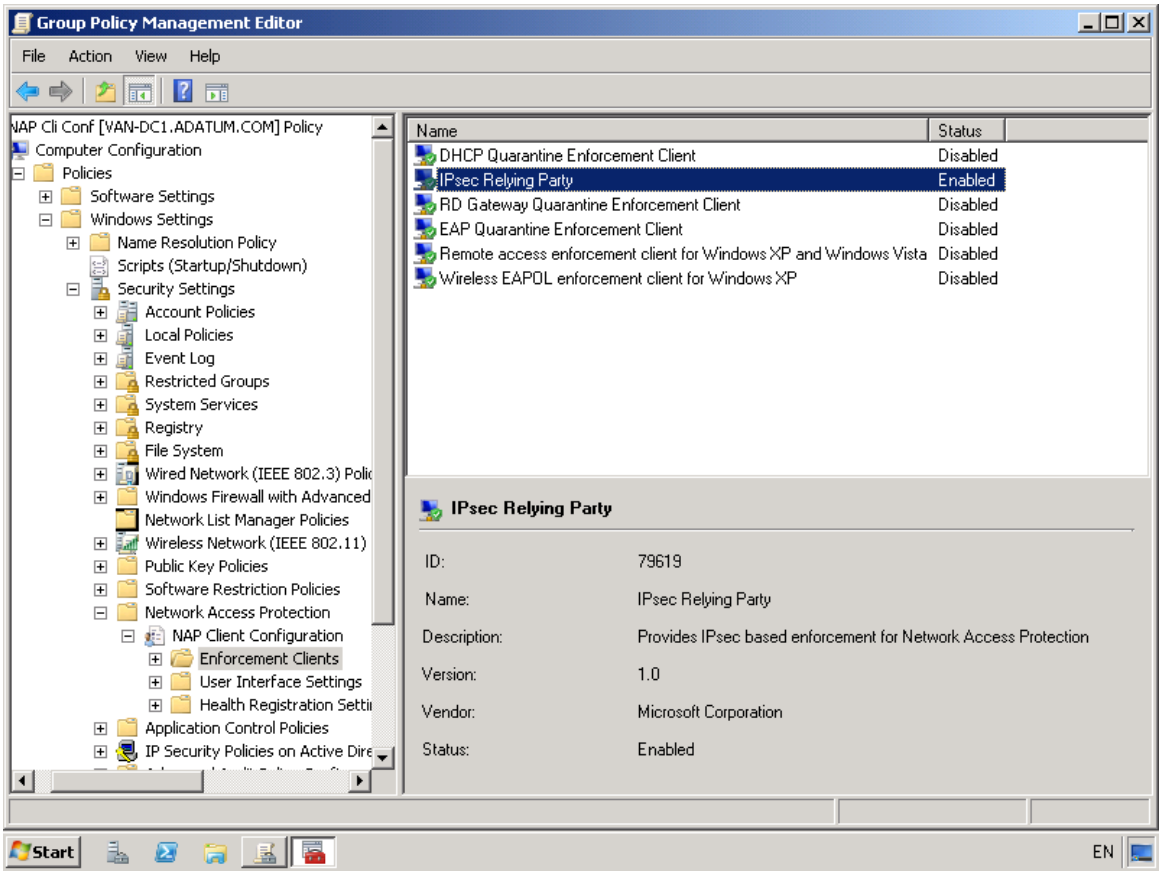
7.10 ÁBRA AZ ELVÁRT FELTÉTEL BEÁLLÍTÁSA

7. Ezzel végeztünk is az NPS-ben, ergo indítsuk el a HRA-t az Administrative Tools-ból. Itt viszonylag kevés dolgunk lesz, a bal oldali keretből válasszuk ki a Certification Authority-t, és jelöljük ki a CA szerverünket az „Add…” paranccsal. Ha ezzel megvagyunk, akkor válasszuk ki ugyanitt a CA tulajdonságait, és állítsuk be a következő kép alapján a „Use enterprise certification authority” alatt kétszer a korábban elkészített egészségi tanúsítványunk sablonját. És ezzel végeztünk is a HRA-val.

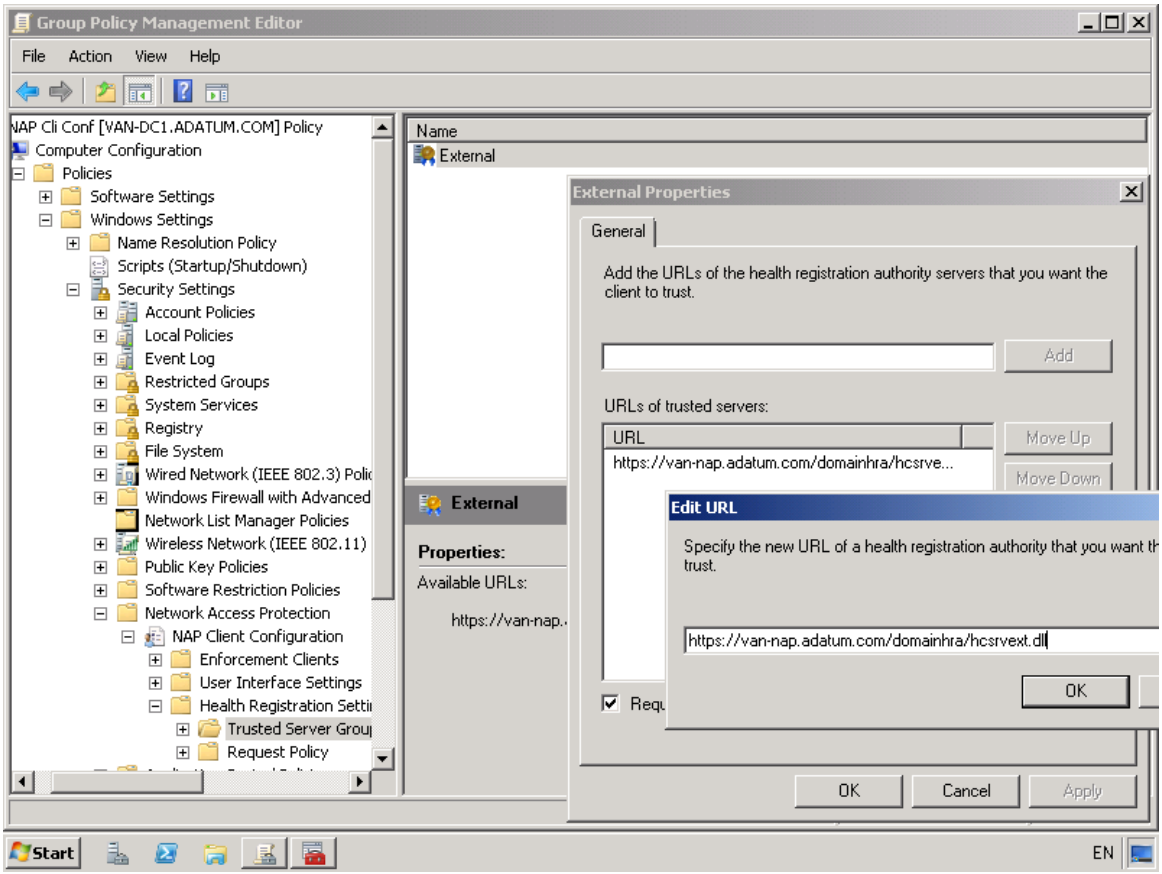


7.11 ÁBRA A HRA BEÁLLÍTÁSA

8. Jöjjön viszont a Csoportházirend, definiáljunk egy külön GPO-t, majd állítsuk be a következő opciókat:
   a) Határozzuk meg az EC típusát (IPSec Relying Party, lásd a következő képet)!
   b) Jelöljünk meg egy URL-t, amelyen a NAP szerverünk elérhető kívülről is (a példában erre szükségünk lesz), mint egy megbízható HRA (7.13 ábra)!
   c) Állítsuk be, hogy a NAP szolgáltatás minden érintett kliensen automatikusan induljon (Security Settings > System Services)!
   d) Állítsuk be azt is, hogy a Security Center (Administrative Templates > Windows Components > Security Center) mindig legyen bekapcsolva (ez egy tartományban alapértelmezés szerint ki van kapcsolva)!

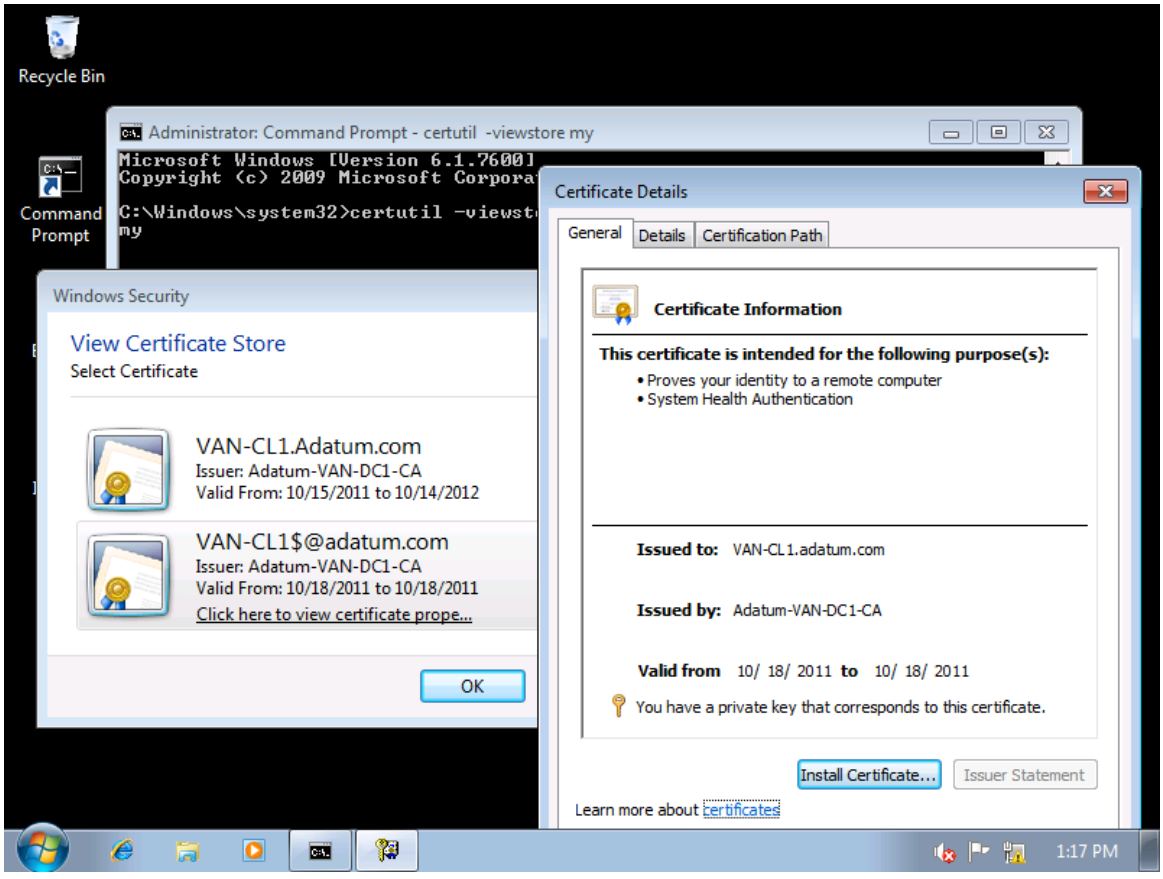


7.12 ÁBRA AZ IPSEC EC BEKAPCSOLÁSA A CSOPORTHÁZIRENDBEN



7.13 ÁBRA AZ EXTERNAL KAPCSOLAT KONFIGURÁLÁSA

9. Most már csak egy dolog van hátra, engedélyezzük pl. a VPN szervert is betöltő Forefront TMG-n vagy UAG-on a NAP használatát, illetve a laptopokon futtassunk egy gpupdate /force parancsot még a belső hálózaton, hogy a Csoportházirend beállításokhoz hozzájussanak.
10. Sétáljunk el a kliensre, ami közben már kikerült a hálózatból és most kívülről próbál egy VPN-nel (vagy éppen DirectAccess-szel, lásd következő fejezet) kapcsolódni. Ha ez sikerül neki, akkor két dologból is látszik hogy a NAP működik:
    a) Kapcsoljuk ki a próba miatt Microsoft Update klienst kézzel! A NAP először üzen egy buborékban a Tálcán, hogy probléma van, de a remediation azonnal visszakapcsolja.
    b) Gépeljük be a „certutil – viewstore my” parancsot! Ekkor megtekinthetjük az éppen létező egészségi tanúsítványunkat.



7.14 ÁBRA AZ EGÉSZSÉGI TANÚSÍTVÁNY

Összegezzük még egyszer!
Amikor a kliens a külső hálózatból csatlakozik, a NAP ellenőrzés is megtörténik és ha be van kapcsolva (a példám szerint) a Microsoft Update, akkor megkapja a kliens a spéci tanúsítványt és működik az IPSec csatorna kiépítése. Ha nem, akkor pedig a remediation állapotától függően vagy automatikusan bekapcsolódik a Microsoft Update, vagy nem lesz addig kapcsolat, amíg kézzel nem korrigálunk. Ha nincs

kapcsolat, akkor azért nincs mert az említett tanúsítványt ilyenkor nem kapja meg a kliens. Korrekt.

Végül ennyi kattintgatás után, mielőtt démonizálnánk a NAP-ot, tisztázzuk azért azt, hogy mire nem lesz jó?

- NEM véd a felhasználói támadások ellen
- NEM VPN karantén
- NEM ISA/TMG kiszolgáló
- NEM kell feltétlenül hozzá speciális hardver
- És persze NEM kell hozzá külön licenc sem

7.2 Több mint VPN – DirectAccess

A 2007-es RSA konferencián beszélt *Bill Gates* először arról a vízióról, hogy VPN vagy bármilyen más távelérési módszer nélkül is el kellene tudnunk érni biztonságosan a belső hálózatunk erőforrásait, instant módon, azaz bármilyen manuális teendő nélkül, gyakorlatilag teljesen automatikusan. Ez remekül hangzott az elképzelés szintjén, hiszen akár rendszergazda vagyok, akár felhasználó, ezzel az eléréssel csak a probléma van. A VPN bonyolult (is tud lenni, főképp, ha szimpla felhasználók vagyunk), ha komolyan vesszük, kell a Smartcard\PKI, sokszor egy automatikus default gateway átirányítással is jár (a split tunnel-t nem szeretik általában a céges környezetben), vannak olyan hálózatok (pl. hotelek vagy egyéb szigorú céges hálózatok), ahonnan nem használható, vagy csak PPTP, és sorolhatnám még a problémákat. Summa summarum: nem igazi az élmény.

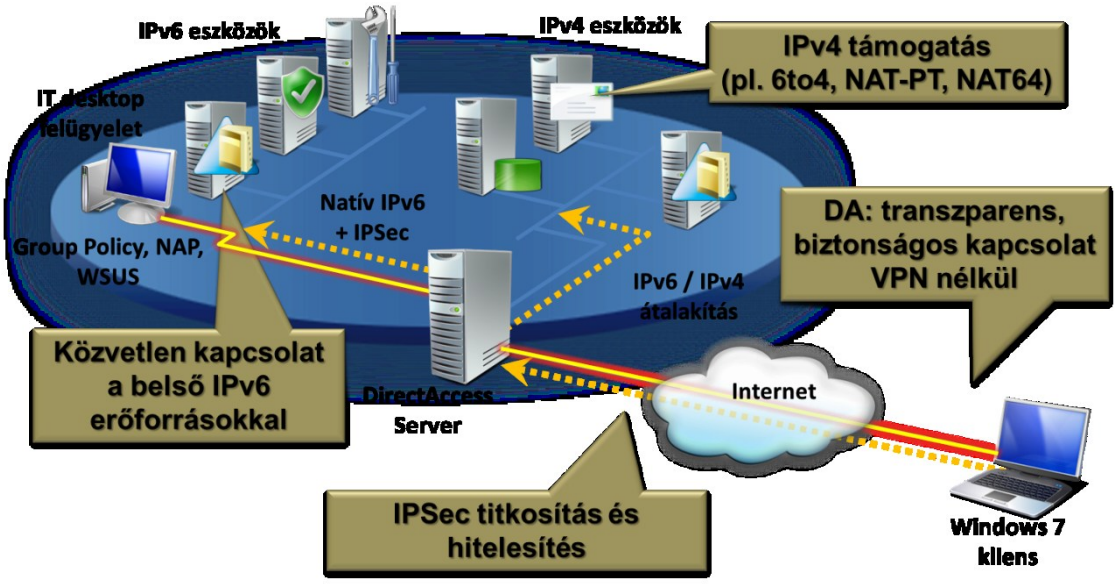
7.2.1 Mi is ez?

A DirectAccess azaz a Windows Server 2008 R2-vel és a Windows 7-tel megvalósított közvetlen elérés viszont az. Mivel jómagam például rendkívül sokat vagyok távol az irodától, a távoli elérés az első pillanattól kezdve fontos volt. Anno minden gépemhez beszereztem a smartcard olvasót (a Dell Tablet PC-hez nem volt egyszerű), mindenhol használtam a CMAK-kal csomagolt IT Connection Manager-t az összes kritériummal együtt (a részletek nem publikusak). Működik, de mindez csak kínlódás a DA-hoz képest.

Ugyanis most már semmit nem kell tárcsázni, semmit nem kell elindítani (kritériumok persze ugyanúgy lehetnek, például megkövetelhető a smartcard használat), csak indítom a böngészőt, és beírom az intranetes szerver nevét vagy pl. a fájlszervert a Start/Run-ba. Nincs hosszú ellenőrzés, terjedelmes karantén vizsgálat, csak egy internet kapcsolat kell.

Ráadásul, mivel már a belépés előtt éled, a céges környezetben kötelező frissítések és házirendek letöltése sem csak a VPN kapcsolat után indulhat, hanem ettől függetlenül, azaz bármikor, ha van a gépnek net elérése. Persze nem arról van szó,

hogy az összes "internetes" forgalom "befelé" megy (de ezt is lehet, ha szükséges), a normál forgalom továbbra is az ISP-nken keresztül zajlik, csak az a különbség, hogy mivel rögvest kapcsolatban lehetünk pl. a cégünk Perimeter hálózatában lévő DA szerveren keresztül a belső WSUS/SCE-vel/SCCM-mel, stb., nem kell ehhez megvárni a klasszikus VPN csatlakozást. Ez jó az üzemeltetőknek, és végül is jó nekem is mint felhasználónak.



7.16 ÁBRA EGY (MAJDNEM) TELJES DA INFRASTRUKTÚRA

Mindeme "csoda" alapja több hálózati technológia együttes alkalmazása, úgymint IPSec (hitelesítés és titkosítás) illetve az IPv6 a kétirányú kapcsolat felépítéséhez, ideális esetben tökéletes point-to-point security kialakítása a NAT, a NAT-T és az egyéb NAT problémák nélkül.

Viszont ha még nincs teljes IPv6 infrastruktúránk[102], akkor az ISATAP-ra, a Teredo-ra, a 6to4-re is szükségünk lehet az IPv4/v6 átalakításhoz szerver illetve kliens oldalon[103]. Kis segítség ezek értelmezéséhez:

- Teredo: NAT Traversal
- IPv4 tunneling: mindegyik átalakítás IPv6 belecsatornázása IPv4-be.
    - ISATAP: az IPv4 címek egy linken belül vannak (pl. belső hálózat)
    - 6to4: publikus IPv4 címekhez, bárhol, nincs NAT
    - Teredo: az IPv4 címek privát címek, bárhol, NAT-T
- Split DNS és a DA használat "követése": Name Resolution Policy Table

[102] Alapértelmezés szerint a Vista, WS08, Windows 7, WS08 R2 OS-ekben natív módon implementálva van, a hálózati hardver eszközök persze még külön kérdést képeznek.

[103] Vagy egy NAT-PT (RFC 2766) képes Layer2/3 hálózati eszköz, azaz switch vagy router (mivel az R2 ezt nem nyújtja) vagy egy Forefront UAG 2010, ami szintén képes a teljes átalakítást elvégezni.

> Az NRPT-hez még egy mondat, mivel ez érdekes újdonság, amely a Windows 7-ben debütál. Az NRPT elsődleges célja az, hogy szeparálni tudjuk a kliens oldalon a Internet/Intranet forgalmat, tehát abban az esetben, ha a kliens az interneten lóg, az első DNS infó keresés helye a NRPT lesz - és ha egy DA-n keresztüli, belső hálózati név/cím eléréséről van szó, akkor ott kell lennie ebben a táblában a mi megfelelő DNS szerverünknek (Csoportházirend > Name Resolution Policy), és már indulhat is a titkosított DNS lekérdezés vagy mehet titkosítás nélkül is - pl. az élő DA kapcsolaton keresztül.

Plusz itt van még nekünk egy új, a Microsoft által fejlesztett protokoll, az IPHTTPS. Csak a Windows 7 illetve az R2 esetén, a proxy vagy tűzfal mögött elhelyezett hostok képesek az IPv6 csomagokat IPv4 alapú HTTPS session-okbe "gyömöszölni". Ezzel persze akadhatnak teljesítmény gondok, éppen ezért ez csak a tartalék forgatókönyv, arra az esetre, ha a kliens szimpla IPv6 alapon (illetve a fentebb említett átalakítási megoldásokkal) nem tud kapcsolódni.

No és persze a különböző hitelesítési protokollok is szükségesek, ezek közül jelen pillanatban elsősorban a smartcard, azaz egy multifaktoros hitelesítés a lehetőség. A gépnek értelemszerűen tartományi tagnak kell lennie, illetve jó tudni azt is, hogy az üzemeltetők megszabhatják a belső erőforrások elérését, azaz adhatnak elvileg korlátlan hozzáférést, vagy csak bizonyos szerverek/gépek elérését, nagyjából ahogyan pl. egy Remote Desktop Gateway-nél.

> E rövid áttekintés után még egy dologba gondoljunk bele: azok a klienseink, akik használják a DA-t, azon kívül, hogy a belső hálózatba csont nélkül beleláthatnak, egymással is kommunikálhatnak majd, amelyet elsősorban a különböző P2P alkalmazásokkal fognak tudni igazán összehozni, de a lista szélesíthető. Ezek között vannak/lesznek olyanok, amelyeknél nincs szükség plusz lépésekre a biztonságos kommunikációhoz, a többi esetben (pl. Remote Assistance, Remote Desktop, File/Printer Sharing, stb.) viszont - nekünk üzemeltetőknek - gyakorlatilag IPSec transzport szabályokkal kell majd engedélyeznünk alkalmazásonként külön-külön vagy éppen mindent megengedve, vagy adott esetben tiltani a kapcsolódás lehetőségét.

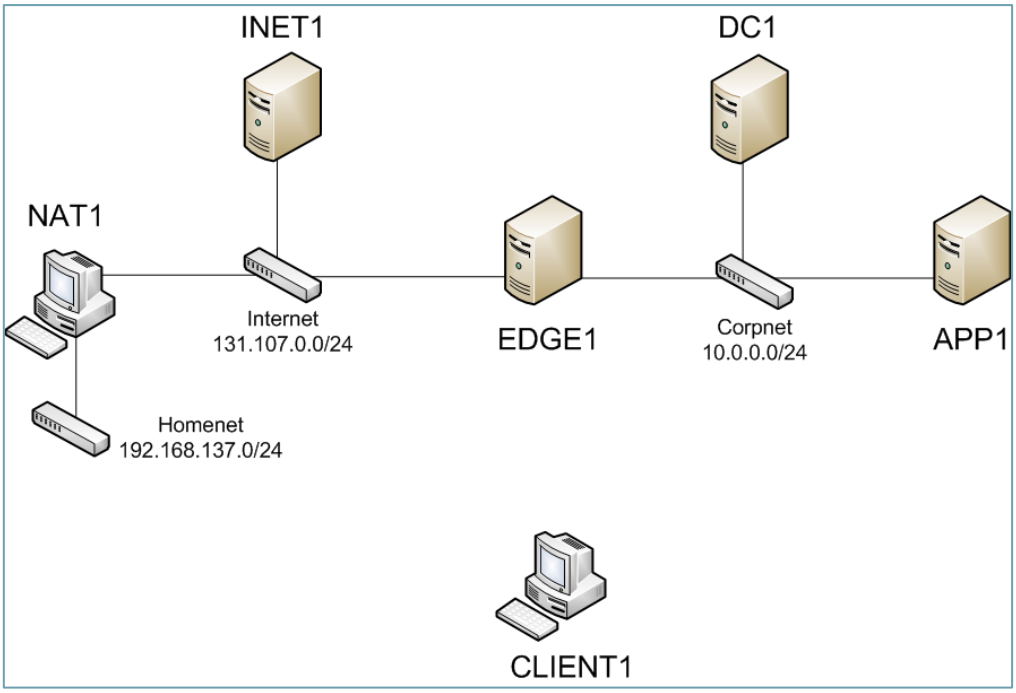
Mindjárt konfigurálunk, de előtte tekintsük át egy elképzelt[104] DirectAccess környezet összes szoftveres elemét és a velük szemben támasztott elvárásokat:

- EDGE gép

[104] Azért nem csak elképzelt, nálam virtuális környezetben működik is ☺, viszont a teljes leírás és a step-by-step dokumentum letölthető a netről: http://www.microsoft.com/download/en/details.aspx?id=24144

  - Egy dedikált, tartományba léptetett R2-es DirectAccess kiszolgáló (nem DC) két hálózati kártyával (intranet/internet), sőt a külsőn két statikus, publikus és *szomszédos* IPv4 címmel
  - A DirectAccess egy képesség, a Server Managerben a Features alatt találjuk
  - IIS, a CRL elérés miatt (az IP-HTTPS-hez)
  - Két darab különböző tanúsítvány, egy az IP-HTTPS-hez a DA gép nevével (privát kulcsokat is tartalmaznia kell), és egy másik, azaz a Root CA tanúsítványa
- DC1 gép
  - AD (sőt ha smartcard-ot akarunk használni, akkor csak R2-es AD jöhet szóba), és egy AD biztonsági csoport a DA-t használni óhajtó kliens gépfiókok számára
  - Csoportházirend, de nem kell majd vele bíbelődni, csak maximum az ellenőrzés során
  - DNS, DHCP szerepkörök
  - PKI infrastruktúra[105] (AD CS), EKU-s[106] kiszolgáló tanúsítvány sablon, autoenrollment, illetve egy korrekt CRL publikálás, amely az EDGE szerverre irányul, és elérhető a DA kliensekről is
  - Tűzfal szabályok, az ICMPv6 forgalom apropóján
  - Az ISATAP eltávolítása a DNS global block query list-ből
- APP1 gép
  - IIS7, ami lehet a DA szerveren is, vagy más kintről elérhető kiszolgálón, a lényeg, hogy a DA kliensek számára biztosítani kell az ún. "Network Location Server" szerepet, amely segítségével kiderül, hogy a DA kliens az intraneten vagy az interneten van éppen
  - Ennek a oldalnak is SSL-lel kel működnie, tehát ide is kell egy szerver tanúsítvány.
- CLIENT1 gép
  - Csak Windows 7 Enterprise vagy Ultimate kiadás
  - Csak a tartományi fiókkal rendelkező Windows 7 kliensek használhatják a DA-t, tehát be kell léptetni
  - Értelemszerűen minden belső erőforrás elérését le kell tesztelni még akkor, amíg belső hálózatban van, illetve a végső DA kiszolgáló konfig után a Csoportházirend változásokat magára kell, hogy húzza

[105] Igazából elég a saját tanúsítványkiadó, mivel állandó lesz a belső hálózati elérés, íme egy újabb előny ☺.
[106] Enhanced Key Usage, azaz a kiterjesztett kulcshasználati információk.



7.17 ÁBRA A KÖRNYEZET

Az ábrán szerepel még két további gép is, de ezek elsősorban a virtuális tesztkörnyezet miatt vannak beépítve, a valóságban nem szükségesek.

- INET1 gép
  - Egy internetes szolgáltatót szimbolizál, publikus IP-vel rendelkezik, DHCP és DNS kiszolgáló is van rajta, abban a szituációban segít, amikor a laptopunkkal egy nyilvános helyen netezünk
- NAT1 gép
  - Ez egy Windows 7, ami gyakorlatilag a NAT kiszolgáló, és az otthoni egyszerű ADSL routert helyettesíti, amely mögött ülünk a laptopunkkal, ha hazaértünk a munkából

A teljes elképzelés szerint három darab hálózatunk van:

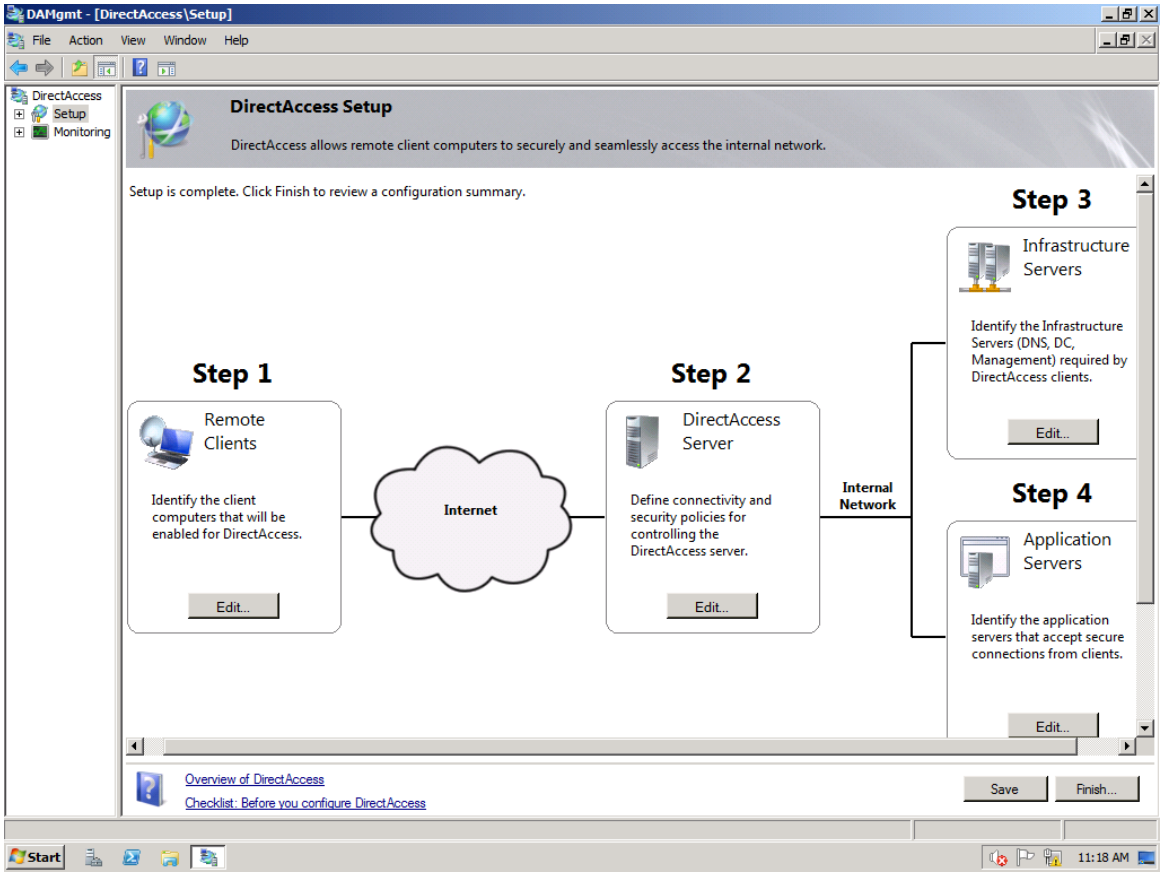
- Az Internet (131.107.0.0/24)
- Az otthoni hálózat (Homenet; 192.168.137.0/24) NAT-tal kapcsolódva a nethez
- Belső hálózat (Corpnet; (10.0.0.0/24) a DA által elválasztva[107]

7.2.2 VARÁZSOLJUNK!

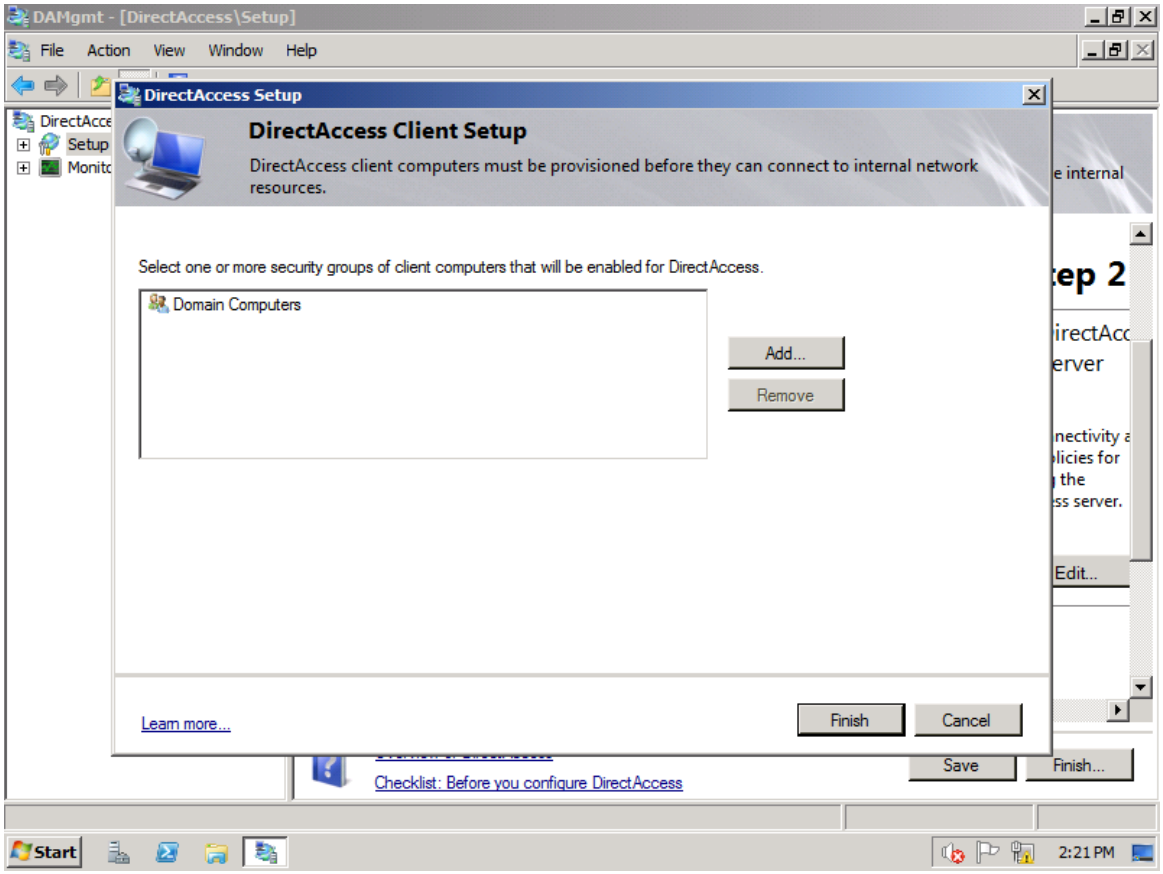
A cél az, hogy a kliens bármelyik hálózatban is van, állandó és automatikus kapcsolatot tartson a belső hálózat teljes vagy részleges elérésével. Ha minden előfeltételt megteremtettünk, akkor varázsoljunk egy jó nagyot a DirectAccess

[107] Most a DA szerver végső elhelyezésével, azaz pl. a tűzfalakkal kapcsolatos felállással nem foglalkozunk, a TMG könyvben leírtam az összes lehetőséget, sőt mi több, a megoldásokat is (a linket lásd az 5.3.2 fejezetben).

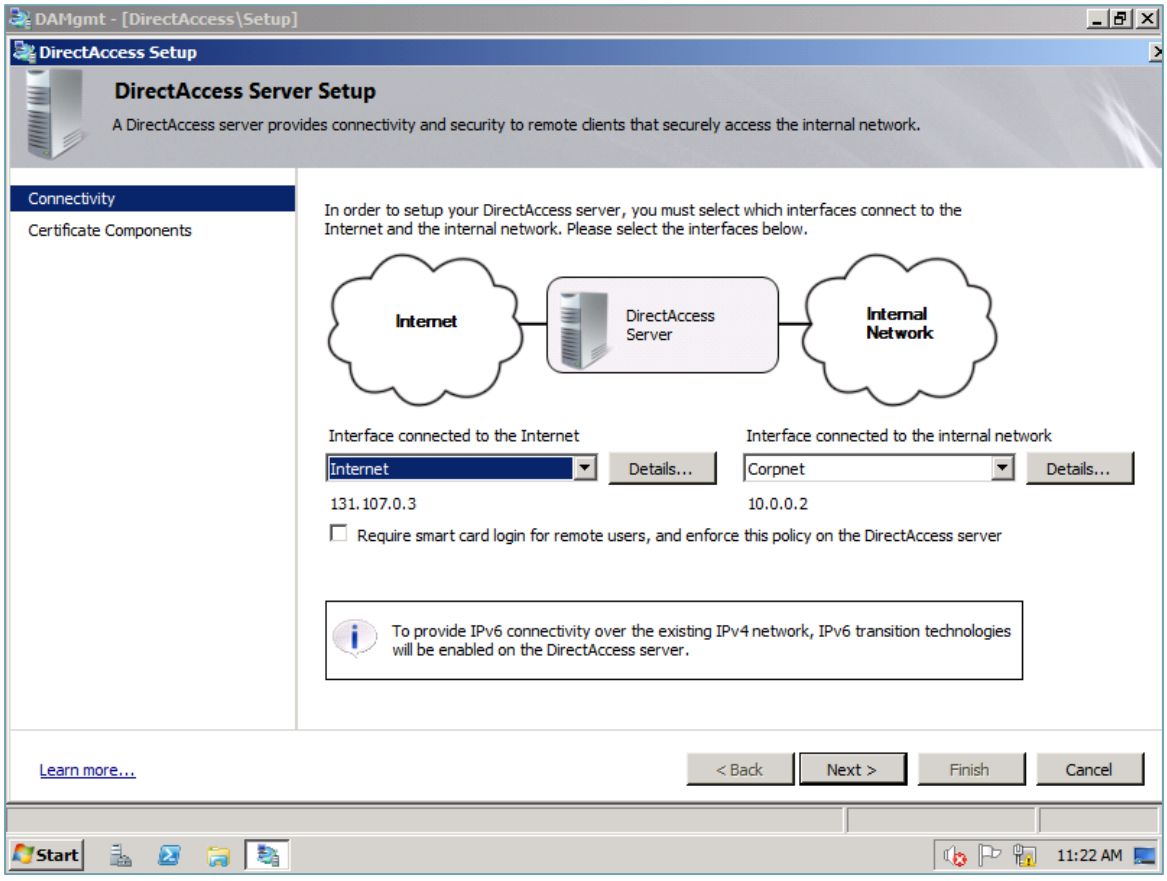
szerveren, azaz indítsuk el az Administrative Tools-ból a DirectAccess Management MMC-t!



7.18 ÁBRA 4 LÉPÉS KELL (A FELBONTÁS KICSI, NEM AZ ÁBRA NAGY)

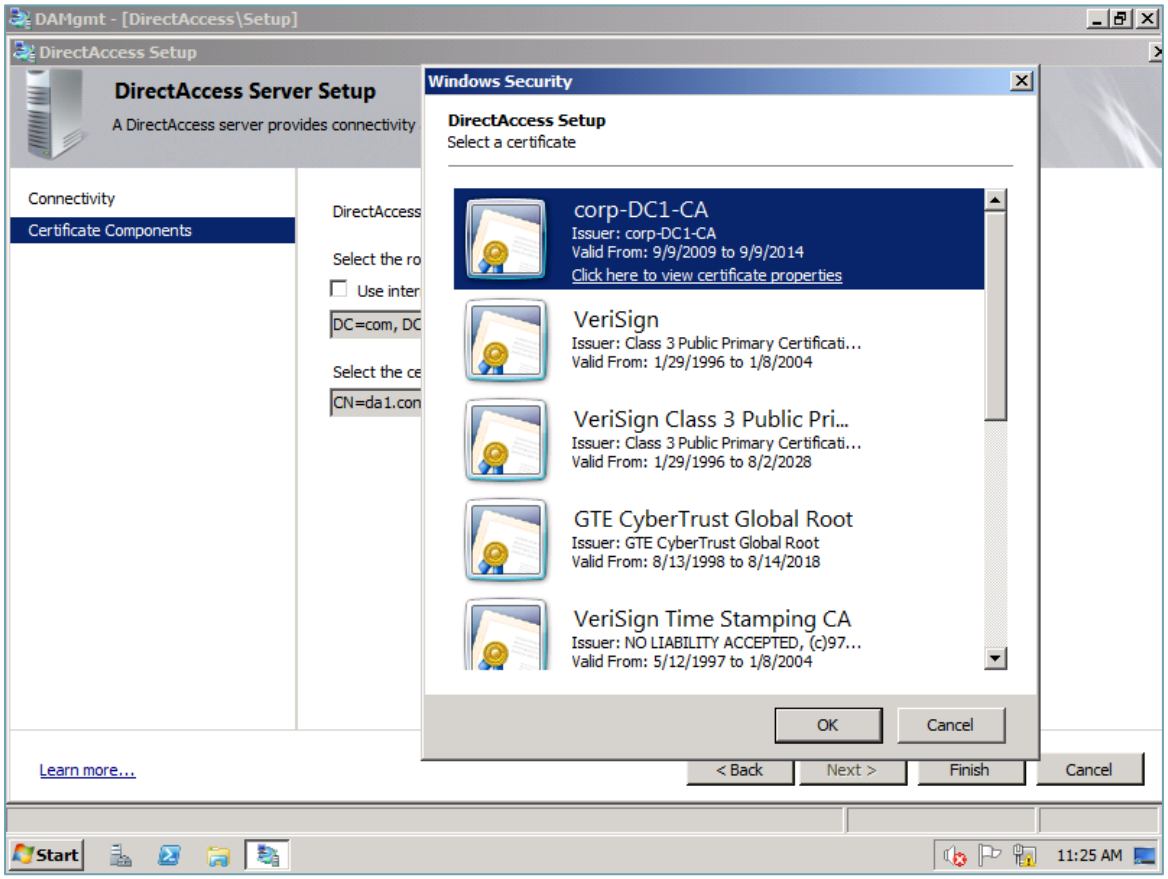


7.19 ÁBRA AZ ELSŐ LÉPÉS EGYSZERŰ, ADJUK MEG A DA KLIENSEK CSOPORTJÁT



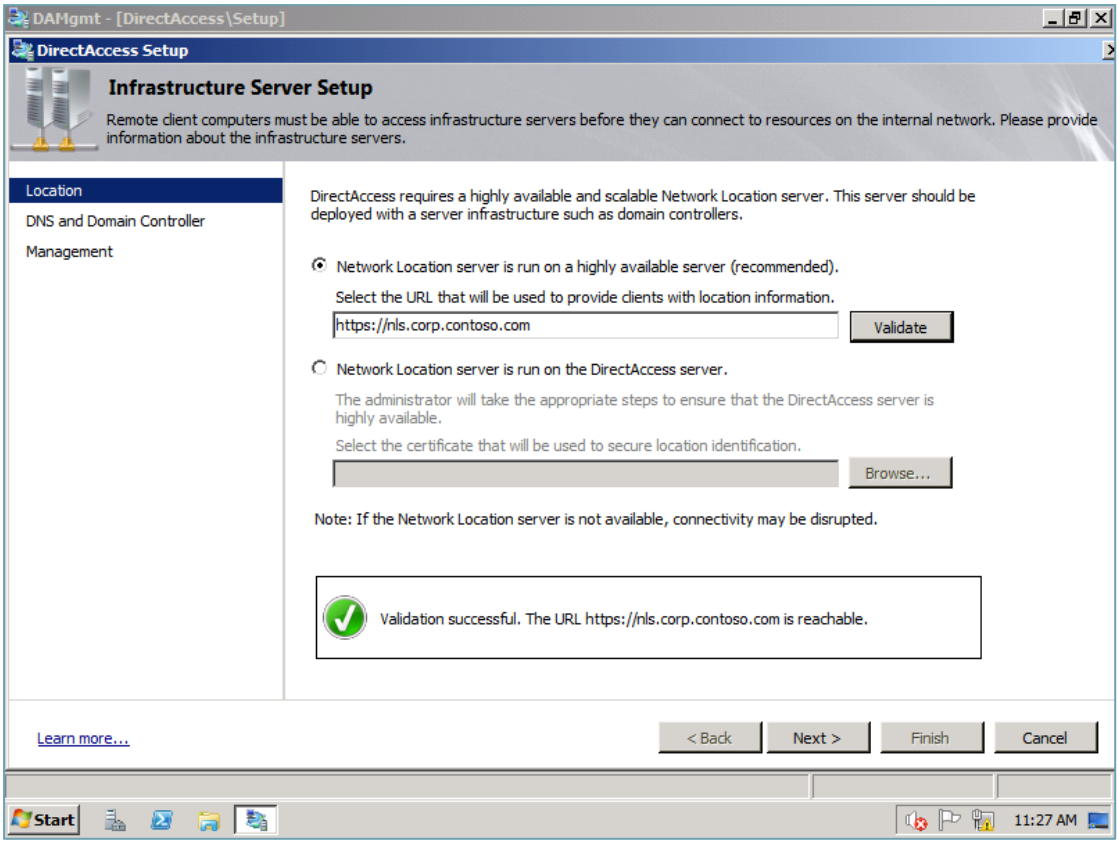
7.20 ÁBRA ITT MÁR VAN EZ-AZ, RÉSZLETEK KÖVETKEZNEK

Két fő rész van ebben az ablakban, egyrészt a külső és a belső interfészt kell megadni (ha valamit nem jól állítottunk be a TCP/IP-ben, azonnal sikít), illetve itt írhatjuk elő kötelező smartcard használatot. Ha a „Certificate Components”-re vagy Next-re megyünk, akkor pedig a két tanúsítvány betallózása a következő lépés.

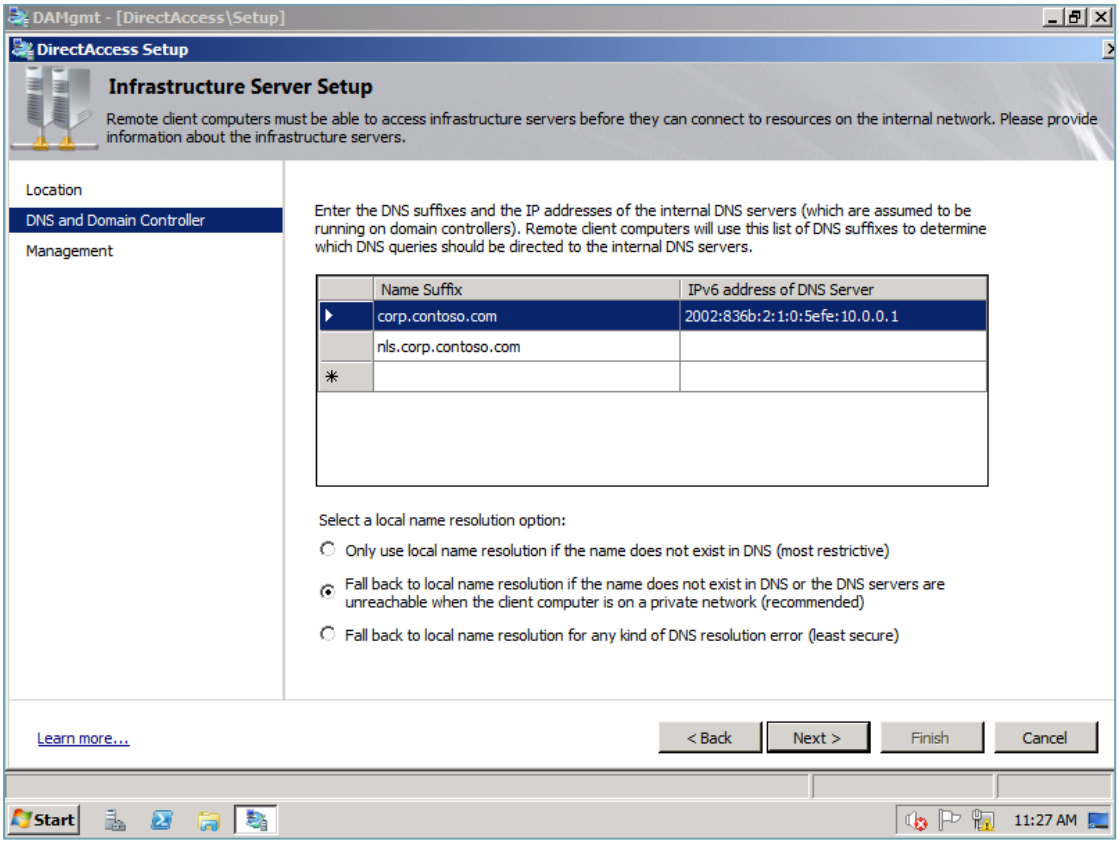


7.21 ÁBRA VÁLASSZ ROOT CA TANÚSÍTVÁNYT

Ha megvan, jöhet a Step 3, azaz az Infrastructure Server Setup.

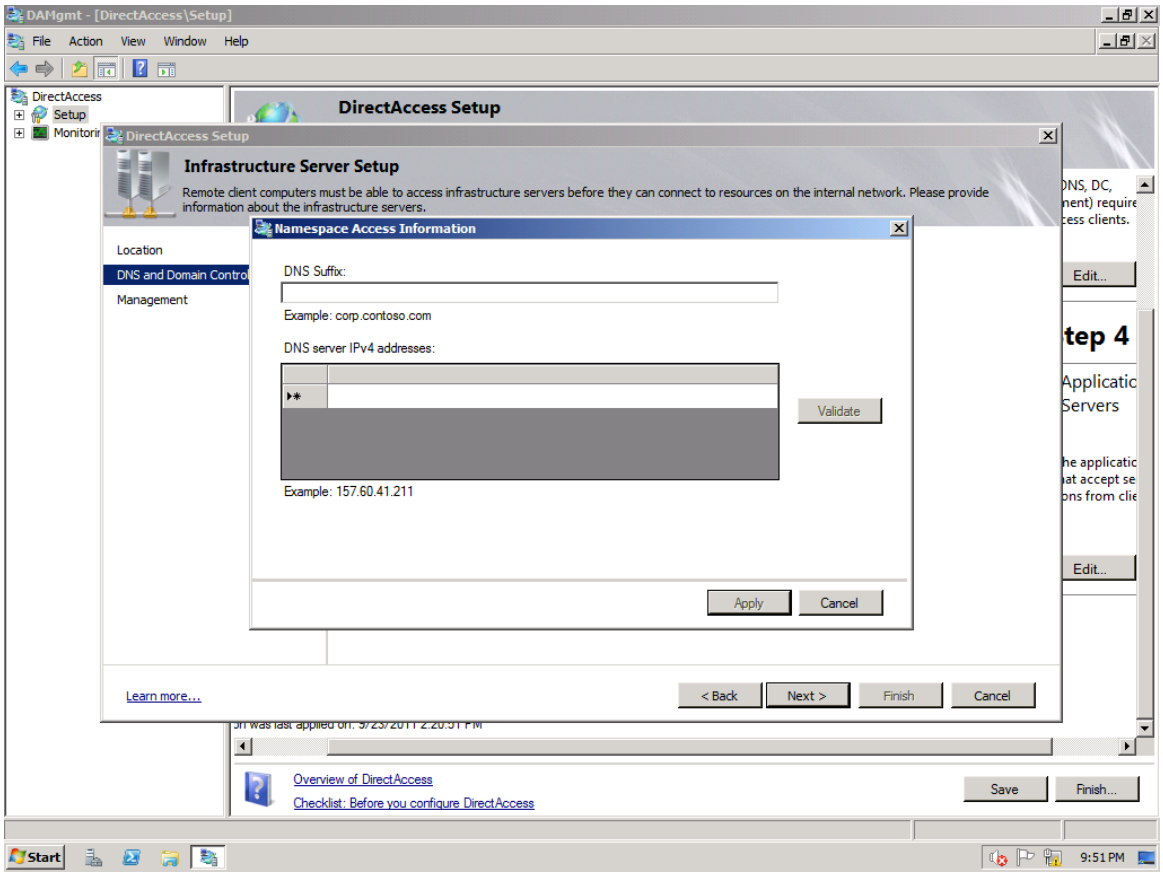


7.14 ÁBRA AZ NLS SZERVER BEÁLLÍTÁSA ÉS ELLENŐRZÉSE



7.22 ÁBRA A GÉPEKET BEÍRJA AUTOMATIKUSAN, AZ OPCIÓK KÖZÜL NEKÜNK KELL VÁLASZTANI

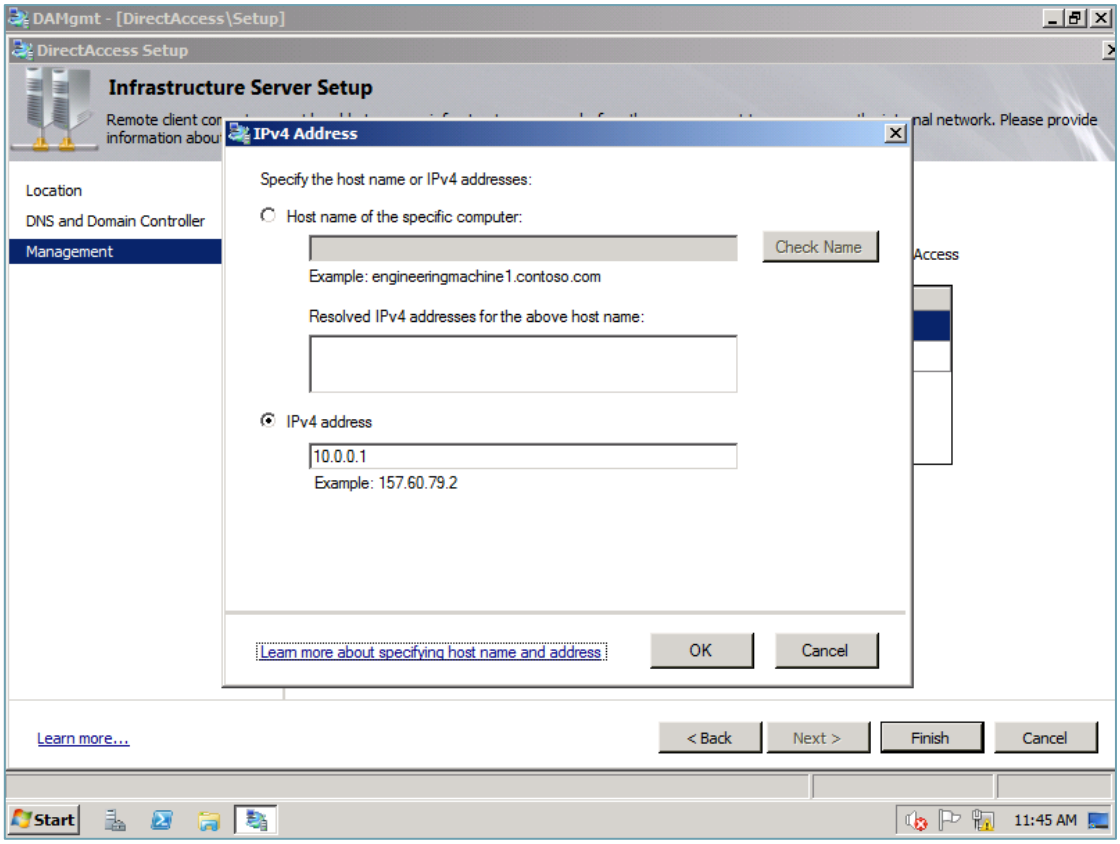
Ezen a lépésen belül van még két fontos ablak, egyrészt a DNS és Domain Controller gépek megadása és a local names névfeloldás (azaz a korábban említett NRPT) körüli beállítások:



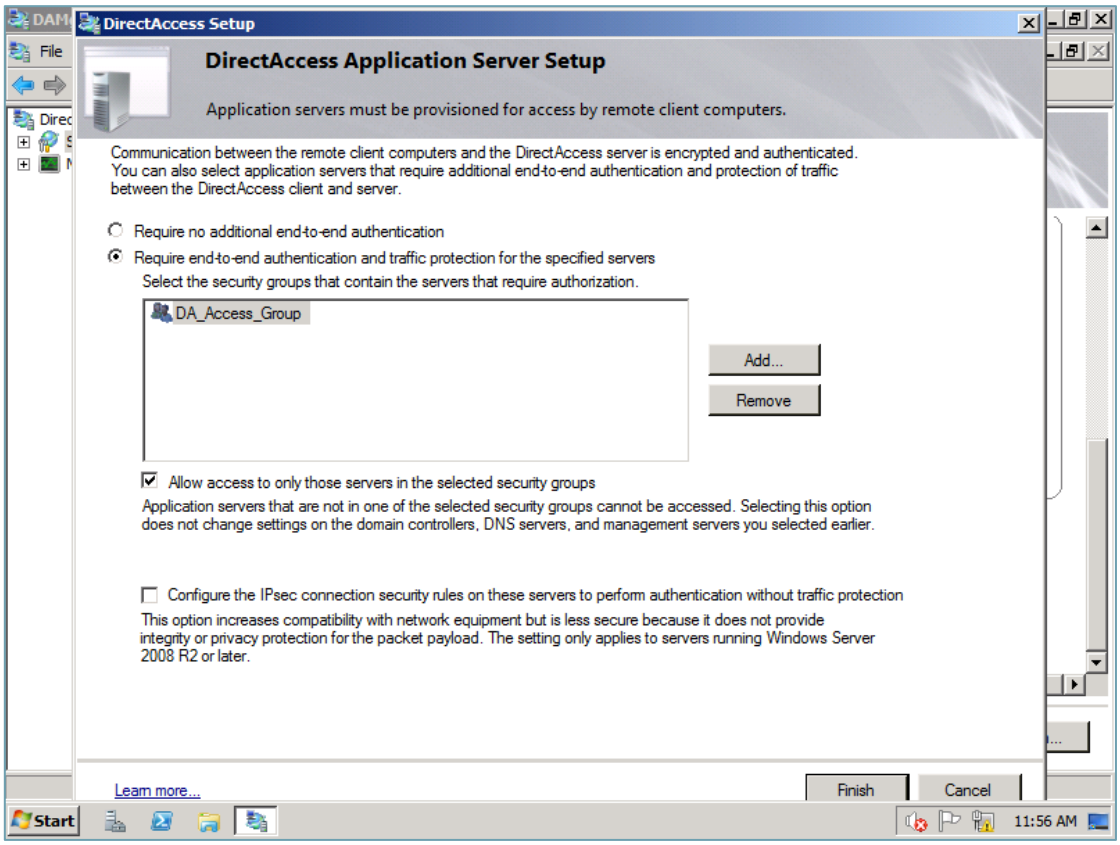
7.23 ÁBRA HA SZÜKSÉGES, EGY-EGY DNS SUFFIX-SZET RÁÍRÁNYÍTHATUNK A BELSŐ DNS SZERVERRE

3 lehetőségünk van, az első a szigorú, azaz csak és kizárólag az NRPT-t használja (magyarul csak azok a DNS infók élnek, amelyek helyben, és ebben szerepelnek), a második a „Fall back”, azaz elsődleges a megszokott DNS elérésünk (pl. otthon az ISP) és másodlagos az NRPT, vagy akkor is él ez a lehetőség, ha nem elérhető a szokásos. A harmadik is Fall back a helyire, de csak akkor, ha bármilyen DNS feloldási hiba van.
Még egy kicsit maradunk a harmadik lépésnél és a következő, Management ablakban megadhatjuk a klienseinket felügyelő (pl. egy SCCM vagy egy WSUS) szerverek elérését.

Ezután már csak egy lépés marad, az elérhető belső hálózati erőforrások kiválasztása, az a fajta szelekció, amikor korlátozzuk a belső hálózat erőforrásainak elérését, amit egy end-to-end hitelesítés kikényszerítésével tehetünk meg, illetve AD biztonsági csoportok formájában tovább szűkíthetjük az elérést, majd azért engedhetünk a gyeplőn egy kicsit, az IPSec kapcsolatok biztonsági beállításainak módosításával.

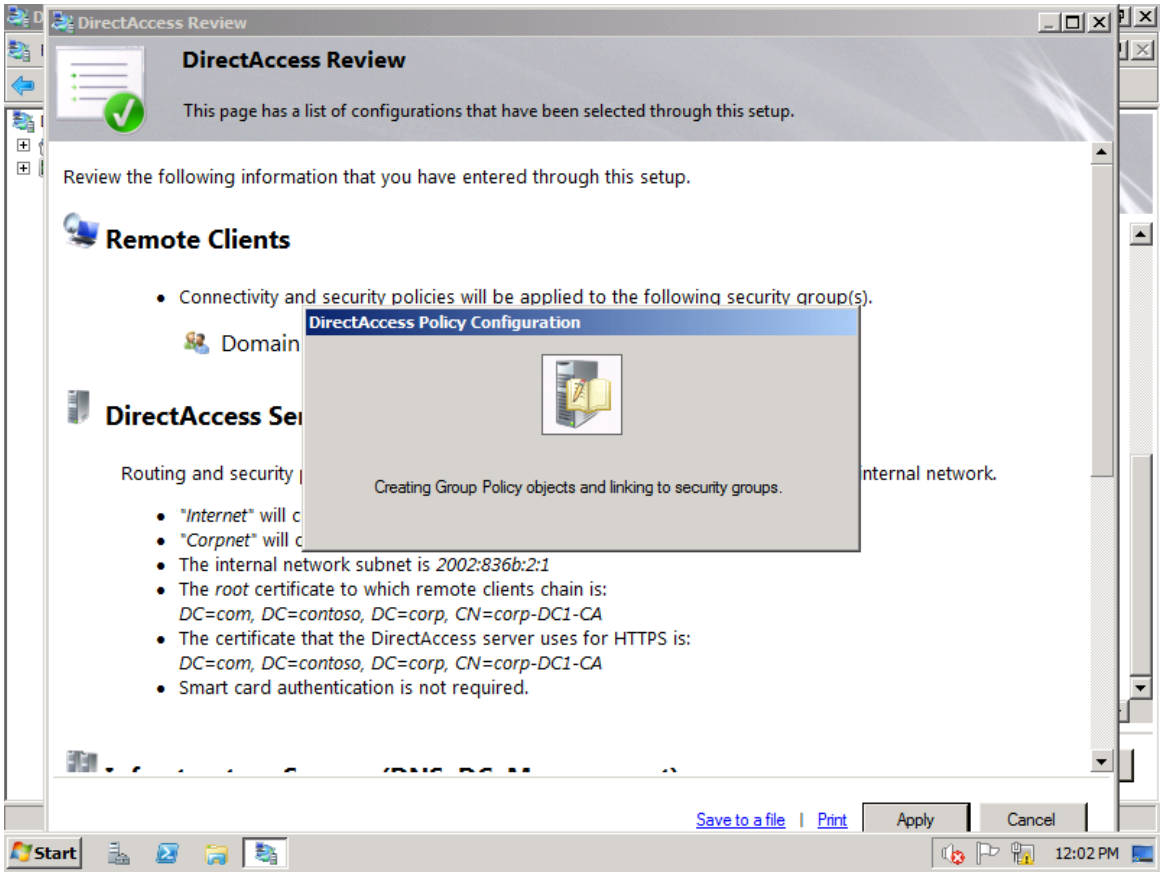


7.24 ÁBRA SZERENCSÉRE ELÉG AZ IPV4 CÍM, MAJD KORRIGÁLJA



7.25 ÁBRA RESTRIKCIÓ!

Ha kész, akkor nincs több ablak, de teendő azért még igen, mentsük el a konfigot a Save gombbal (szépen jelzi, hogy hol van ez a konfig fájl), majd nyomjuk meg a Finish-t is! Erre kapunk egy összegző ablakot, majd ha az Apply-t használjuk, akkor végzi el az érdemi munkát, azaz elkészíti a 2 db, az összes beállításunkat és adatainkat tartalmazó Csoportházirend objektumot – tehát nekünk ezzel nem kell foglalkozni.

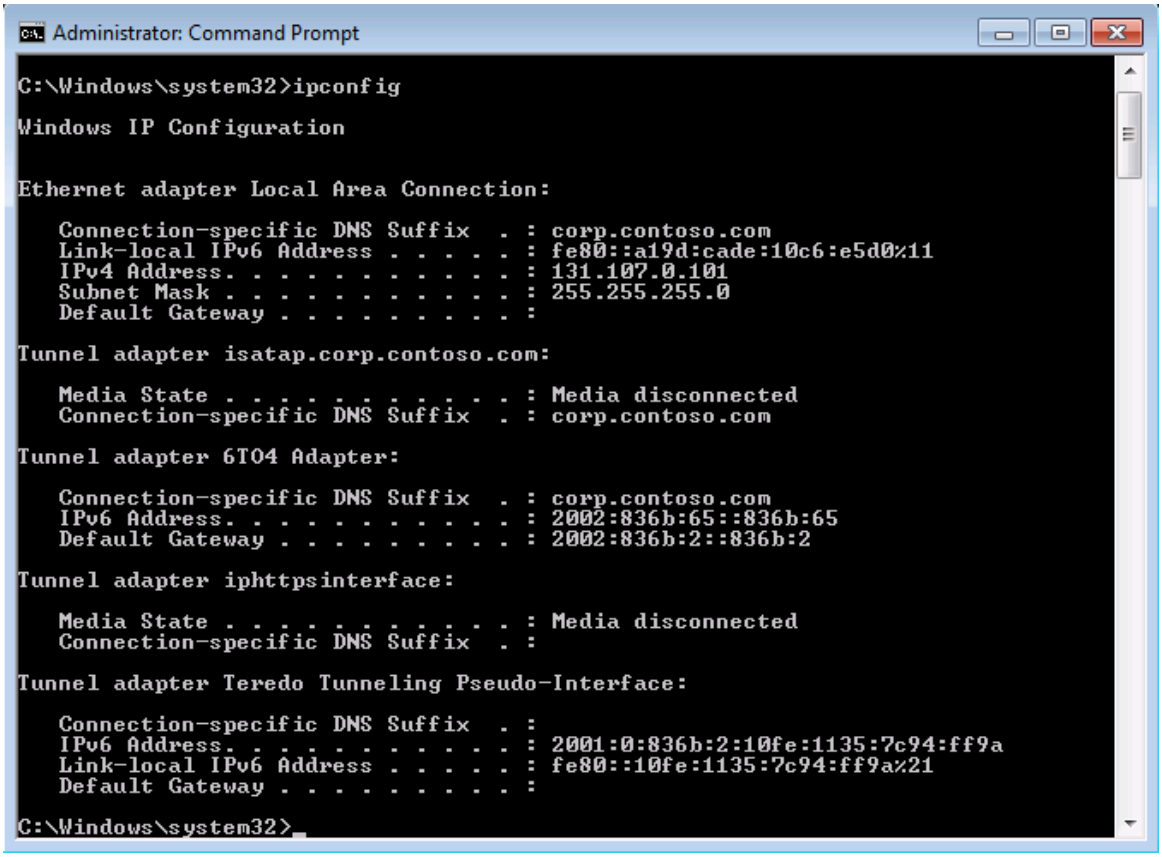


7.26 ÁBRA DOLGOZIK SZÉPEN

Gyakorlatilag ezzel végeztünk is, a sikerről képernyőképek formájában nehéz beszámolni, demózni sem volt könnyű sosem, hiszen csak annyi történik, hogy mindig működik, bármelyik hálózaton is található a gépünk. Ezután némi utómunka marad már csak, mint pl. a DC és az APP szerver IPv6-os infóinak frissítése (net stop/start iphlpsvc), illetve a kliens gépen egy „gpupdate”.

A kliens működéséről még annyit, hogy ugye, ahogy már erről szó volt, 3 külső tranziciós IPv6 protokollunk, amelyek automatikusan jutnak lehetőséghez az adott hálózat működési jellemzőitől függően, tehát:

- Ha kimegyünk a belső hálóból, és egy olyan hálózatba kapcsolódunk majd, ahol pl. publikus IP címünk lesz, akkor első körben jön a 6to4, ha esetleg ez valamiért nem működik (pl. egy proxy, stb.), akkor a Teredo. Azt, hogy melyik interfész él, az ipconfig paranccsal kiválóan lehet látni.

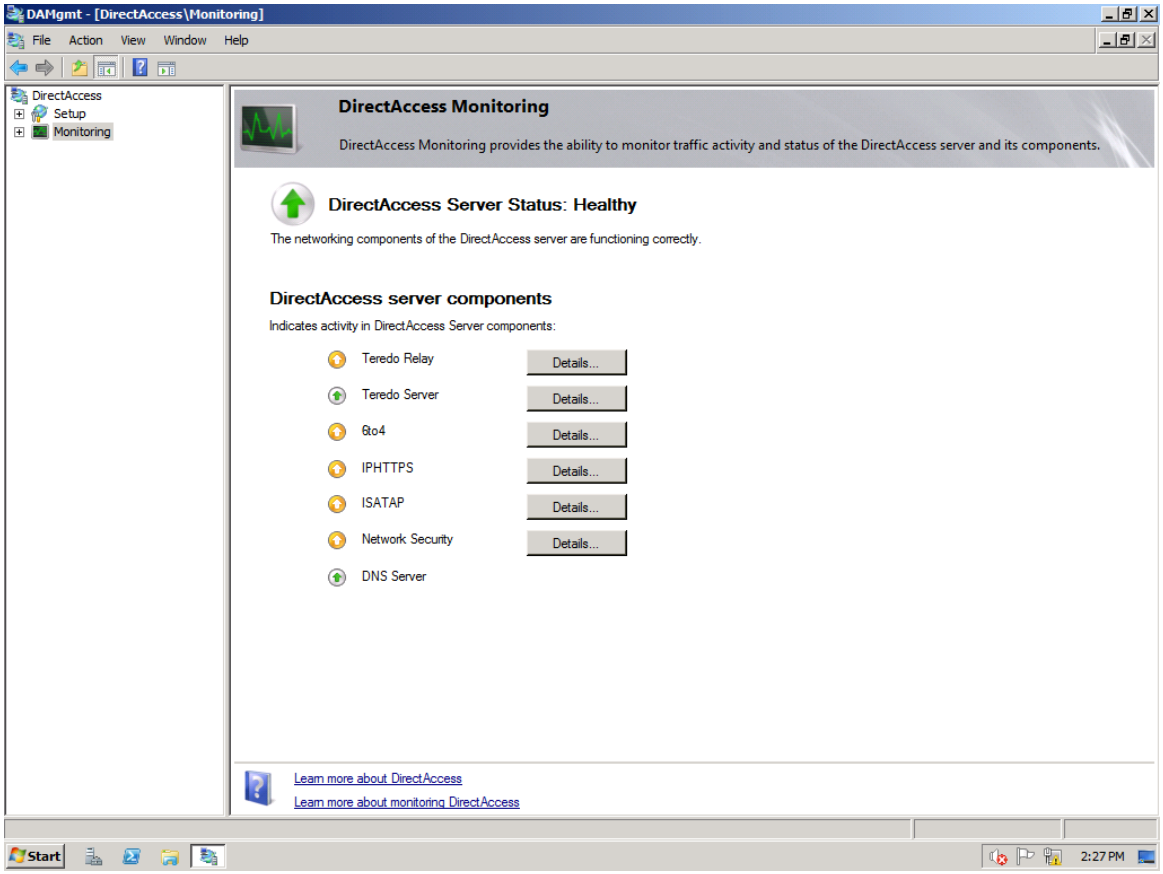


7.27 ÁBRA AZ IPCONFIG MINDENT ELÁRUL, MOST ÉPPEN AZ INTERNET HÁLÓBAN VAGYUNK, 6TO4-GYEL, DE LÁTSZIK, HOGY VAN MÉG LEHETŐSÉG

- Ha egy NAT-olt hálózatban vagyunk, pl. otthon, akkor a 6to4 egyből nem lesz megfelelő, a Teredo viszont igen, de ez sem 100%, proxy vagy hálózati eszköz szintén akadályozhatja. Ekkor jön az IPHTTPS, ami viszont a tapasztalatom szerint nem élesedik automatikusan, tehát nekünk kell kézzel tiltani - a Teredo-t, a következő paranccsal: „netsh interface teredo set state disabled [108]”. Ha jól van konfigurálva a DA, és a kliens is rendben van „tanúsítványilag” is (pl. CRL elérés), akkor az ipconfigból jól látszik, hogy sikerül beizzítani az IPHTTPS interfészt, ami aztán tűzfalon, proxy mindenen áthasít majd.

Azt, hogy éppen milyen protokollok és milyen forgalmi adatokkal működnek a DA szerveren, illetve hogy a DNS feloldás rendben van-e, azt a DirectAccess Management MMC-ből a „Monitoring” pont alól tudjuk ellenőrizni.

[108] Az engedélyezés és a tiltás között kicsit kevés a logikai összefüggés ☺: „netsh interface teredo set state enterpriseclient”

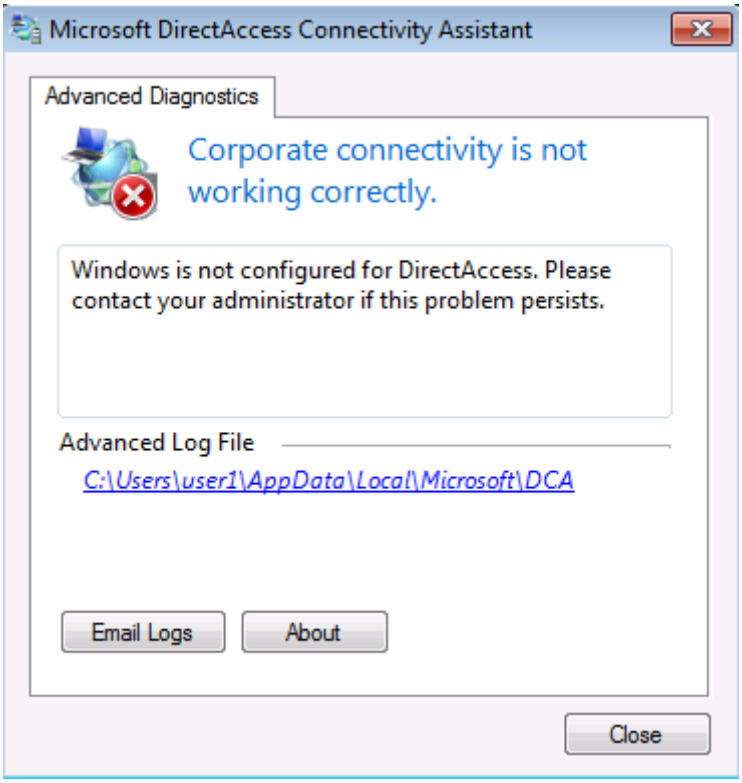


7.28 ÁBRA NU, MI MEGY ÉPPEN? (A SÁRGÁK INAKTIVITÁST JELÖLNEK, A ZÖLD MŰKÖDÉST.)

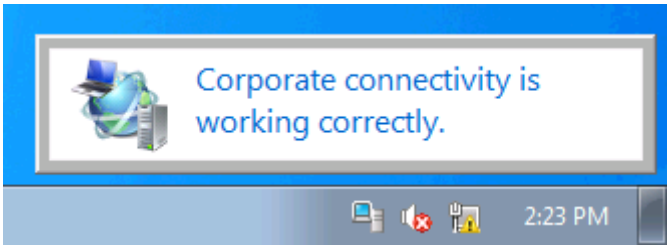
Még egy utolsó könnyítés (nehéz befejezni ezt az alfejezetet), mivel van egy probléma még: a kliensen elég nehéz látni, hogy most éppen működik vagy nem működik a kapcsolat. Gyárilag nincs semmilyen segédeszköz az operációs rendszerben erre, a felhasználó pedig nem fog ipconfig-ot beütögetni, de ha mégis, érteni nem fogja ☺.

Ezért készítette a Microsoft a DirectAccess Connectivity Assistant-ot, ami letölthető[109], és beüzemelhető, a Tálcán egy ikon formájában fog vizuális jelzést adni a DA kliens állapotáról. Kapunk egy telepítőt a kliensre, de ez még kevés lesz, a mellékelt Csoportházirend sablonok segítségével be is kell konfigurálnunk pár opciót, pl. azt, hogy mi a címe az NLS szerverünknek, amivel a segédeszköz ellenőrzése működni fog, vagy pl. az NPRT kliensoldali használatát is szabályozhatjuk egy kicsit. Illetve viszonylag egyszerűen tudjuk majd hibakeresésre is használni, lásd a következő képet.

[109] Itt mindent megtalálunk majd ehhez, pl. a részletes Deployment Guide-ot is: http://technet.microsoft.com/en-us/library/ff384241.aspx



7.29 ÁBRA ITT ÉS MOST BAJ VAN, NÉZZÜK MEG A NAPLÓFÁJLT IZIBE.



7.30 ÁBRA KÉSZ IS VAN, „TUDÁS ELLEN NINCS ORVOSSÁG”.

7.3 AMI A TELEPHELYEKEN FONTOS: BRANCHCACHE

Tömören összefoglalva: egy régi problémára egy új megoldás. A probléma az, hogy a telephelyeken lévő számítógépekről a központi erőforrások (fájlszerver, webszerver, alkalmazások, stb.) elérése és futtatása nehézkes, és így a felhasználók munkavégzése csorbul. Persze a WAN kapcsolat fejlesztése, a sávszélesség emelése gyógyír lehetne a fájdalmunkra, na de ez erősen költségfüggő téma, vagy akár fizikailag is megvalósíthatatlan.

De van megoldásunk az R2-ben (és csak abban), Windows 7 kliensekkel, a HTTP/S, a BITS (tipikusan Windows Update) és az SMB (fájlszerverek elérése) protokolloknál és ez a BranchCache. Ami ráadásul transzparens a felhasználók számára, értékes sávszélességet szabadít fel, plusz SSL támogatással is bír, tehát biztonságos is egyben.

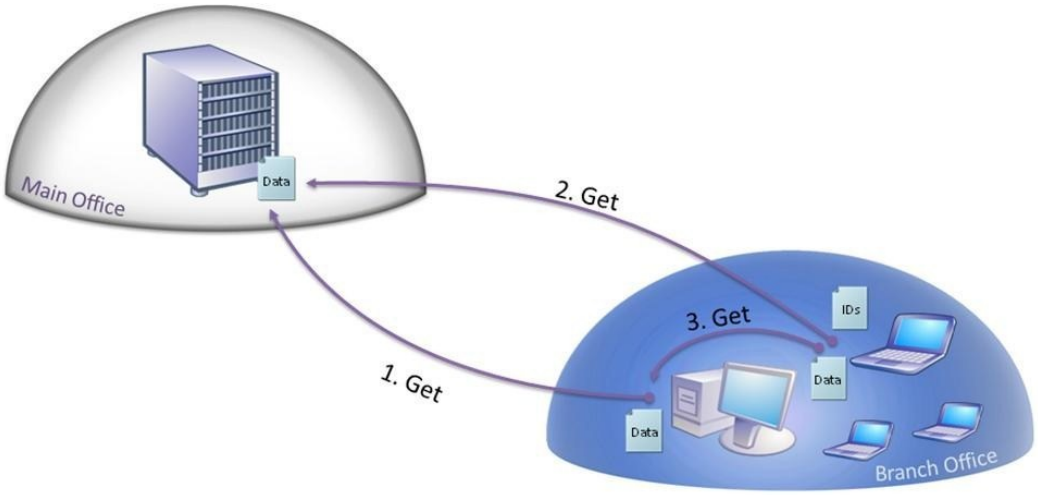
Csupa jó hír, nem?

Azonnal jelezni kell, hogy két fő típus is rendelkezésre áll, azaz kétfajta forgatókönyv létezik a telephely ellátottsága alapján:

1. Nincs szerver, viszont kevés felhasználó van – elosztott (Distributed cache)
2. Van szerver és sok felhasználó van – központi (Hosted cache)

7.3.1 A KÉT ÜZEMMÓD

Az első esetben (maximum 100 gépig ajánlott) tehát csak kliensek (a BranchCache szempontjából csak Windows 7) alkotják a telephelyi hálózatot, tehát a központi BranchCache szerver segítségével megszerzett gyorsítótárazott anyagok tárolása ezeken a klienseken történik majd meg, külön-külön. A BranchCache engedélyezése pedig a Csoportházirenden keresztül megy, és helyben a netsh-val fogjuk tudni piszkálni a lokális paramétereket.



7.31 ÁBRA ELOSZTOTT ÜZEMMÓD

A folyamat a következő módon néz ki, lépésenként:

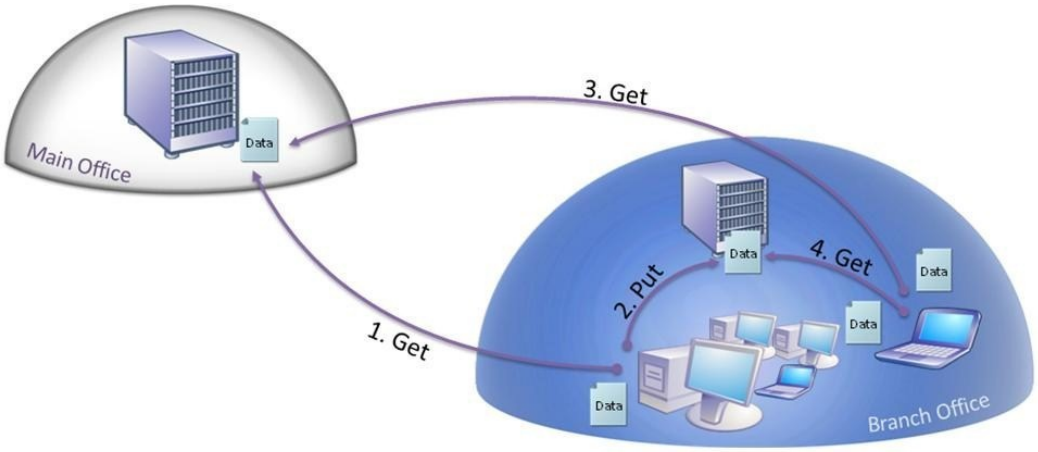
1. A kliens a központban lévő, már BC-vel működő intranet szerverről le akar tölteni egy fájlt.
2. Elsőre nem kapja meg, csak egy a hitelesítési / engedélyezési procedúra zajlik le, illetve egy „content metadata” csomagot kap csak a kezébe.
3. Ezzel a csomaggal és a WS-Discovery protokoll segítségével körbekérdezi a szomszédjait, hogy esetleg valamelyik letöltötte-e már a fájlt és esetleg tárolja is jelen pillanatban. De nem, mi most az elsők elsője leszünk, tehát a közvéleménykutatás eredménye most még zéró lesz.
4. Így aztán a kliensnek le kell töltenie a fájlt, teljes valójában, viszont immár a saját, erre a célra fenntartott gyorsítótárba teszi bele.
5. Ezután, hogy hogy nem, a második kliensnek is szüksége lesz erre a fájlra (mert ez pl. a fizetési jegyzék egy Excelben). Ugyanígy felszalad a központba, a hitelesítés és az engedélyezési eljárás ugyanaz lesz, és ugyanúgy megkapja a

„content metadata” csomagot is, benne a fájl blokkjai alapján kiszámolt hash-ekkel együtt.

6. Ezután viszont a WS-Discovery-vel összefütyül az egyes klienssel, az egyes jelzi, hogy talált, süllyedt, a második kliens pedig szépen elkéri tőle a fájlt, de ez a transzfer már titkosítva, a fenti szervertől kapott hash-ekből kombinált kulccsal történik meg.
7. A kettes kliens megpróbálja visszafejteni a fájlt, azaz az imént, helyben megszerzett fájl blokkjaiból kiszámolt hash-eket összehasonlítja a fentről kapott hash-ekkel, és ha rendben van, akkor már meg is győződött arról, hogy a tartalom változatlan, tehát felhasználható. Ha viszont változott, akkor sem szükséges az egészet leszedni újból, hanem csak a megváltozott blokkokat (a hash-ekből minden kiderül), ergo így is sokkal gyorsabb lesz.

A második esetben, amikor is egy R2-es szerveren - akár több más szerepkör mellett – a BranchCache képesség is fut, kicsit összetettebb az üzembe helyezés, viszont több előnye is van:

- 7/24-ben elérhető, mivel általában nem kapcsoljuk ki a szervert
- Valószínűleg jóval nagyobb tárterületet engedélyezhetünk
- Valószínűleg jóval nagyobb hálózati teljesítménnyel szolgálja ki a klienseket



7.32 ÁBRA KÖZPONTI ÜZEMMÓD

1. Ugyanaz, mint az előbb, a kliens felkúszik a központba, és a hitelesítés / engedélyezés után megkapja a szokásos csomagot.
2. A kliens keresi a fájlt a helyi hálón a hash-ekkel operálva, és ha ez az első próbálkozás, akkor fentről tölt.
3. Rögtön ezután a kliens egy SSL kapcsolatot épít ki a lenti BC szerverrel, és felajánlja neki a fájlra jellemző azonosító csomagot vizsgálatra.
4. A lenti BC szerver elfogadja ezt, és gyorsan megmondja a file blokk információ alapján, hogy mi van meg belőle, és az esetleges hiányzó/megváltozott blokkokat elkéri. Ha semmi nincs meg a fájlból, akkor az egészet elkéri.

5. Ha ezután egy másik kliens akar egy fájlt, akkor a fenti szerverhez megy újra a szokásos kezdő lépésekkel, és megkapja a szokásos azonosítót is.
6. Ezt a telephelyen használva a Hosted Cache szerverünk kötelességének érzi, hogy titkosítsa a szokásos módon, a szokásos méretre jellemző hash-ekkel, majd visszaküldje a kliensnek.
7. A kliens visszafejti, összehasonlítja a fentről kapott adatokkal, és boldogan konstatálja, hogy a telephelyi BC-től is megkaphatja az ezek szerint változatlan tartalmú fájlt, el is kéri, és használja, hurrá.

7.3.2 A BranchCache konfigurálása

A szolgáltatás konfigurálása sokkal kevésbé bonyolult, mint az elmélet, viszont értelemszerűen eltér egymástól a két forgatókönyv, plusz lesz majd közös teendő a központban is. Kezdjük először egy áttekintéssel, azaz az első lépésekhez nézzük át ezt a táblázatot!

Szerepkör	Helyszín	Mit is kell telepíteni?
BITS alkalmazás szerver, pl. WSUS	Központ	BranchCache képesség (Server Manager)
Webszerver	Központ	BranchCache képesség (Server Manager)
Fájlszerver	Központ	BranchCache rész szerepkör a File Services szerepkörön belül
Hosted cache szerver	Telephely	BranchCache képesség (Server Manager) és hosted cache kijelölés
Kliens	Telephely	Nincs telepítés, csak engedélyezés

7.33 ábra Hogy ne csak kapkodjuk a fejünket

És akkor kezdjünk el sorban haladni, az eleje egyszerű, csak a Server Manager kell hozzá, a negyedik sorhoz viszont már kell segítség:

Netsh BranchCache set service mode=HOSTEDSERVER

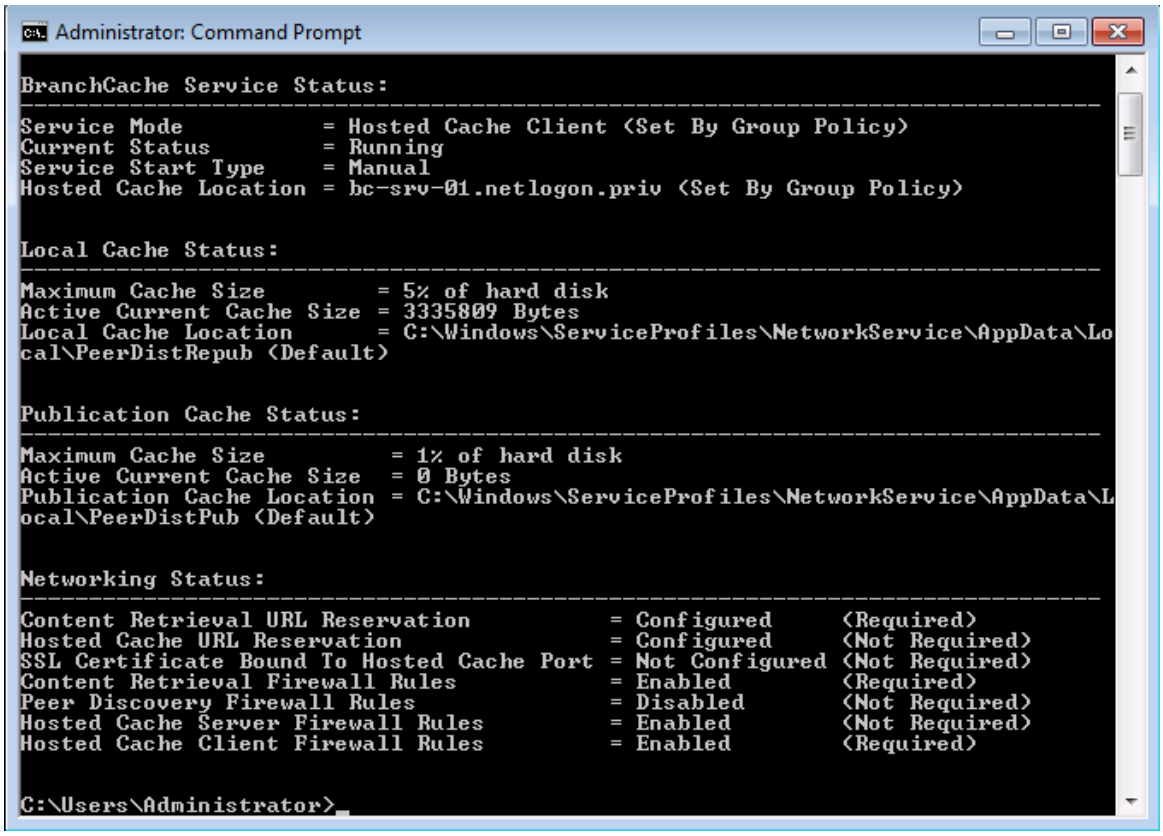
Ahogy a táblázatban is szerepel, a Windows 7-ben már alapértelmezés szerint „benne van” a BC kliens, csak engedélyezni kell, itt pl. az első módszerhez:

Netsh BranchCache set service mode=distributed

A következő parancs viszont bármelyik esetben használható, mégpedig az összes állapotinfó lekérdezésére:

NetSh BranchCache show status all

A következő képen használtam is ezt a parancsot, és jól látható, hogy ez egy Hosted Cache kliens a telephelyen, megvan a helyi BC szerver címe is, maximum 5%-ot használhat a lemezből, és az is, hogy már most is van kb. 3,3 MB a cache-ben, plusz alul a beállított jellemzők szummája is megtekinthető.[110]

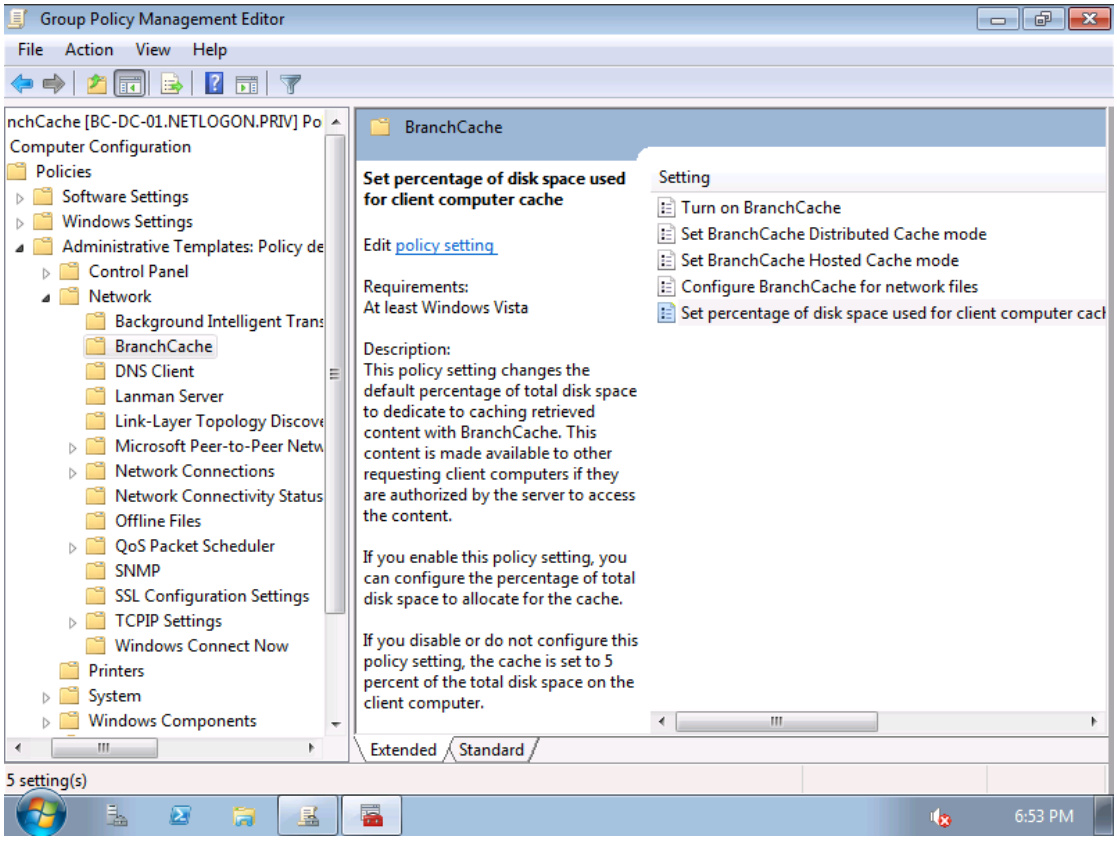


7.34 ÁBRA *NETSH BRANCHCACHE SHOW STATUS ALL*

De ha sokkal okosabbak vagyunk (és ha van tartomány [111]), akkor a Csoportházirendből érdemes mindezt beállítani, mivel így egyszerűbb.

[110] A „netsh branchcache reset" is jól jöhet, ezzel egy reset-et adhatunk a BC kliensnek.

[111] De a Helyi házirendből is elérhető, ha esetleg utáljuk a parancssort.

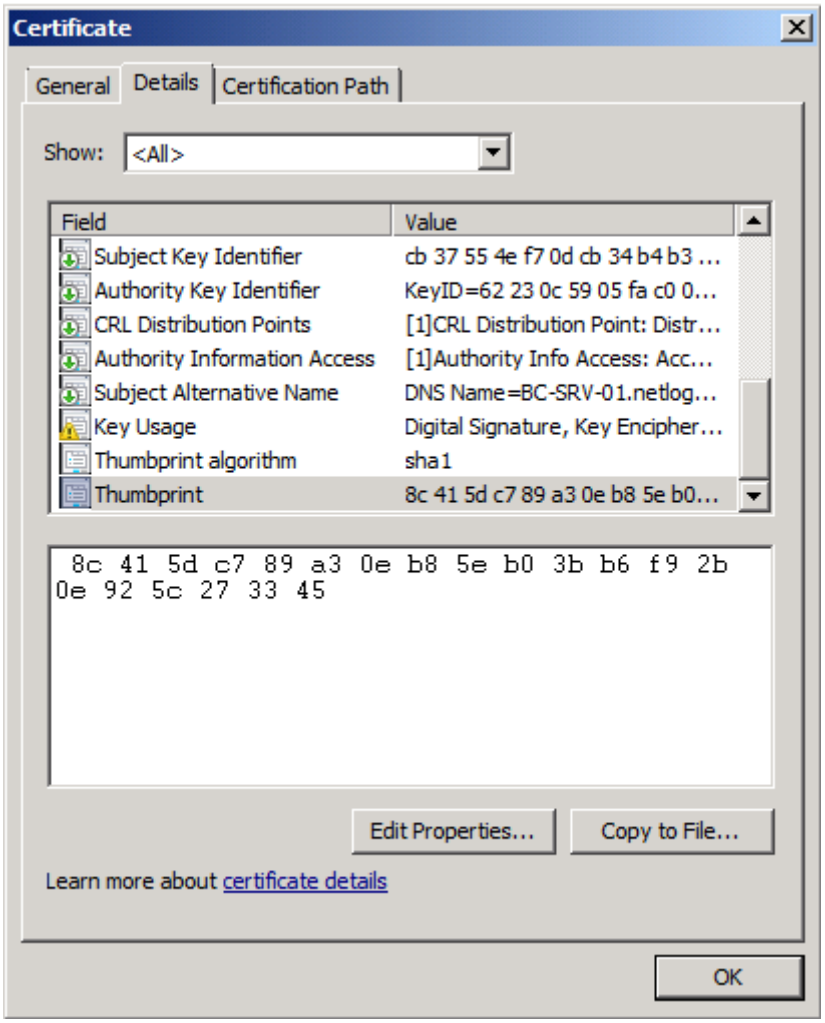


7.35 ÁBRA 5 OPCIÓ A CSOPORTHÁZIRENDBEN

Illetve a bekapcsoláson kívül további beállításokat is láthatunk az adott GPO-ban, pl. a működési típust vagy a cache céljaira lefoglalt hely méretét innen is be tudjuk állítani, de persze a netsh-val is lehet majd, helyben mindent.

A telephelyi szervernél azért nem csak ennyi a mulatság, egyrészt a netsh-val a méretet és egyebeket állítsuk be, de szó volt arról is, hogy SSL-lel kapcsolódik a kliensekhez, nos ez nem megy egy tanúsítvány nélkül, amit egyrészt be kell szerezni például a központban lévő CA szervertől (semmi extra, sima szerver tanúsítvány), de akár egy önaláírtat is használhatunk. Viszont aztán hozzá is kell rendelni a BranchCache szolgáltatáshoz, na ehhez viszont nincs GUI, ezért trükközni kell, méghozzá - milyen meglepő - a netsh-val.

Az első lépés az, hogy meg kell szereznünk az adott tanúsítvány SHA-1 hash-ét, azaz a thumbprint-jét, ami egy jó hosszú számsor. Ha megnyitjuk az adott .cer fájlt, akkor a Details fülön legalul megtaláljuk.



7.36 ÁBRA A TANÚSÍTVÁNY JÁTÉK KEZDŐDIK

Ha ez megvan, kimásolhatjuk egy text fájlba, szedjük ki belőle a szóközöket, és illesszük be a következő parancsba az *SHA-1_Hash* sztring helyére:

netsh http add sslcert ipport=0.0.0.0:443 certhash=SHA-1_Hash appid={d673f5ee-a714-454d-8de2-492e4c1bd8f8}

Ezzel aztán jól hozzárendeljük a tanúsítványt a BranchCache szolgáltatáshoz, ami nem túl barátságos művelet, de legalább csak egyszer kell megtenni. A következő paranccsal viszont ellenőrizhetjük, hogy jól kopipésztelünk-e?

netsh http show sslcert

Szóval így vagy úgy, de végre belőttük a klienseket és a lenti szervert, és dolgoznak is, de mi a helyzet a központban? A sima telepítések után van még dolgunk? Van bizony.

Emlékszünk a content metadata infóra és a hash-ekre? Akkor arra is, hogy ezek feltétlenül és egyúttal számtalan esetben szükségesek a normál BranchCache működés során, bármelyik forgatókönyvben ? Ezzel még nem is lenne akkora baj, de a gond ott van, hogy a hash-eket az R2 *online* csinálja, ami derekasan lassítja a folyamatot a szerveroldalon, ráadásul pl. egy webszervernél elsőre sosem csinálja meg, csak a második kérésre. De szerencsére segíthetünk neki, méghozzá kétféle módon is:

1. Parancssorból, manuálisan generálva használjuk a következő parancsot, megosztásonként: *hashgen –f E:\Test_share*
2. Csoportházirendből: *Computer Configuration > Administrative Templates > Network > Lanman Server > Hash Publication for BranchCache > Allow hash publication only for shared folders on which BranchCache is enabled*[112]

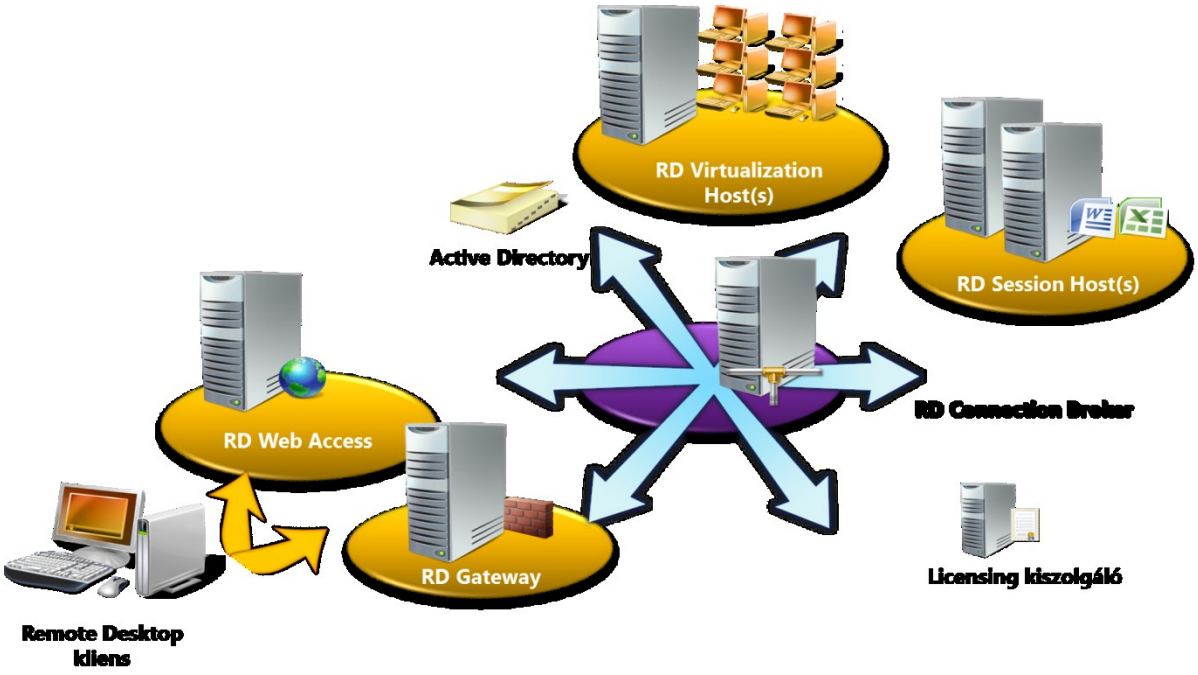
És akkor zárásképpen az alfejezet és egyben a fejezet végén, egy kis BranchCache FAQ-kal kedveskednék a Nyájas Olvasónak:

- Mikor lesz Vistára, XP-re, NT4-re kliens?[113]
  - Nem lesz.
- Mekkora a cache-be kerülési limit értéke?
  - 64 Kbyte.
- Milyen titkosítást használ?
  - Speciális sablonon alapuló AES128-at.
- Ha nincs WAN, működik?
  - Nem. Kell a kapcsolat pl. a hitelesítés / engedélyezés és a content metadata adatok miatt a központi szerverrel.
- Meddig marad a cache-ban a tartalom?
  - A beállított limit eléréséig vagy a „netsh branchcache flush” parancs manuális kiadásáig.
- Server Core-on fut?
  - Igen, sőt nagyon igen!
- WSUS-sal érdemes kombinálni?
  - Nagyon is.
- Milyen egyéb integrációt képzelhetünk el?
  - Pl. SharePoint-tal vagy éppen a DirectAccess-szel.

[112] Ehhez elfelejtettem egy dolgot: az adott megosztás tulajdonságainál, a Caching gomb alatt között engedhetjük/tilthatjuk a BranchCache-t.
[113] Viszont ne felejtsük: a Vistánál már van BITS PeerCaching, az is valami, sőt.

8 RDS + VDI

Anno amikor a Windows Server 2008-at teszteltem, teljesen megdöbbentem, hogy a terminálszolgáltatások területen mennyi változás és újdonság jelent meg már a béta verziókban is[114], akkor arra gondoltam, hogy a TS fejlesztő csapat durván kreatív munkát végez. A véleményem nem változott később sem, azaz az R2-re ugyanez elmondható, csak bírjuk követni az újdonságokat. Most megpróbáljuk.



8.1 ÁBRA A KOMPLEXITÁS BIZONYÍTÉKA

De mielőtt elkezdenék áradozni a rész szerepkörökről, muszáj megemlíteni, hogy az „átnevező kommandó” hálás tevékenysége miatt kialakulhat bennünk némi zavar. Az elmúlt tizenvalahány évben és így a Windows Server 2008-ban még Terminal Serverként (TS) emlegettük ezt a szerepkört, de a név az R2-ben megváltozott, mostantól az „RD”, azaz a Remote Desktop az előtag, tehát a helyes rövidítés az RDS (Remote Desktop Services).

Illetve még annyit elöljáróban, hogy itt sem választom ketté a két operációs rendszert, hanem megpróbálom az R2 apropóján megközelíteni a témát, ugyan a fejlesztések miatt van jó pár különbség az R2 előnyére, de egyúttal a változások növekményesek, azaz minden benne van az R2-ben, ami korábban is elérhető volt.

8.1 Session Host

[114] És aztán persze meg is maradt a véglegesben - mert nem mindig van ám ez így.

Azért is ezzel kezdem, mert ez a képesség a klasszikus, a Windows Server 2008 előtti terminálszerver. Azaz az, amikor még tényleg csak egy távoli szerverre történő belépési lehetőséget jelentett az RDP protokoll segítségével, és a felhasználók szempontjából pedig egy központi helyen, a kiszolgáló desktop környezetében történő alkalmazásfuttatást.

Az RDSH tehát több - maximum a licenszeink számának megfelelő mennyiségű – bejövő kapcsolatot fogad el, és egy-egy felhasználó részére egy-egy session-t foglal le, amelyből persze a felhasználó semmit nem lát, csak azt, hogy neki van egy számítógépe, alkalmazásokkal. Ennek a lehetőségnek a megteremtéséhez három rendszerszolgáltatást használ az operációs rendszer:

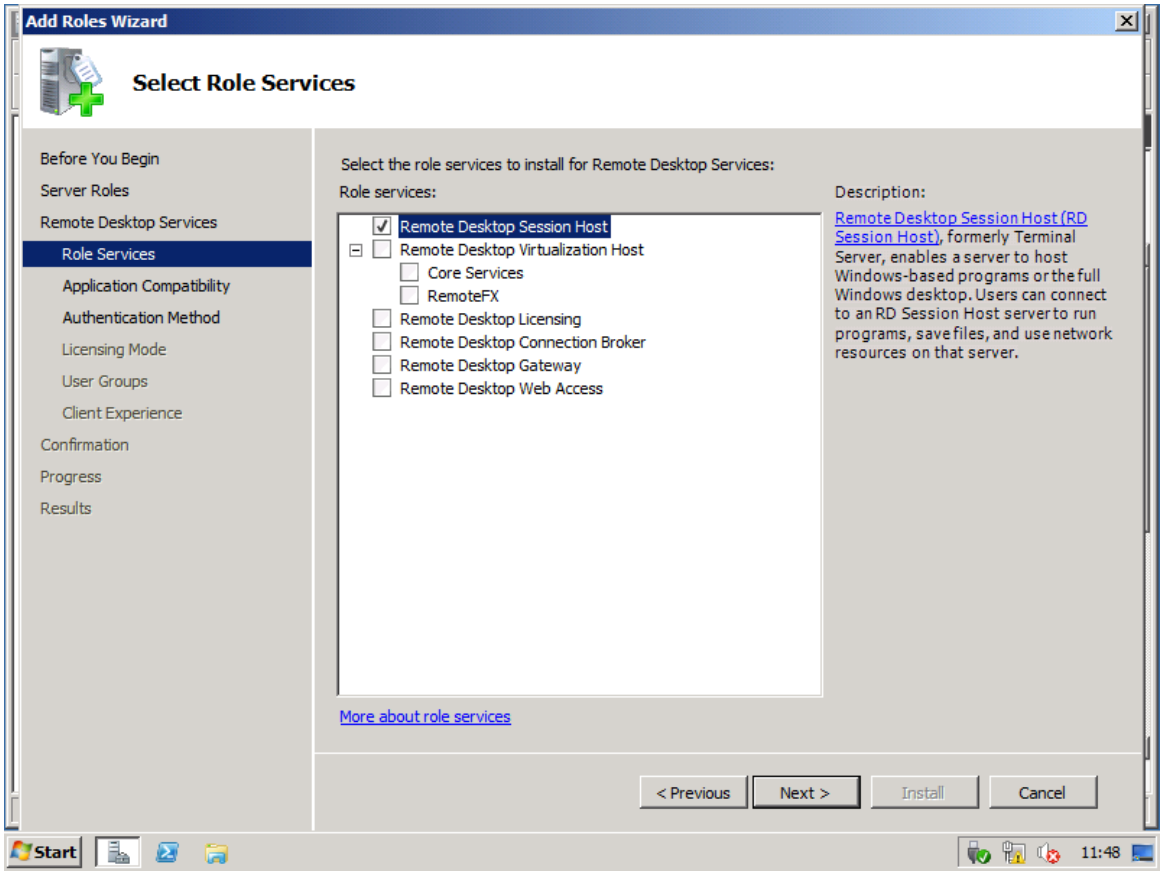
- Remote Desktop Services (az interaktív belepéshez)
- Remote Desktop Configuration (rendszer konfiguráció, a „SYSTEM” biztonsági kontextusban, tehát igen magasan)
- Remote Desktop Services UserMode Port Redirector (eszköz átirányítások biztosítása)

> A Windows Server 2008 előtt, ha szerettük volna pl. egy konfiguráció változtatás miatt leállítani vagy újraindítani az akkor még „Terminal Server” néven hívott szolgáltatást, akkor csak az egész gép újraindítás volt a megoldás. Ma már ez nem így van, a szervizeket akár VBScript-tel, akár PowerShell-lel, akár a konzolon a Services MMC-ben kézzel is megtehetjük.

Ha szeretnénk egy RDSH szervert telepíteni, a Server Manager-ben kell kezdenünk, figyelembe véve azt az ökölszabályt, hogy például tartományvezérlőkre [115] nem telepítünk RDS szervert, illetve igazából semmi más nagy szerepkörrel nem kombináljuk az RDS-t, főképp azért, mert ezt a szervert tényleg interaktív módon fogják a felhasználók használni.

És persze természetesen alaposan meg kell terveznünk az adott szerver hardveres konfigurációját is, hiszen adott esetben, magas felhasználószámmal és sok alkalmazással extrém terhelésnek is ki lesz téve ez a gép[116].

[115] Biztonsági és praktikus (üzemeltetési) okokból sem.
[116] A méretezéshez egy komoly segítség, a Remote Desktop Load Simulation Tools: http://www.microsoft.com/download/en/details.aspx?id=2218



8.2 ÁBRA ÍME AZ ÖSSZES NAGY RDS ALKOTÓELEM, DE NEKÜNK MÉG CSAK AZ RDSH KELL

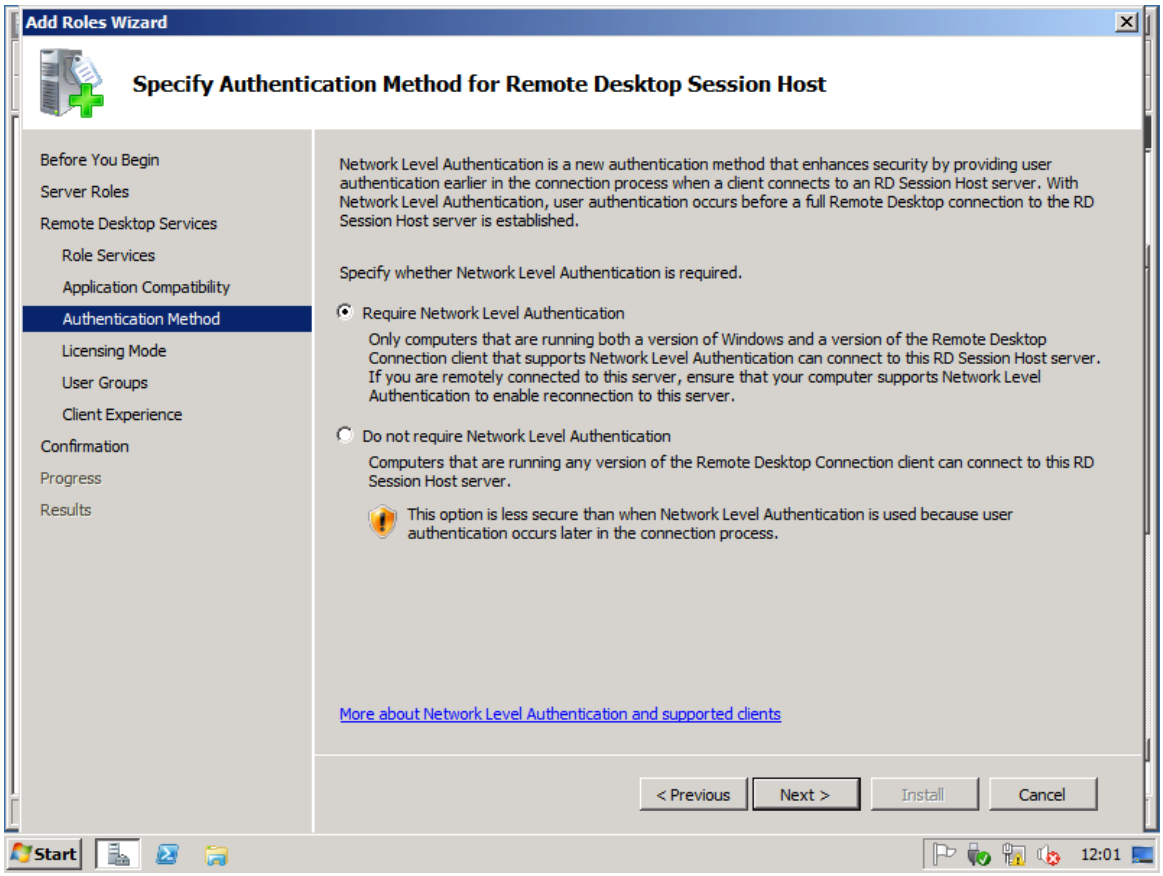
Ez egy olyan telepítő varázsló, amely további jelzéseket is ad, illetve további kérdéseket is feltesz, például az alkalmazás-kompatibilitással kapcsolatban jelzi, hogy akkor telepítsük ezt a komponenst, ha még nem pakoltuk tele a szervert alkalmazásokkal, mivel (és ez persze korábban is így volt) az RDSH előtti alkalmazások kicsit másképp, vagy éppen sehogy sem fognak működni a terminálszolgáltatások használatakor.

A következő lépésben pedig az NLA (Network Level Authentication) alkalmazása a kérdés. Az NLA további biztonságot és szerver erőforrás takarékoskodást jelent, és arról van szó, hogy a felhasználó a terminálkapcsolat indításakor nem a szerver desktopját, azaz a logon képernyőt kapja, hanem csak egy autentikációs ablakot. Tehát csak és kizárólag akkor eshetünk rá teljes sávszélességgel a szerverre, ha biztosan van a belépéshez jogosultságunk. Arról nem is beszélve, hogy egyfajta DoS (Denial-of-Service) kísérletet is kivédünk ezzel, a helytelen belépési kísérletek elkerülésével, amivel meg a szerver hardvert kíméljük meg a plusz terheléstől.

A NLA csak a RDC 6.x kliens felett működik, és a CredSSP-t használja (Credential Security Provider CredSSP) a korai hitelesítésre, ergo:

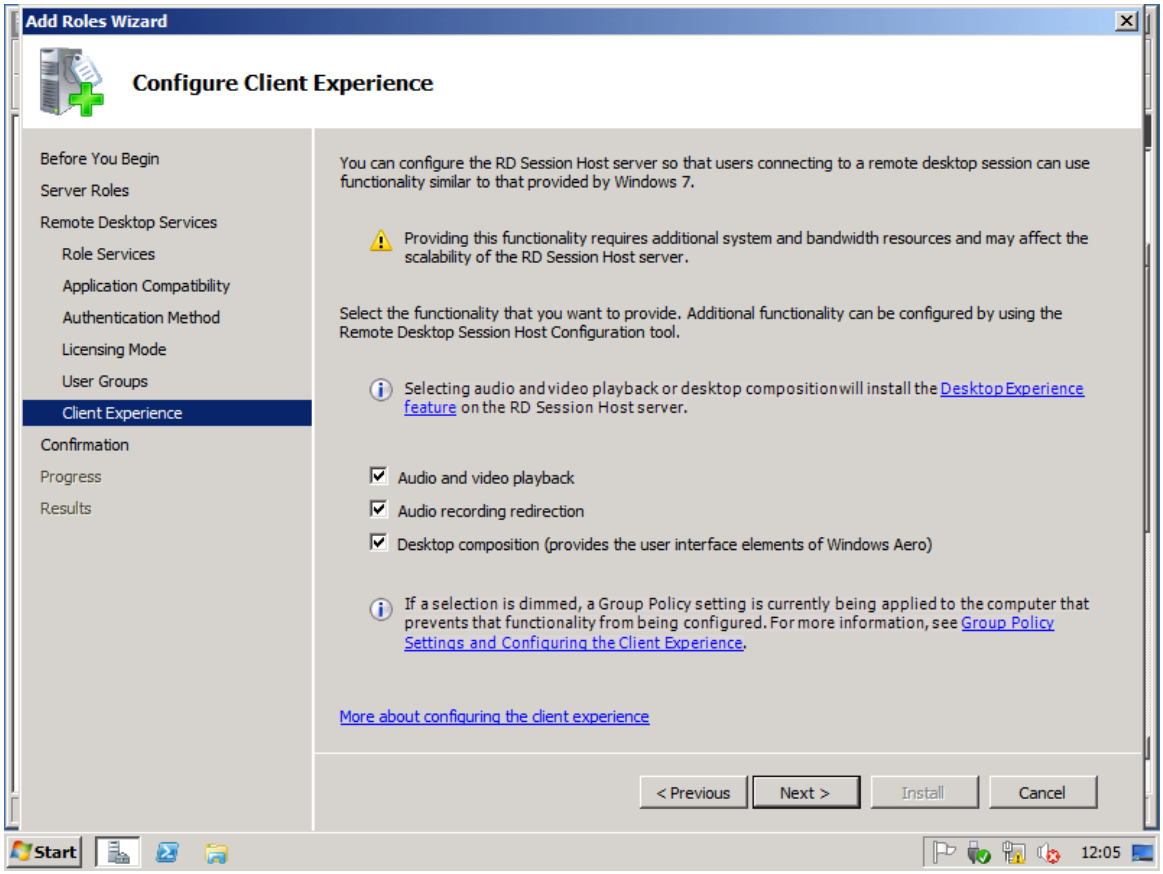
- Csak a CredSSP támogatással rendelkező operációs rendszerek használhatják az NLA-t (Windows 7, Vista SP1 vagy későbbi, XP SP3).

- Az NLA nem elérhető a Vista RTM vagy az XP SP2 számára, mivel a CredSSP támogatás mindkét esetben a következő szervizcsomaggal érkezik.
- Nem kell azért ezt itt véglegesen eldöntenünk, természetesen később is lesz lehetőség változtatni ezen a beállításon.



8.3 ÁBRA NLA VAGY NEM

Ezután még egy – szerencsére későbbre is halasztható - kérdés is lesz, mégpedig a licenszelésről. Lépjünk ezen is túl, és akkor már csak az RDSH felhasználói körét kell kiválasztanunk, megfelelő alapossággal (persze ezen is változtathatunk később). Viszont ami most jön, az teljesen új elem, ugyanis az RDSH számos, a felhasználói élményt alaposan növelő szolgáltatással is rendelkezik, ezek közül itt hármat rögtön ki- vagy bekapcsolhatunk, de később lesz még több is.

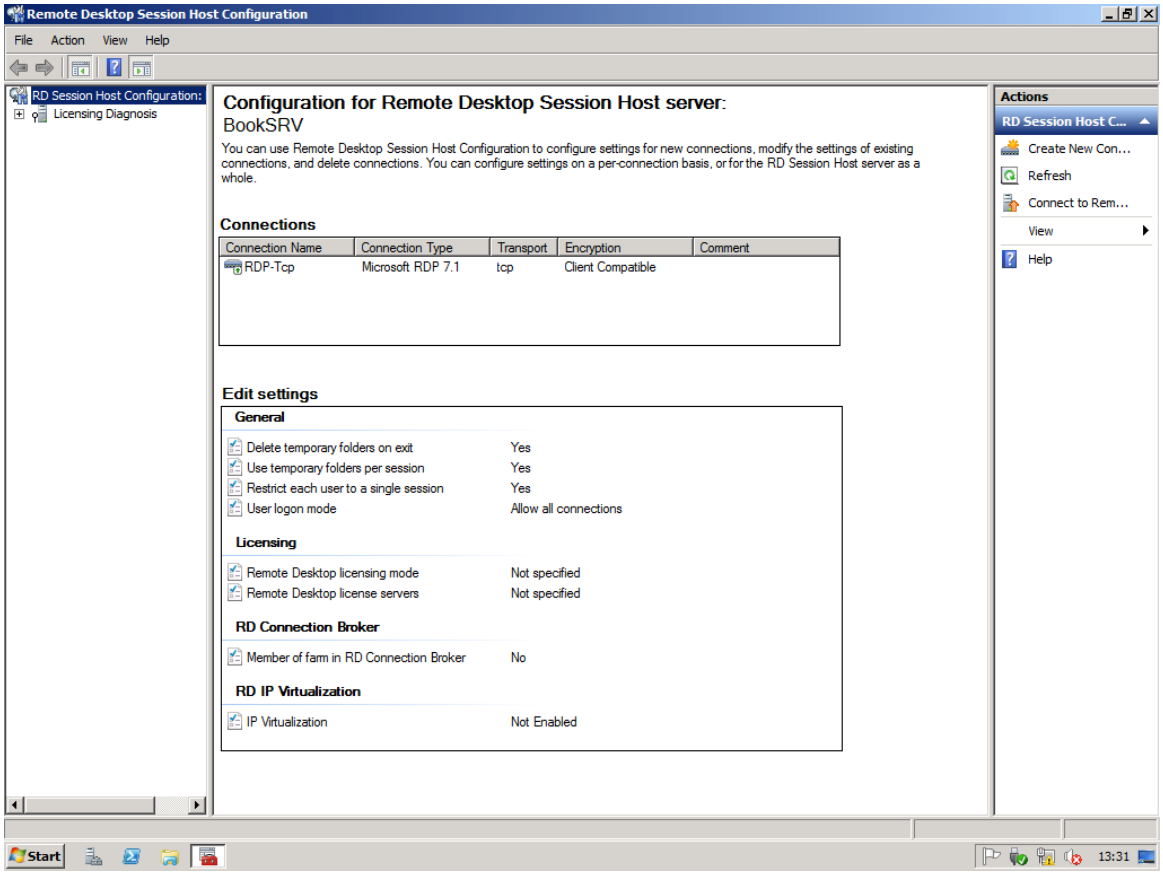


8.4 ÁBRA A UX AZ EGEKBEN IS LEHET

A harmadik sok esetben tényleg fontos lehet – a felhasználók számára, ti. az olyan megjelenítésbeli extrák, mint a Windows Flip, a 3-D ablak kezelés vagy a az ablakok átlátszó kerete, melyek mind részei a távoli „Aero Glass” lehetőségnek.

Ha viszont az „Audio and Video Playback” vagy a „Desktop Composition” élményt bekattintjuk akkor ne csodálkozzunk, hogy a „Desktop Experience” képesség is felkerült automatikusan rendszerünkbe (Desktop Themes, Windows Media Player, stb.).

Több dolgunk nincs, egy újraindítás után immár birtokba is vehetjük az RDSH-t, azaz egyből lett is egy terminálszerverünk. Vizsgáljuk is meg, ízibe, a Remote Desktop Session Host Configuration elemet elindítva (Administrative Tools \ Remote Desktop Services)!

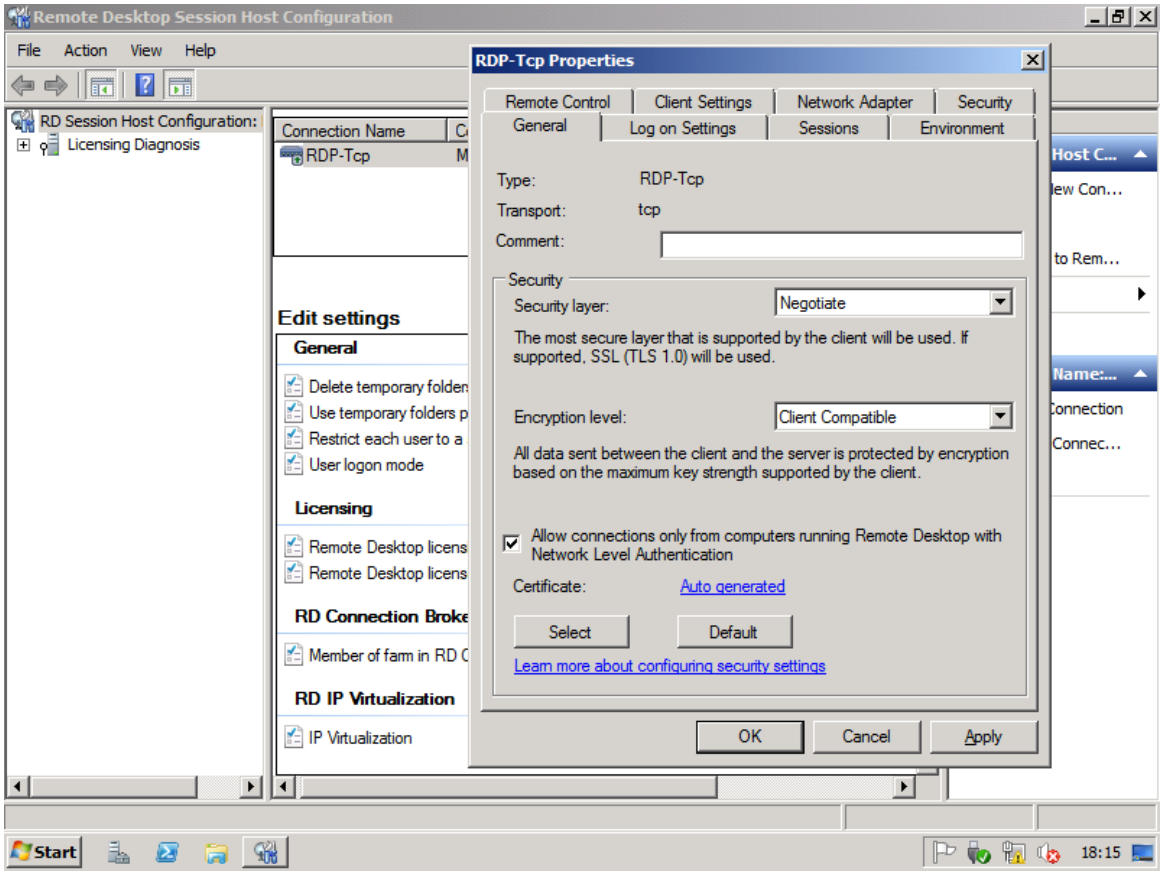


8.5 ÁBRA AZ RDSH-BAN TÖBB VAN, MINT ELSŐRE GONDOLNÁNK

A „Connections” szakaszban az RDP kapcsolatok közös jellemzőit tudjuk konfigurálni. Ha kicsit jobban megnézzük, látható, hogy ez már a 7.1-es RDP-t jelenti, ami az R2 SP1-es verzió. Ha 6.1-et látunk itt, akkor a Windows Server 2008-at használjuk, ha a 7.0-át, akkor az R2 RTM kiadást.

> Egyébként, ha az ezt megelőző telepítési procedúrát nem csináltuk meg, akkor is elérhető itt a beállítások egy része, hiszen az admin módú RDP-t is kezelni kell, ami viszont minden Windows Server-ben elérhető (még ha nincs is engedélyezve alapértelmezés szerint). Ugyanez igaz az RDS programcsoportból elérhető „Remote Desktop Services Manager-re, ami kifejezetten az aktív RDP kapcsolatok kezelője, azaz itt nézhetjük meg az aktuális munkamenet listát, itt választhatjuk le vagy léptethetjük ki a felhasználókat, vagy üzenhetünk nekik vagy éppen átvehetjük a képernyőjüket és stb.

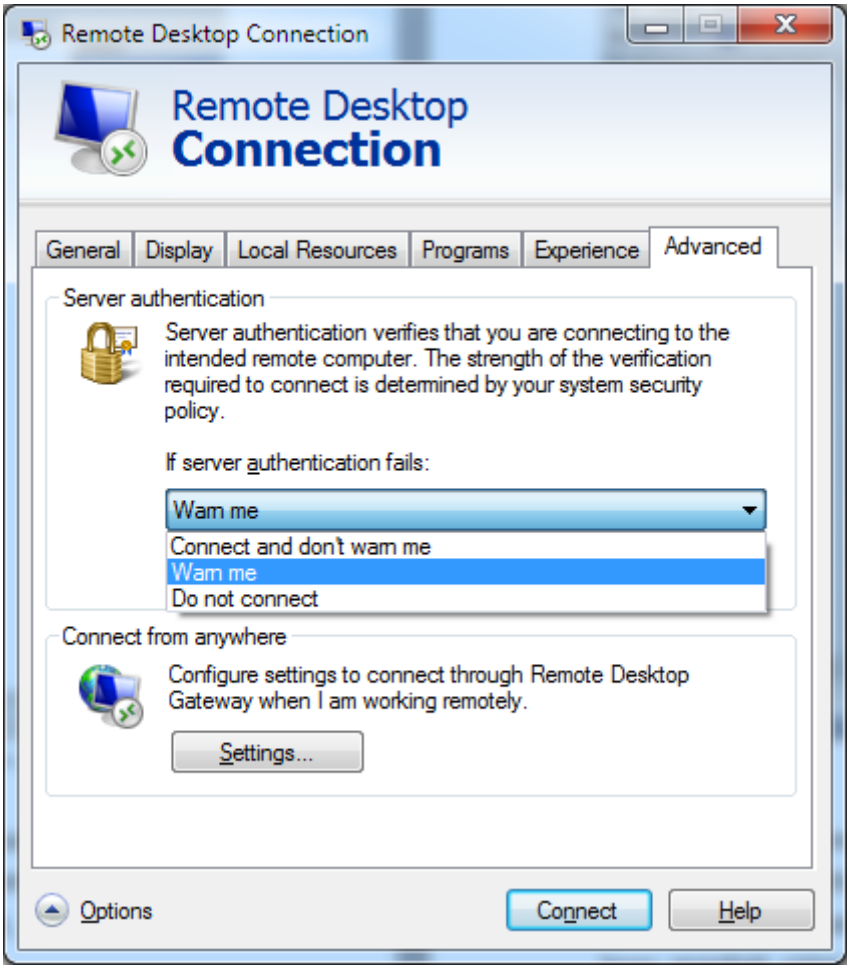
Az RDP-Tcp tulajdonságok közül néhány újdonságot és/vagy fontosat kiemelnék. Kezdjük a „General” fül tartalmával!



8.6 ÁBRA BIZTONSÁG MINDENEKFELETT

Az elsődleges biztonsági beállításokat itt találjuk (alul a már emlegetett NLA). A „Security layer” alatt választhatunk szerver hitelesítési megoldást, RDP, SSL (TLS 1.0) vagy éppen a megegyezéses (Negotitate).

Az utóbbi az alapértelmezés, ami abból indul, hogy mindkét oldal a TLS-t használja majd. Ha nem, akkor attól függ, hogy lesz-e kapcsolódás, hogy a kliensben a következő képen látható beállítás hogy áll.

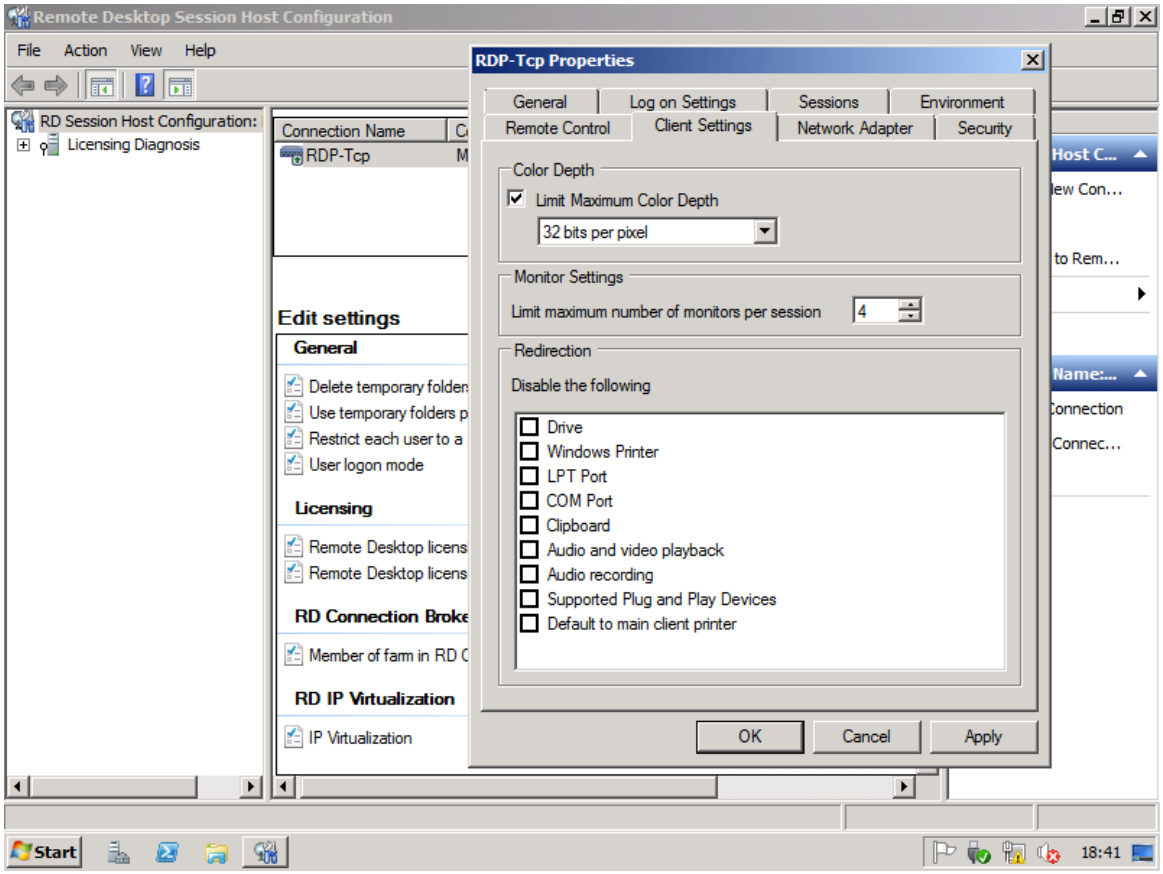


8.7 ÁBRA MI LEGYEN, HA NINCS TLS?

Ez alatt állíthatjuk a minimális titkosítási szintet a szerver és a kliens között, és végül a „Certificate:" mezőben, kicsit eldugva generálhatunk egy önaláíró tanúsítványt, vagy kiválaszthatjuk azt, amellyel a kiszolgáló azonosítja majd magát a kliens felé.

Visszatérve a 8.6 ábra többi fülére, még egyet emelnék ki (a többi vagy ismert, vagy valószínűleg sosem kell hozzányúlni), ez pedig a „Client Settings". Ezen belül a felhasználóink élményfokozását végezhetjük el, azaz egyrészt a profilban megjelenő felhasználói környezet grafikai jellemzőit szabályozhatjuk (színmélység [117], több monitoros környezet, audio/videó lejátszás), másrészt az eszköz átirányításokat (lemezek, printerek, vágólap, PnP eszközök, stb.) engedhetjük vagy tilthatjuk – globálisan és a kliens beállításait felülírva.

[117] Ha pl. levesszük a „32 bits per pixel" értéket kisebbre, akkor kikapcsoljuk az Aero-t, ez néha - például csekély sávszélesség esetén - igen sokat segít.

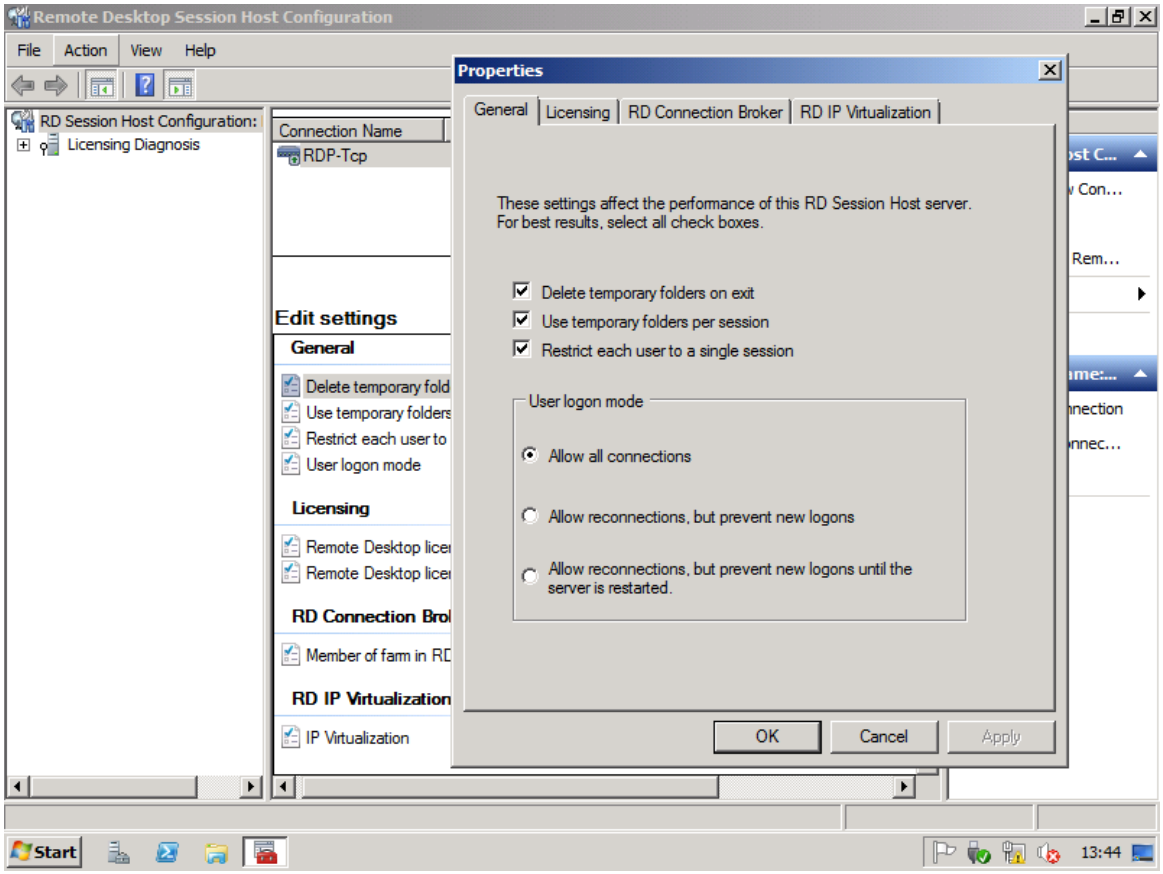


8.8 ÁBRA AZ UX FEJEZET FOLYTATÓDIK

Ha végeztünk az RDP-Tcp füleivel, és ezek után viszont az „Edit Settings” részbe kattintunk, mindig ugyanaz a panel jön majd fel, igaz, több füle is van, kicsit trükkös, de ez ilyen.

A tartalma azért vigasztaló, ugyanis rögtön az első fülön (General) egyrészt a felhasználók munkamenet korlátozásait (felhívnám a figyelmet az egyetlen használt session-re utaló opcióra: „Restrict each user to a single session”), másrészt a belépési módokat tudjuk szabályozni, és pl. karbantartás esetén jól tudjuk használni a „Drain” üzemmódot[118], a második vagy a harmadik lehetőség választásával.

[118] Ilyenkor ugyanis új RDP kapcsolatokat nem fogad el a szerverünk, de a meglévők maradhatnak és akár újra is csatlakozhatnak, ha megszakad a kapcsolat.



8.9 ÁBRA A TELJESÍTMÉNY OPCIÓK

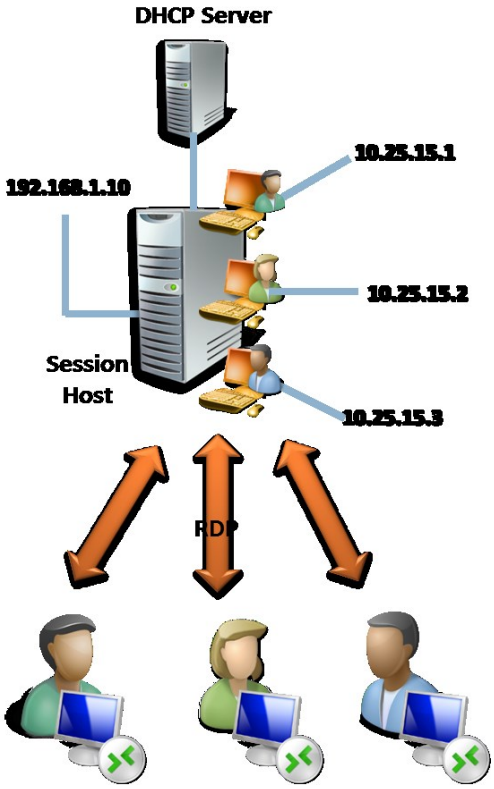
A második fül, a licenszelés témakörhöz tartozik, ugyanis itt adhatjuk meg a már előzetesen felkonfigurált licensz kiszolgálónk nevét, a licenszek típusát, és mindezt egészen egyszerű módon. Ha ezt nem tesszük meg, akkor 120 napig a Tálcán felbukkanó buborékok formájában folyamatosan kapjuk majd a felszólítást erre.

> Csak a tisztánlátás kedvéért: nem itt konfiguráljuk és érvényesítjük a megvásárolt licenszeinket, itt csak egy hivatkozást adunk meg a megfelelő szerverre és a típusra (persze könnyen lehet, hogy önmaga lesz a célpont). A licensz kiszolgáló beállítása, aktiválása és a licenszek érvényesítése egy külön alkalmazásban történik, ez szépen látszik is a 8.2 képen.

Az RD Connection Broker rész már sokkal izgalmasabb, igaz, most még nem tartunk ott, hogy ezzel is foglakozzunk, most csak annyit, hogy egy RDSH sokféle módon kapcsolódhat egy RDCB-hez, vagy lehet egy VDI környezet része is (lásd később), sőt egy RDS farm tagja is, amelyben az NLB segítségével épp magas rendelkezésre állást művel. Szóval, jóval több ám az RDSH, mint ami az elődje, azaz egy klasszikus TS volt, de tényleg nem tartunk még itt, be is fejezem.

Ami viszont ide tartozik, az az IP virtualizáció, merthogy ilyet is tud a mi RDSH-nk. Van, amikor arra van szükség, hogy az adott session például egy (rosszul megírt) alkalmazás igénye miatt kivétel nélkül mindig ugyanazt az IP címet kapja. Ez eddig

orosz rulett volt, mert vagy így volt, vagy nem, most már viszont beállítható akár minden egyes felhasználónak egy dedikált, egyedi IP cím.



8.10 ÁBRA ARCUK NINCS, DE EGYEDI IP CÍMÜK VAN!

Ezt persze csak akkor tehetjük meg, ha van egy DHCP szerverünk, meg tisztázni kell azt is, hogy melyik interfész hálózatán óhajtunk ilyesmit csinálni, és persze biztos, ami biztos alapon fallback van (a gép eredeti IP-je), de ennyi, a DHCP-ben például semmi extrát nem kell konfigurálni, megy magától. Ja és el ne felejtsem, 2 db Csoportházirend opció is rendelkezésre áll, az egyikkel ki-be kapcsolhatjuk az IP virtualizációt, a másikkal meg pl. letilthatjuk a belépést, ha nem kap pl. az adott alkalmazás a DHCP-től címet.

Van itt még valami, ami viszont a GUI-n nem látszik, de azért létezik, sőt alapértelmezés. Úgy hívják, hogy DFSS (Dynamic Fair Share Scheduling), vagy röviden FairShare. Ez egy CPU időzítő megoldás a terminál felhasználók számára, mondhatni egy proaktív igazságosztó. Merthogy elvileg és eddig egy user egy munkamenetben[119] simán kisajátíthatta a processzort, de ennek vége, a munkamenetek súlyozásra kerülnek, a kernel scheduler leosztja a lapokat, mindegyik munkamenet kap egy szeletet a CPU-ból egy adott időintervallumra, és ha ezt eléri, akkor a következő menet kezdetéig kényszerpihenőre kerül. Rend a lelke mindennek.

[119] Annyira írnám a session-t, csak hát ez egy magyar nyelvű könyv.

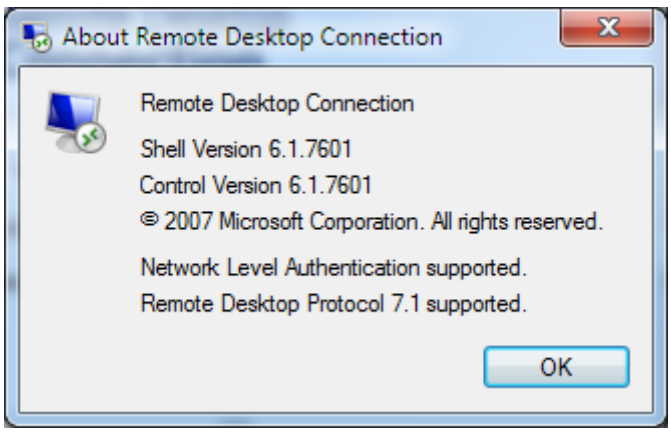
> Ha már itt tartunk, és szó van a folyamatok erőforrás kihasználásáról, akkor nézzünk utána a Windows Server Resource Manager + RDS témakörnek (például a Windows Server 2008 apropóján, mert ugye ott nincs még FairShare). http://technet.microsoft.com/en-us/library/cc742814.aspx

És még valami, ami szintén ide tartozik. Ez az Easy Print, ami két fő részből áll, az ún. RD Easy Print meghajtó programból és a hozzá tartozó Csoportházirend opciókból. Az Easy Print támogatás az RDP 6.1 kliens óta létezik.

No ez az a pont amikor meguntam a kliensek külön-külön emlegetését, innentől az alábbi táblára fogok hivatkozni, a következő képen meg egy módszert látunk arra, hogy kideríts ük, hogy milyen klienssel is rendelkezünk.

	Win7/ R2	Vista SP+	Vista SP+	XP SP3	XP SP3	XP SP2	XP SP2
	RDC 7.0	RDC 7.0	RDC 6.1	RDC 7.0	RDC 6.1	RDC 6.1	RDC 5.2
Távoli Asztal elérés	igen	igen	igen	igen	igen	igen	igen
RemoteApp elérés	igen	igen	igen	igen	igen	igen	**nem**
Saját desktop elérés a Connection Broker-en keresztül	igen	igen	igen	igen	igen	igen	igen
Közös desktop elérés a Connection Broker-en keresztül	igen	igen	igen	igen	igen	igen	igen
RemoteApp használat, virtuális asztal elérés és szimpla terminálkapcsolat közvetlenül az OS-ből	**igen**	nem	nem	nem	nem	nem	nem
RemoteApp használat, virtuális asztal elérés és szimpla terminálkapcsolat a Web Access-ből	igen	igen	igen	igen	igen	igen	nem
Státusz (és szétkapcsolás) tálca ikon	**igen**	**igen**	nem	nem	nem	nem	nem

8.11 ÁBRA A 7.1-ES (W7/R2 SP1) LEMARADT, DE ÚGYIS CSAK EGY DOLOG LENNE BENNE: A REMOTEFX



8.12 ÁBRA INDÍTSUNK EGY MSTSC-T, ÉS KATT AZ ABOUT-RA AZ ABLAKVEZÉRLŐ GOMBON

Szóval az Easy Print bármilyen RDP kapcsolat esetén (RemoteApp, Web Access is) lehetővé teszi, hogy a kliens a saját - *bármilyen* típusú - nyomtatóját minden további beállítás és egyéni meghajtó program telepítés nélkül használhassa. Aki küszködött már a 20 Ft-os printerek 64 bites, szerverre passzoló driverével, vagy akinél az erővel belehegesztett, elvileg univerzális driver nap mint nap kék halálba menekült, az nagyon fogja ezt a lehetőséget értékelni. A technológia mélyebb részleteitől megkímélném itt az olvasót[120], de a kulcsszavak az XPS formátum, a GDI konverzió és a .NET Framework, bár az utóbbi már nem lényeges a W7/R2 páros esetén (előtte viszont az Easy Print sikertelen működésének az oka 90%-ban a hiánya vagy a rossz verziója volt).

Azt viszont még jó ha tudjuk, hogy a rendelkezésre álló Csoportházirend opciók a finomhangolást segítik, ugyanis ezekkel tudjuk először is engedélyezni ezt az opciót elsődleges módszerként, illetve óvatosságból azt is megszabhatjuk, hogy csak a kliensen lévő alapértelmezett printert használhassuk automatikusan.

Nos, miután egészen jól kivégeztük az RDSH-t, haladjunk tovább még újabb és még izgalmasabb területekre!

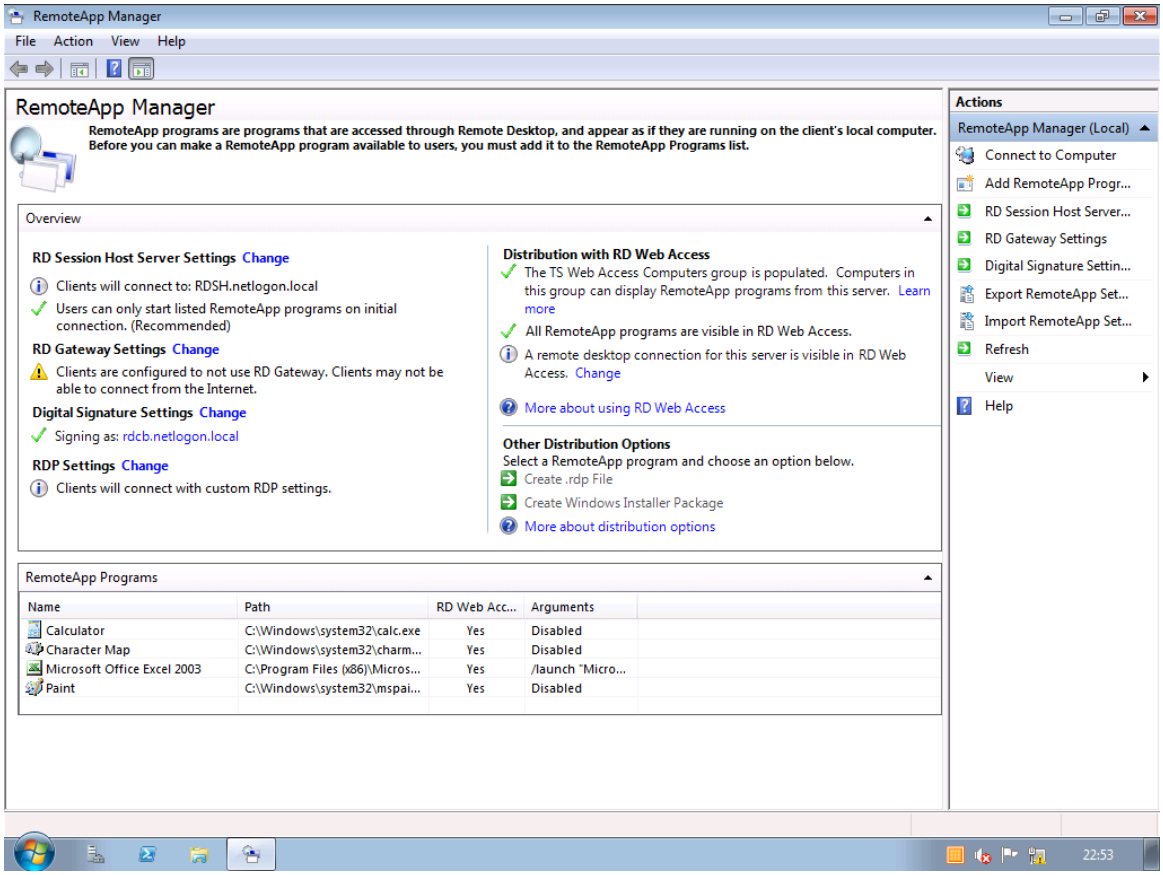
8.2 RemoteApp

A RemoteApp komponenssel könnyedén és látványosan megoldhatjuk a terminálkliensek alkalmazás „ellátását" és használatát. A klasszikus felállás szerint a vékony kliensről - szemmel is látható módon - egy RDP kapcsolatot kell kiépítenünk, majd az adott kapcsolaton (ablakon) belül futtatják a felhasználók a számukra engedélyezett alkalmazásokat.

Ezzel viszont van egy komoly probléma.

Egyrészt nincs szükség arra, hogy az egész szerver desktopot (Asztal, Start menü, stb.) is lássák, mivel tipikusan az alkalmazások miatt használunk egy RDS szervert, és nem a környezet miatt. Másrészt biztonsági és erőforrás okok miatt is jobb lenne, ha nem kellene betölteni mindent a munkamenetbe. Harmadrészt rengeteg dolgot tiltania kell az üzemeltetőknek, ha olyan környezetet akarnak, ami sokáig bírni fogja – ugye tudjuk, hogy a felhasználók iszonyú kreatívak is tudnak lenni a problémagyártásban persze, nem a megoldásban ☺. Szóval egy egyszerűbb, biztonságosabb és üzembiztosabb módszerre lenne szükség. Nos, ez a RemoteApp.

[120] De azért egy remek olvasnivaló házi feladatot adok: http://blogs.msdn.com/b/rds/archive/2009/09/28/using-remote-desktop-easy-print-in-windows-7-and-windows-server-2008-r2.aspx



8.13 ÁBRA A REMOTEAPP MANAGER

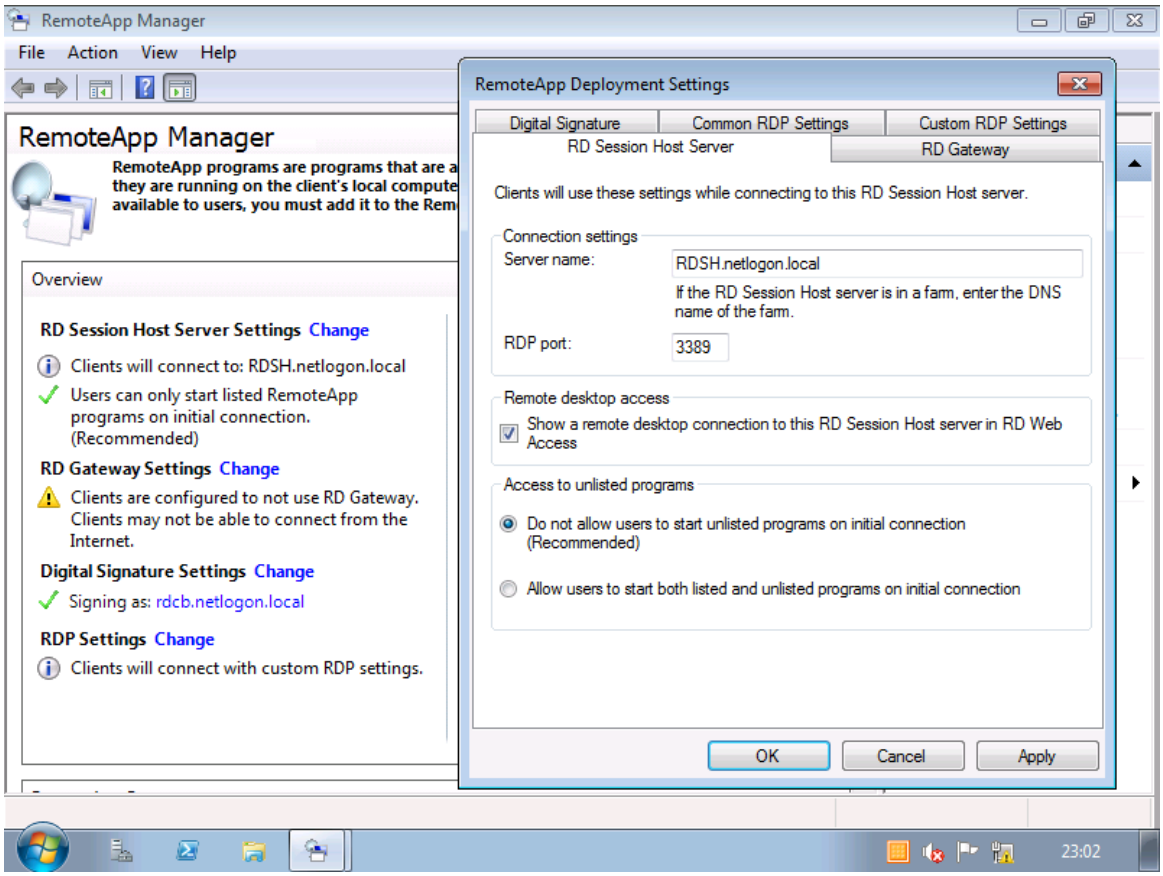
Az új módszer szerint az üzemeltető egy a RemoteApp Manager-ben végzett előkészítés után (több publikálási módszer közül választva) parancsikon(ok)at helyez el a felhasználó gépén (a Windows 7-ben még egyszerűbb), amelyekre kattintva az alkalmazás egy RDP kapcsolatot kezdeményez a háttérben. Ennek hatására elindul a kiszolgálón az adott program, amit a felhasználó úgy vesz észre, hogy az alkalmazás rögvest megjelenik a gépén, tökéletes helyi programnak „álcázva" magát. Ha a gép/felhasználó számára több RDS alkalmazást publikálunk ezzel a módszerrel, akkor a már élő RDP kapcsolaton testvériesen megosztoznak majd az alkalmazások, tehát nem a kapcsolatok száma nő. Nem tudom, hogy ezt hogyan tudjuk elképzelni, amíg nem látjuk, mindenesetre rengeteg screencast-tal rendelkezünk a TechNetKlub TV-n többek között e témában is[121].

Nézzük meg most dióhéjban, az üzemeltető oldaláról a teendőket (feltételezve, hogy a publikálandó programok telepítésén már túl vagyunk), de szögezzük le még az elején, hogy a RemoteApp miatt újra át kell futnunk a 8.11 ábrát:

1) A RemoteApp Manager konfigurálása.

121 https://technetklub.hu/tv/Default.aspx?auth=0&sid=21ec0497-3159-4f96-ae7b-352a48dd1692

2) Az adott program terminál programmá "avatása" varázslóval (előredefiniált listát kapunk, amelyet persze tetszés szerint bővíthetünk).
3) Az adott program terminál programként való működésének engedélyezése.
4) Egy .rdp vagy .msi csomag elkészítése a kijelölt alkalmazás(ok)ból szintén varázslóval, pár egyszerű lépésben.
5) A csomagok publikálása a felhasználók számára (parancsikonok kiszórása, megosztott mappa, .msi telepítés a Csoportházirenddel, vagy más disztribúciós szoftverrel, stb.).

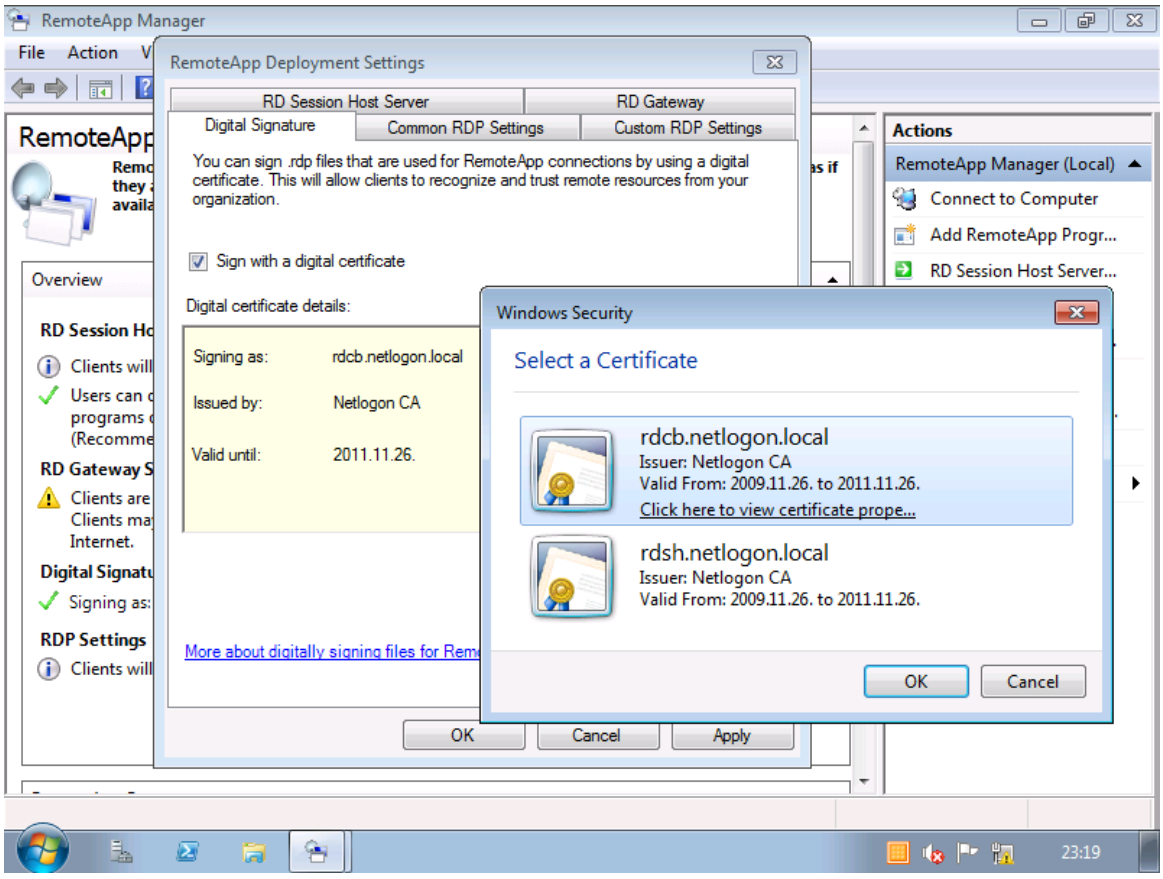


8.14 ÁBRA A REMOTEAPP MANAGER

Az első ponthoz a munkát kezdjük a RemoteApp Managerben, és célszerűen a bal felső sarokban, az RDSH Server Settings alatti „Change” hivatkozásra kattintva. Ezzel megint egy trükkös beállító panelt kapunk, hiszen a fülek majdnem az egész RemoteApp Manager konfigurálását elérhetővé teszik ☺, de nem baj, haladjunk!

Az RDSH Server fülön alapdolgokat állítunk be, leszámítva talán az „Access to unlisted programs” részt, ahol egész egyszerűen megtiltható,hogy a felhasználó számára nem engedélyezett, de publikált alkalmazások láthatóvá váljanak, pl. a Web Access alatt. Az RD Gateway fül alatti beállítások csak akkor szükségesek, ha valóban az RD Gateway-on keresztül érkeznek a kliensek, és akkor ennek a beállításait (név, hitelesítés, stb.) bele kell hegeszteni az alkalmazás .rdp, vagy .msi fájljába. A „Digital

Signatures" fül alatt képesek leszünk aláírni az alkalmazásokat a szerver tanúsítványával, ez pl. az SSO-nál (Single-Sign On, egyszeri/egyszerű bejelentkezés) vagy az eszközátirányításoknál nagyon fontos lesz.

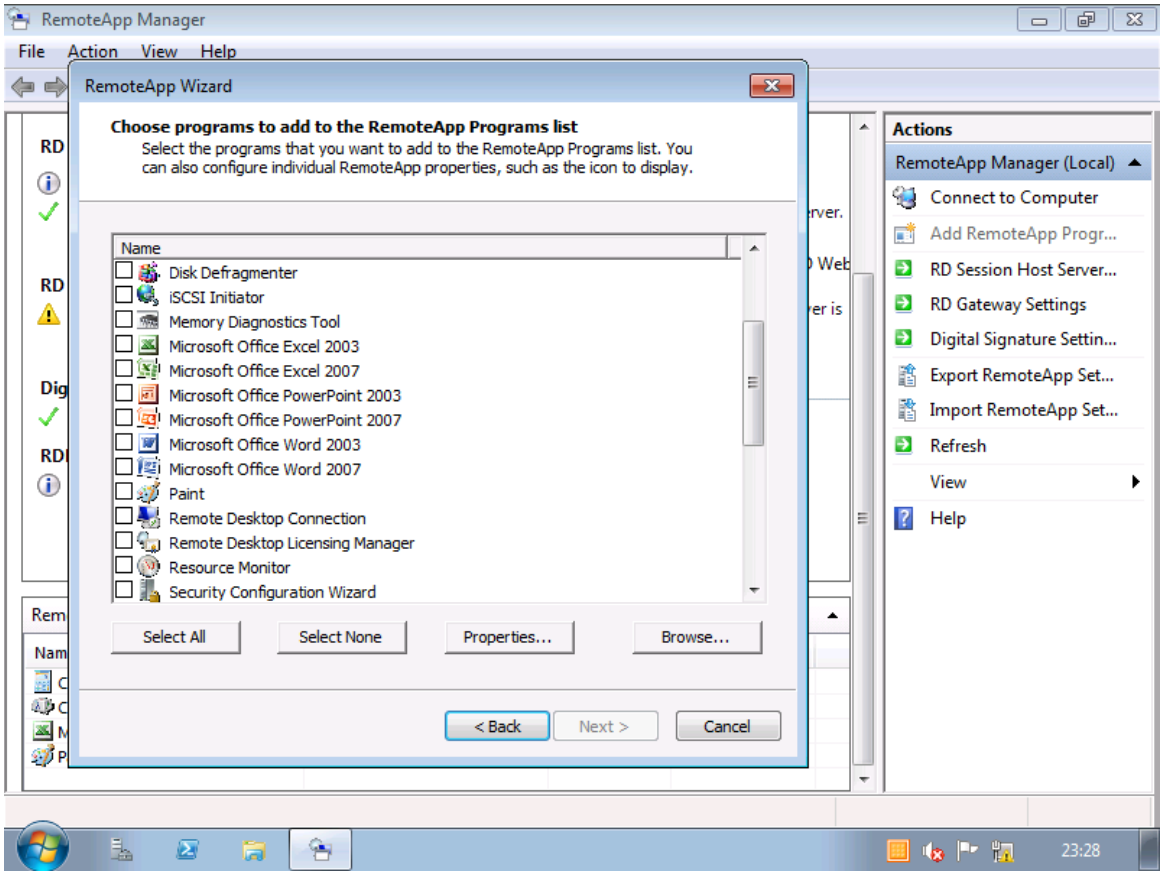


8.15 ÁBRA KÉSŐBB MAJD KIDERÜL, HOGY MIÉRT IS NEM AZ RDSH TANÚSÍTVÁNYÁT HASZNÁLOM...

A Common és a Custom Settings alatt a kliensek működését közvetlenül befolyásoló beállításokat tehetünk meg, az elsőnél kattintgatva választva, a másodiknál pedig gyakorlatilag direktben kopizva szerkesztgetünk. Ez utóbbi borzasztóan fontos lesz, ha olyan beállítást óhajtunk tenni, ami nincs kivezetve sehol sem a grafikus felületre, de mégis szükség lenne rá. Alkalmazási példákat egyrészt vehetünk egy .rdp fájlból, amit akár egy Notepad-dal is megnyithatunk, de ez a lista[122] is nagyon kellemes.

No, most már hozzá is kezdhetünk a 2. ponthoz, azaz egy RemoteApp alkalmazás publikálásához: Action Pane > Add RemoteApp Program.

[122] http://technet.microsoft.com/en-us/library/ff393699%28WS.10%29.aspx



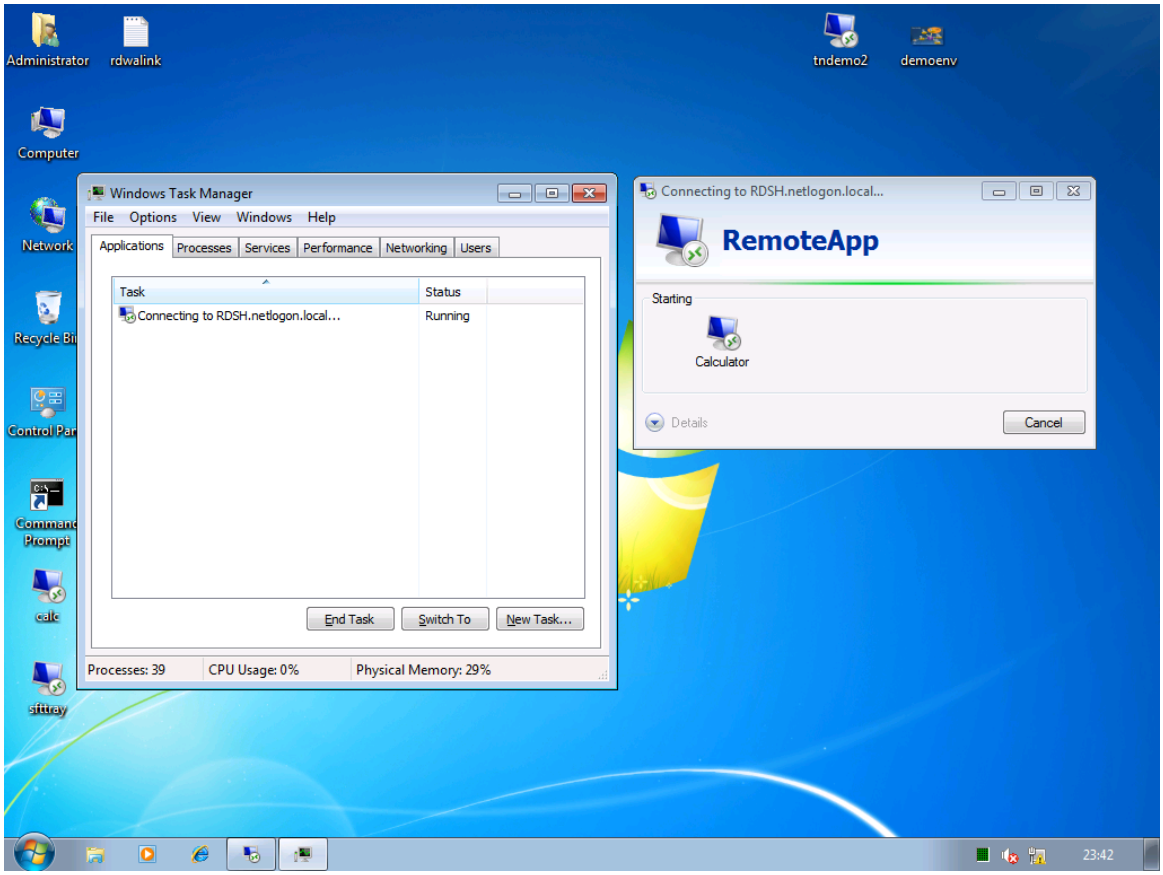
8.16 ÁBRA VÁLASSZUNK ALKALMAZÁST!

Ha megvan az alkalmazás, akkor a „Properties” alatt extra opciókat is beállíthatunk, pl. azt, hogy majd elérhessük-e a Web Access-ből is, meg azt, hogy legyen-e valamely parancssori argumentuma, vagy – és ez nagyon fontos is lehet – „a User Assigment” alatt szűkíthetjük a jogosultsági kört. Ha ezt megtesszük, akkor a felhasználó tényleg csak azt látja, amit szabad.

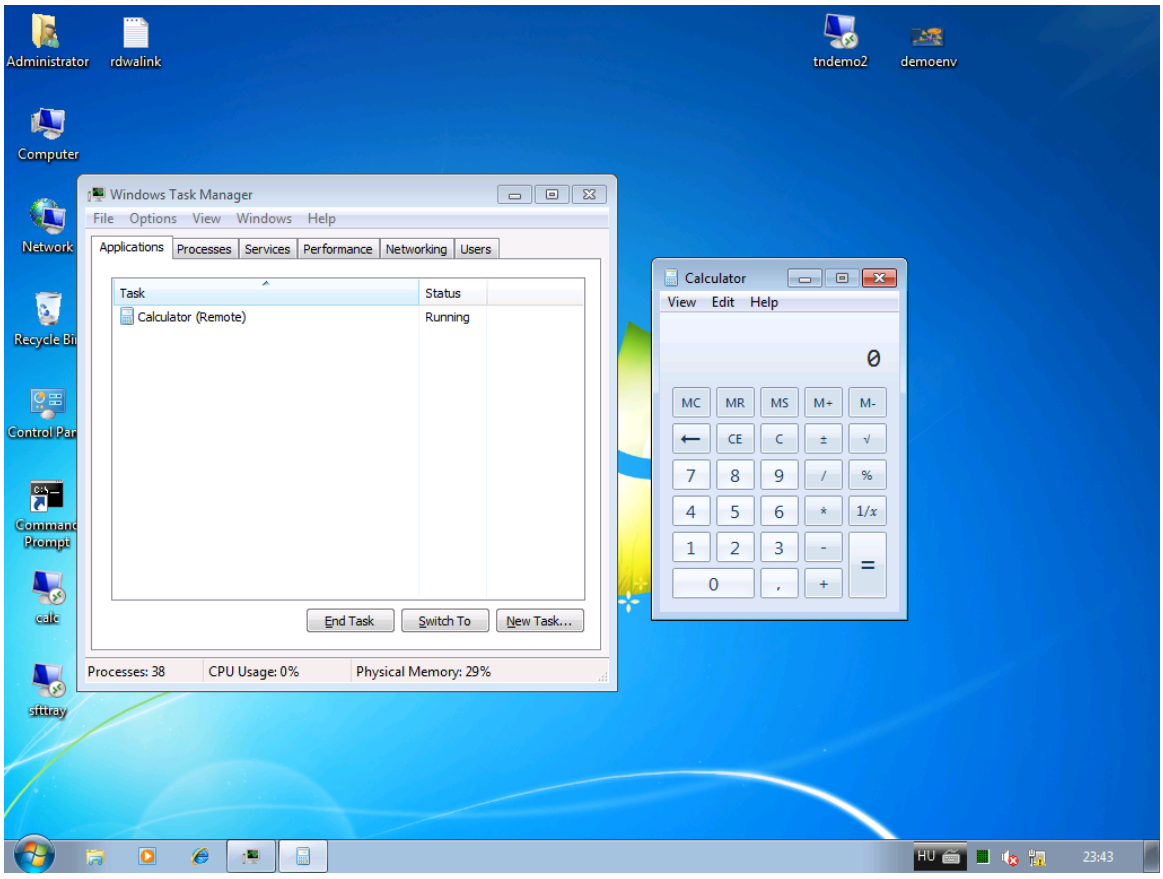
Ha végigverekedtük magunkat a varázslón, akkor a lenti listában viszontláthatjuk az imént engedélyezett alkalmazásunkat és a rá jellemző részleteket. Innen rögvest indíthatjuk is a publikálást (helyi menü > Create .rdp File, vagy Create Windows Installer Package). A különbség a kettő között:

a) .rdp fájl: egyszerűen másolható, de nincs fájltársítás és egy fokkal komplikáltabb szétszórni
b) .msi fájl: alapértelmezésben működik a társítás, és akár egy Csoportházirenddel is kiszórhatjuk, beállítható hogy hova kerüljön (Desktop, Start menü), viszont így vagy úgy, de telepíteni kell

Ha eldöntöttük, akkor még ezt is testre szabhatjuk (szerver cím, RDG, tanúsítvány), és még egyebeket is találunk az .msi-nél, és aztán készen is vagyunk. Innentől már csak el kell juttatni valahogyan a kliensre, és működik is.



8.17 ÁBRA KAPCSOLÓDIK...



8.17 ÁBRA ...ÉS MÁR FUT IS, ÉS CSAK A TASK MANAGERBŐL DERÜL KI, HOGY NEM IS HELYBEN

És akkor most, hogy megvolt a RemoteApp alapozás, bővítsük ki az élményt egy másfajta publikálási módszerrel és az ezen alapuló kliensoldali extrákkal!

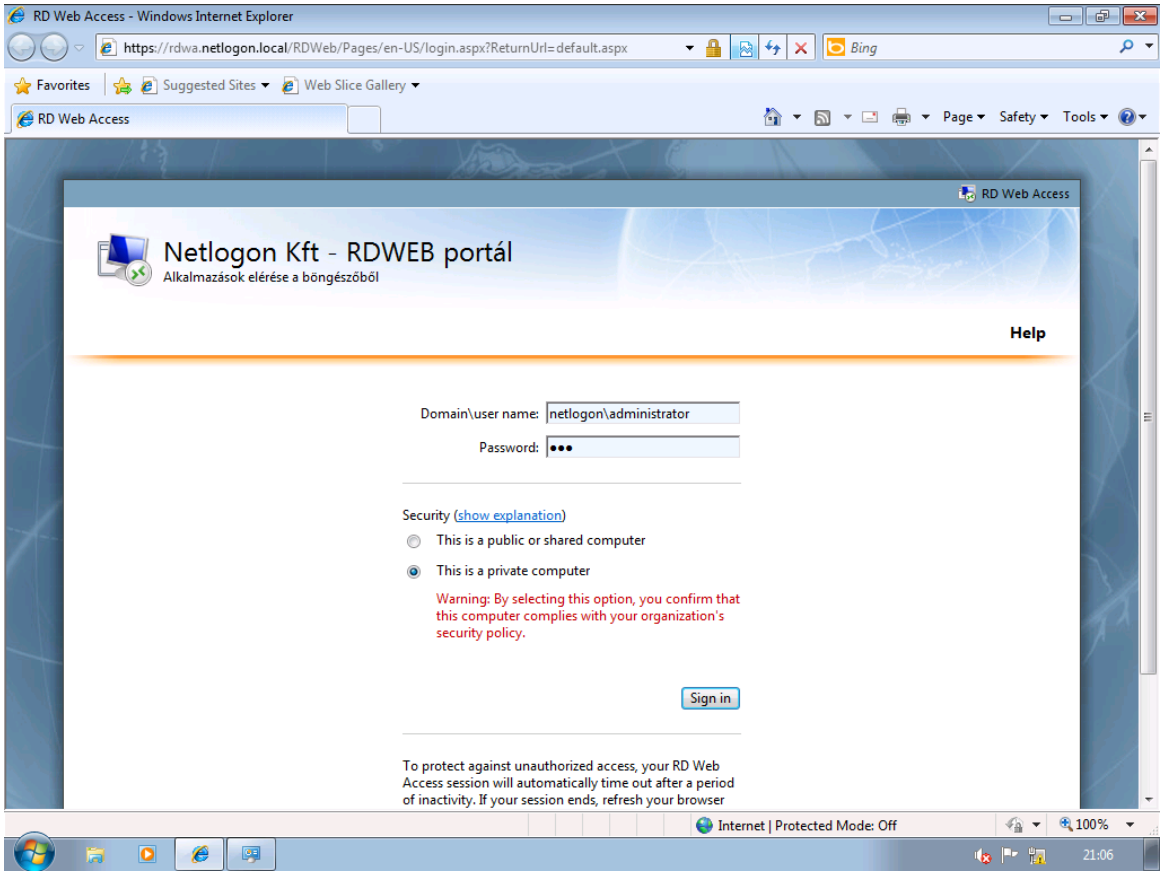
8.3 Web Access

A recept: végy egy IIS-t, tegyél bele űrlap alapú hitelesítést, tanúsítványt, és mondd meg az RDSH-nak, hogy igen, akarjuk a RemoteApp-okat a böngészőből is elérni, és kész a Web Access.

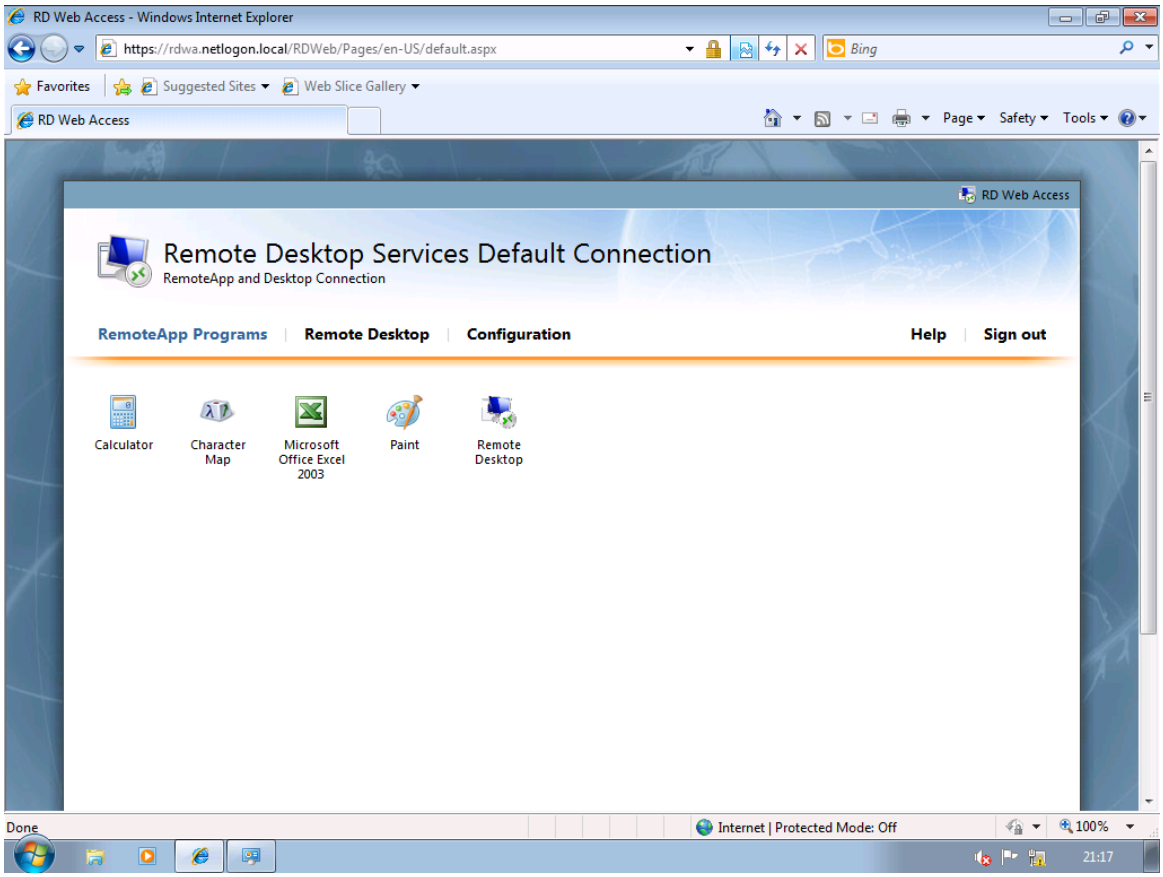
Gyakorlatilag még ennél is egyszerűbb az implementáció, ugyanis azzal, hogy feltelepítjük a komponensek közül (8.2 ábra) a Web Access-t, az első kettő feladatot meg is oldottuk. A kezdő konfigurálásnál még arra kell ügyelnünk, hogy a RemoteApp Manager-ben a jobb felső sarokban *kizöldüljön* a pipa („Distribution with RD Web Access"), amit úgy érhetünk el, hogy az RDSH szerveren a TS Web Access Computers helyi biztonsági csoportba berakjuk az RDWA szerepet betöltő számítógép fiókját (ami egy másik gép is lehet, mert lehet, hogy szeparálunk, azaz elválasztjuk a két komponenst egymástól).

Ezek után az alkalmazásoknak kell megengednünk, hogy látszódjanak a WA alatt, majd az RDWA gépen egy klasszikus szerver tanúsítványt kell belepakolni az IIS alá, és készen is vagyunk.

Ami még hátravan, az az RDWA „rágyógyítása" az RDSH-ra, amit az RDWA gépen a „Remote Desktop Web Access Configuration" ikonon keresztül tudunk beállítani. Ez elindítja a böngészőt az RDWeb oldallal, és így a belépés és a „Configuration" pont kiválasztása után írjuk be az RDSH szerverünk nevét (lásd később, kicsit előreszaladva a 8.26 ábrán).



8.18 ÁBRA AZ RDWEB PORTÁLUNK KÍVÜLRŐL...



8.19 ÁBRA ... ÉS BELÜLRŐL.

De azért értsünk meg egy pár dolgot:

- Az RDWA önállóan, önmagában nem nyújt kapcsolatot, egyszerűbb esetben egy darab RDSH, komplexebb környezetben egy RDSH farm vagy egy RD Connection Broker kell hozzá.
- Űrlap alapú hitelesítéssel dolgozik, ami többek között SSO-t is képes nyújtani, de csak a RemoteApp esetén, és ehhez már a Connection Broker és egy közös tanúsítvány kell, valamint egy megfelelő verziójú RDP kliens (7.0 vagy újabb).
- Központi publikációs üzemmódban is tud dolgozni, ha van a kapcsolati láncban egy az RDWA-t irányító Connection Broker, ami a több RDSH szervert, VDI kapcsolatot és a feed elérést is megoldja, és ilyenkor az RDWA lesz az, ahol minden lehetőséget egyben látunk (később ehhez majd lesz infó és kép is).

Ha jól megnézzük a 8.18-as ábrát, és esetleg azt, amit mi összehoztunk a leírás alapján, akkor rögvest észrevehetjük, hogy én már némiképp testreszabtam a portált, igaz, csak a külső oldalt, de akkor is. Nos ez is egész jól megoldható, de először is essen szó a magyarításról: a szokásos módon kell a nyelvi csomagot felpakolni a szerverre, azaz be kell szerezni a csomagot, majd a Control Panel / Regional Settings alatt hozzá kell adnunk, majd átváltani erre, és akkor az RDWEB is magyarul lesz.

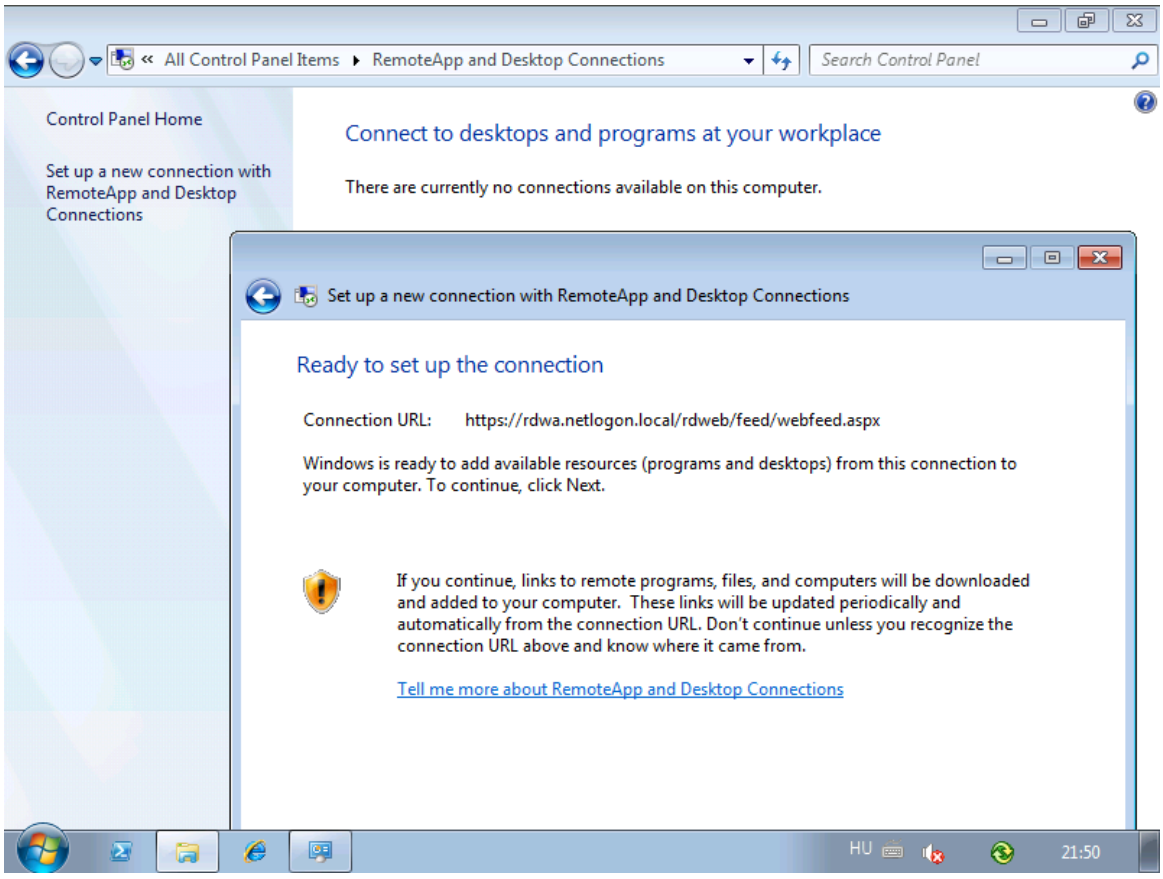
De a portál feliratait is átírhatjuk a saját elnevezéseinkre, amit én műveltem, azt például a %windir%\Web\RDWeb\Pages\en-US mappában lévő login.aspx-ben (én az angolt használom, ha magyarítottunk, akkor a hu-HU mappában tallózgassunk). De megszabhatjuk azt is, hogy a belépési űrlapon melyik profil legyen az alapértelmezett (pl. mindig a privát, ez célszerű, mert különben lesz felugró figyelmeztető panel az alkalmazások indításakor), vagy hogy ne is legyen választás, vagy éppen eltüntethető a portálon belül a „Remote Desktop” tab (a Configuration amúgy is csak az adminoknál jelenik meg), és egyebek. Ezek nem hivatalos, ajánlott módszerek, hanem tipikusan .aspx fájlok átírogatása, de működik, az tuti.[123]

> Vagy például az Integrated hitelesítés is elérhető (és így az űrlapra sem lesz szükség), ugyanis egy tartományon belül a tartományi felhasználónév/jelszó párossal automatikusan a böngésző (az IE biztosan) a háttérben hitelesít majd, ami elsősorban a felhasználónak kellemes, mert nincs gépelgetés. Viszont ehhez sajna nem elég az IIS virtuális mappájában kattintgatni, szintén trükközni kell (és OS limit is van, pl. az XP-vel nem is járható ez az út), de szintén megtalálható a megfelelő leírás a felhőben.

Van viszont egy hivatalos, támogatott, ellenben csak a Windows 7-re alkalmazható extra lehetőségünk is, mégpedig a Control Panelba építve. Ezt úgy hívják, hogy „RemoteApp and Desktop Connections”. A lényege, az hogy ha csatlakozunk az

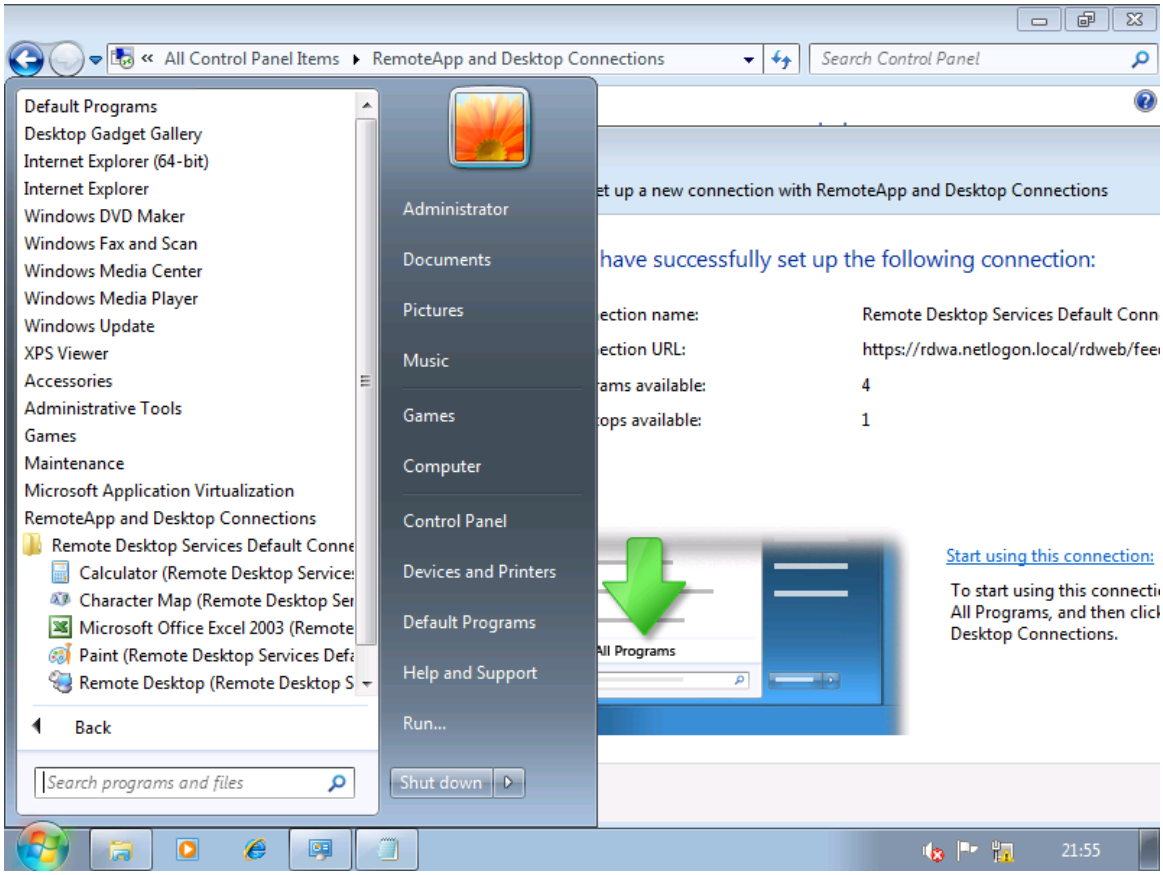
[123] Nem is adok hivatkozásokat, de bárki megtalálja.

RDWA szerverhez egy feed[124] beírásával, akkor egy az egyben letölti a Start menübe az összes RemoteApp-ot, ergo nincs .rdp és .msi terítés, egyből megvagyunk, a felhasználó számára mindez meg teljesen transzparens.



8.20 ÁBRA OLVASSUK LE A PÉLDÁT!

[124] Én nem tudom, hogy ez magyarul hogy van, de nem is akarom tudni :D



8.21 ÁBRA BEVITTÜK A FEED-ET, ERGO NÉZZÜK MEG A START MENÜT

Ha valaki érti a mechanizmust és nagyvállalati szemlélete van, akkor rögtön meg fogja magában kérdezni: és több RDWA szervert használhatunk? Hát persze, sőt a felhasználó ebből sem fog észrevenni semmit a webes felületen, de ez már a következő alfejezet témája, megérkeztünk a sorban következő elemhez, ami a Connection Broker.

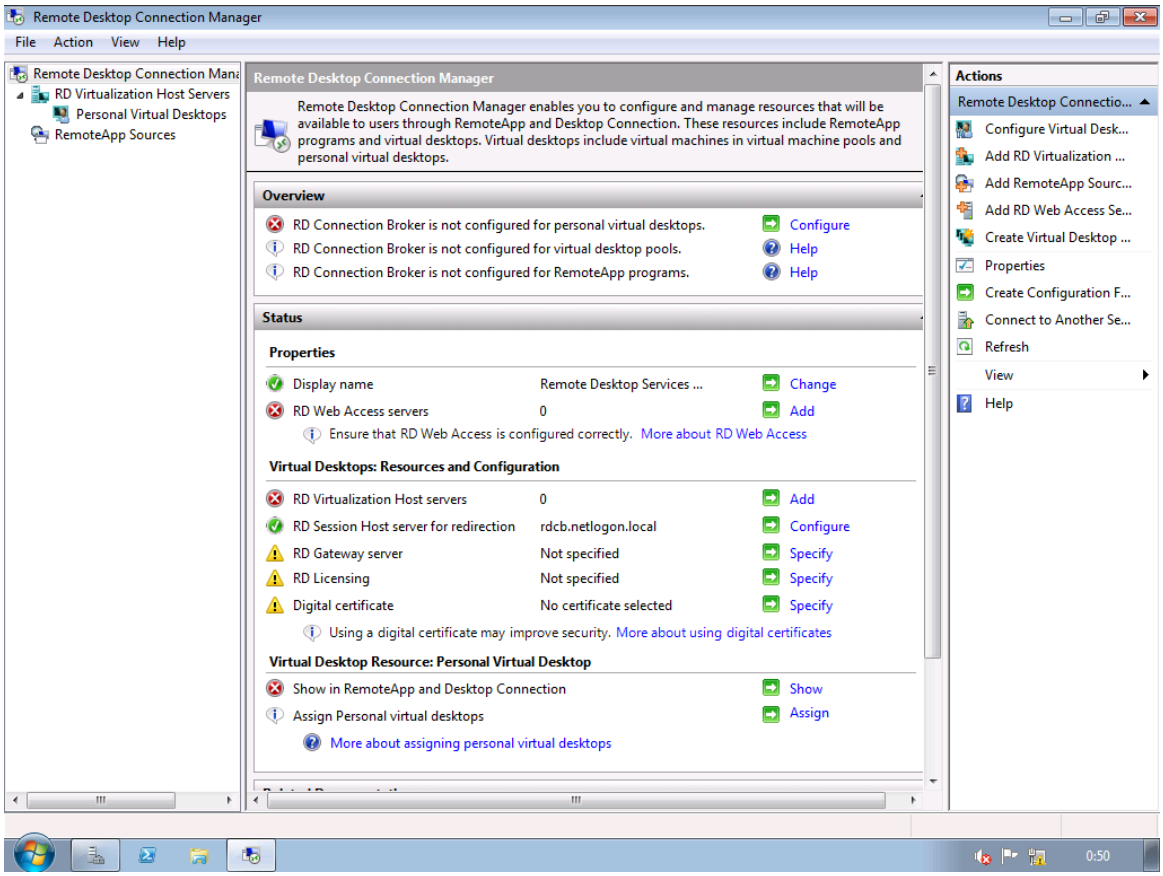
8.4 CONNECTION BROKER

Ez itt kérem a Kánaán, és az RDCB a Főnök. Ide fut be minden kérés, és innen fut ki minden utasítás, kezeli a szóló RDSH gépeket, az RDSH farmokat, az RDWA gépet, mindkét típusú virtuális gépet az RDVH komponensen keresztül, és még folytathatnám - de egyébként mindez már a 8.1-es ábra hatágú kék nyílsorozatából is kiderül. Az viszont nem, hogy az RDCB gyakorlatilag két rendszerszolgáltatásból áll:

- Connection Broker (tssdis)
  - Minden RDS és RDVH kapcsolathoz
  - Minden session információt tárol > a szétkapcsolt session folytatása > CB
- Centralized Publishing (tscpubrpc)
  - RemoteApp és Desktop Management Service
  - A személyes virtuális gépekhez is ez kell majd

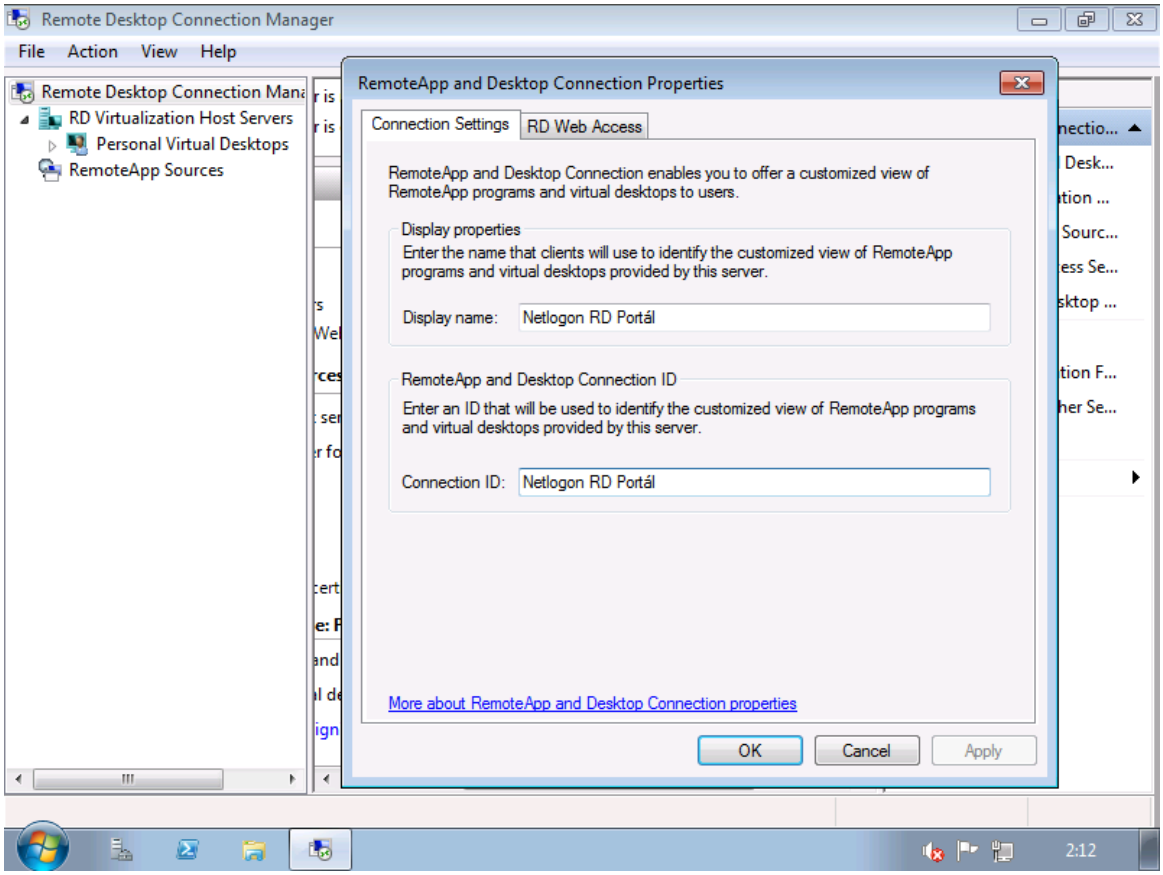
És a legszebb, hogy nem is nagyon bonyolult összerakni – bár lehet, hogy ez nagyon bátor kijelentés. Már sokszor emlegettem (és persze a VDI-nál is visszatérek majd hozzá, mivel tényleg nem lehet kikerülni egyetlen RDS összetevő apropóján sem), de az építés során fogjuk megismerni igazán.

Kezdjünk is hozzá! A feladat az, hogy alapszinten beállítsuk az RDCB-t, illetve a két darab RDSH szerverünket plusz az egyetlen RDWA-t csatasorba állítsuk. Nos, indítsuk el ehhez a Remote Desktop Connection Manager-t!



8.22 ÁBRA MOST MÉG ÍGY NÉZ KI

Elsőre nem valami szép látvány, középen a sok piros kereszt és sárga háromszög, és minimális zöld pipa, de javítunk folyamatosan. Például a „Status” részben a „Display name” alatt a Windows 7-es leendő RemoteApp programcsoportot és a leendő portált egyszerűbben is elnevezhetjük, mint ahogy korábban tettük. Ugyanitt az RDWA szerverünket is bevehetjük a buliba (ez ugyanaz, mint az RDSH-nál a biztonsági csoportba pakolás).

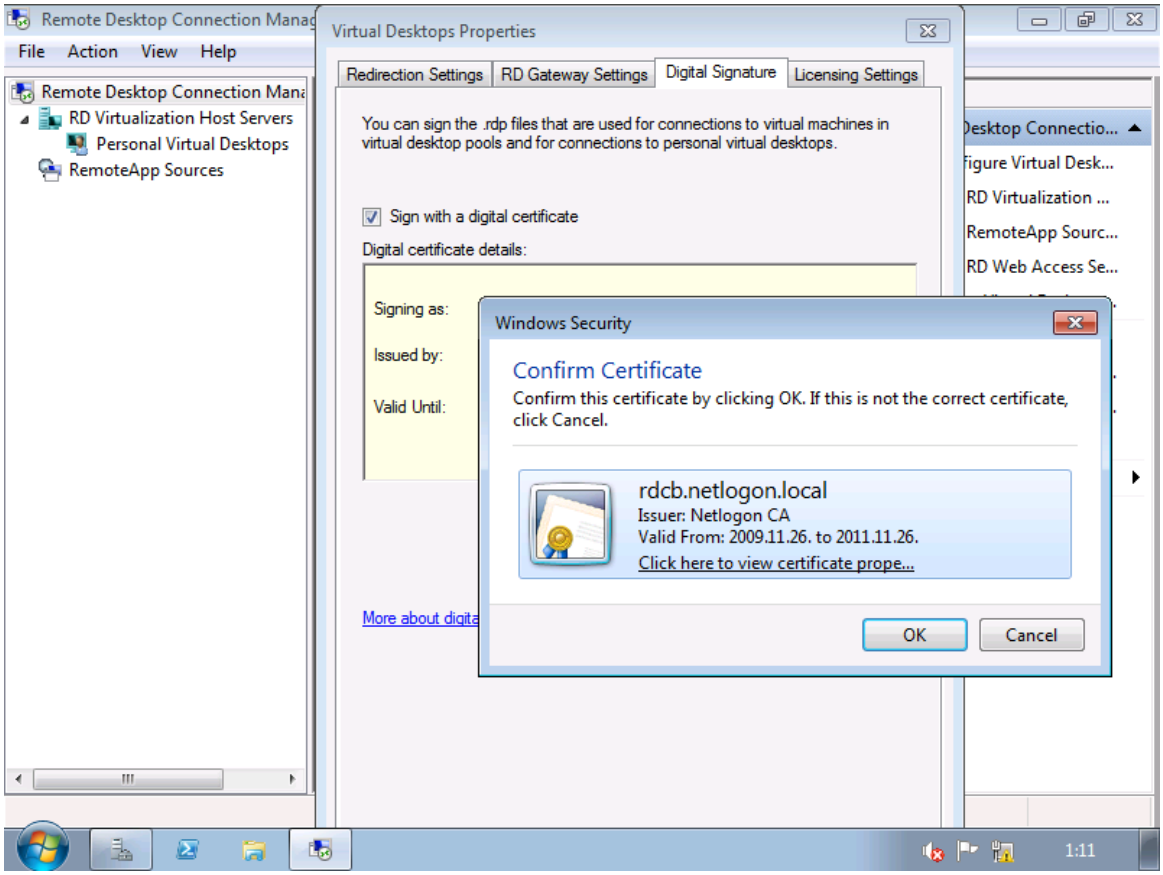


8.23 ÁBRA KEZDJÜK A NEVEKNÉL ÉS AZ AZONOSÍTÓKNÁL

Egyébként, rögtön itt és most gyalogoljunk el a két darab RDSH szerverünkre[125], és ott viszont a TSWA helyi csoportokba tegyük bele az RDWA gép helyett az RDCB-t, mivel innentől nem lesz direkt kapcsolat az RDSH-k és az RDWA között, hanem csak a RDCB-n keresztül.

Ezután haladva lefelé egy másik gyűjtőpanelbe jutunk, ha pl. az RD Gateway linkre kattintunk. Ebben először is a „Redirection Settings" fül köszön vissza, de ez még nem kell nekünk, viszont a másodikon az RD Gateway kiszolgálónkat konfigurálhatjuk, persze ilyen sincs még nekünk, viszont a harmadik fülnél a tanúsítvány beállítása általában elvárt igény.

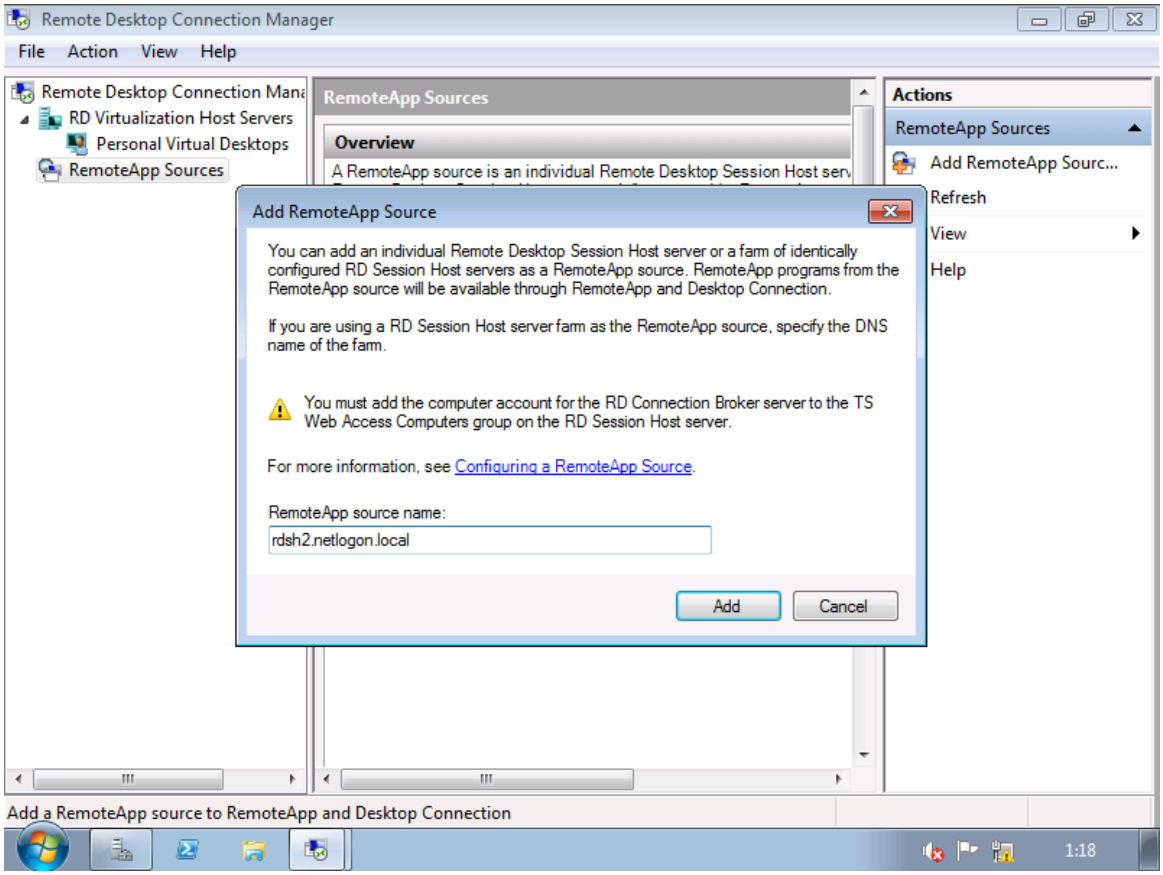
[125] A másodikról még nem volt szó, de a konfigurálás ugyanaz, kivéve, hogy nyilván más alkalmazásokat publikáltunk rajta.



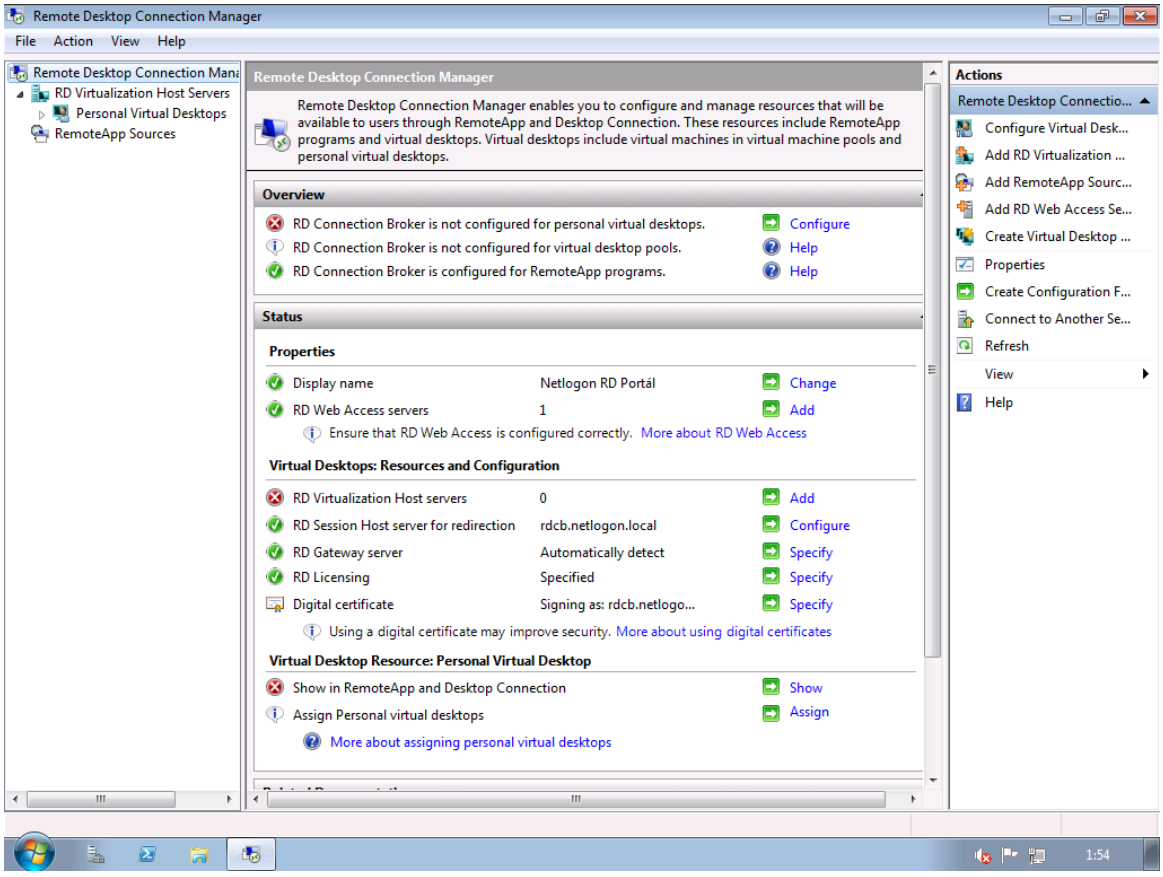
8.23 ÁBRA KEZDJÜK A NEVEKNÉL ÉS AZ AZONOSÍTÓKNÁL

Mint látható az RDCB-nek van sajátja, sőt, sétáljunk el újra a két RDSH-hoz, és ott is ezt a tanúsítványt lőjük be célszerűen, pl. az SSO miatt (erre utaltam a 8.15-es ábránál). A „Licensing Settings” magáért beszél, viszont az összes RDSH és RDWA szerverünk alapbeállítása innentől ez lesz. Ha visszatértünk az alap MMC-hez, akkor már sokkal jobban néz ki „színügyileg”, persze a VDI beállítások hiánya miatt még erősen piroslik.

No és akkor rendeljük hozzá szép sorban a két RDSH szervert az RDCB-hez, a bal oldali keretben a „RemoteApp Source” pont alól, a jobb gombos menüből!

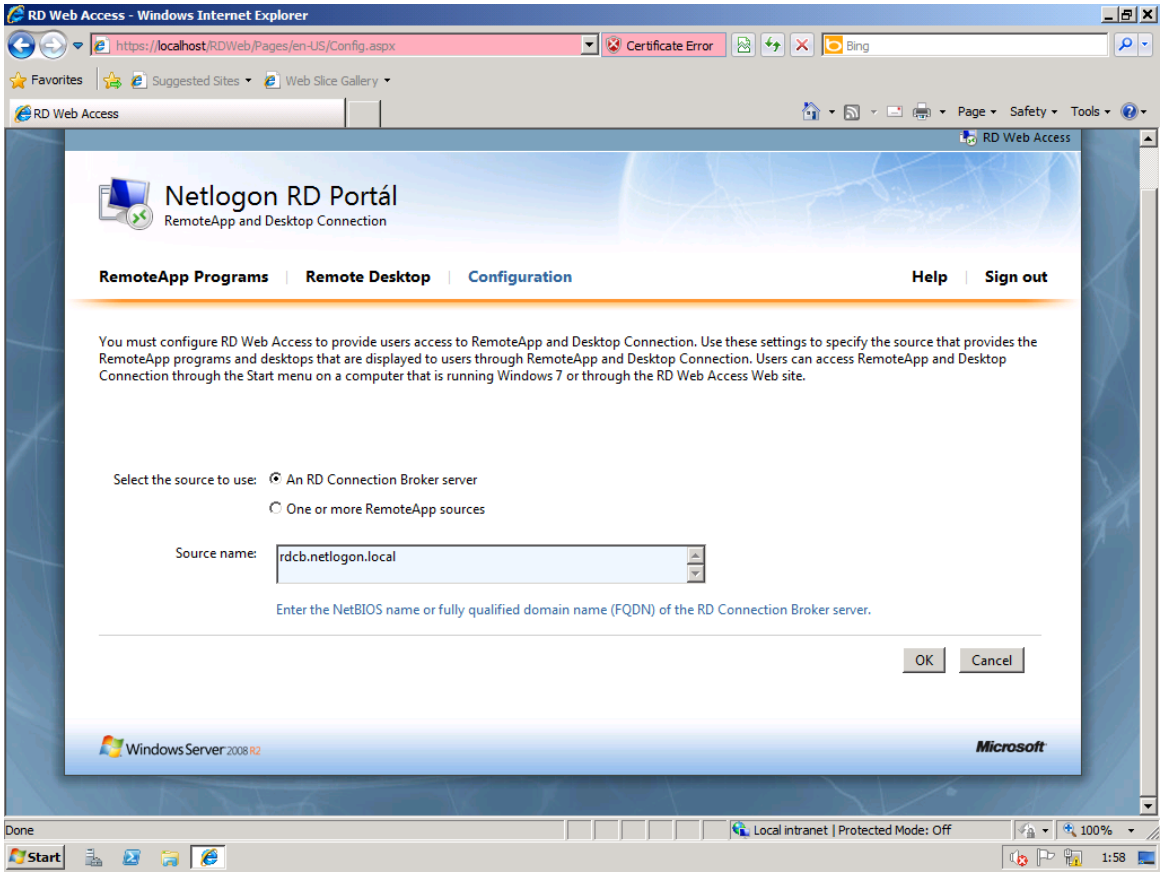


8.24 ÁBRA GYŰLNEK AZ RDSH SZERVEREK



8.25 ÁBRA A SIKER FELÉ HALADUNK

Még egy dolog hiányzik, az RDWA ráhangolása az RDCB-re, amit újra az RDWA gépen végezzünk el, mégpedig az ismerős módszerrel: „Remote Desktop Web Access Configuration” > „Configuration” > az RDSH szerver helyett megadhatjuk az RDCB címét. Ha el is fogadja, akkor biztosan jól dolgoztunk.

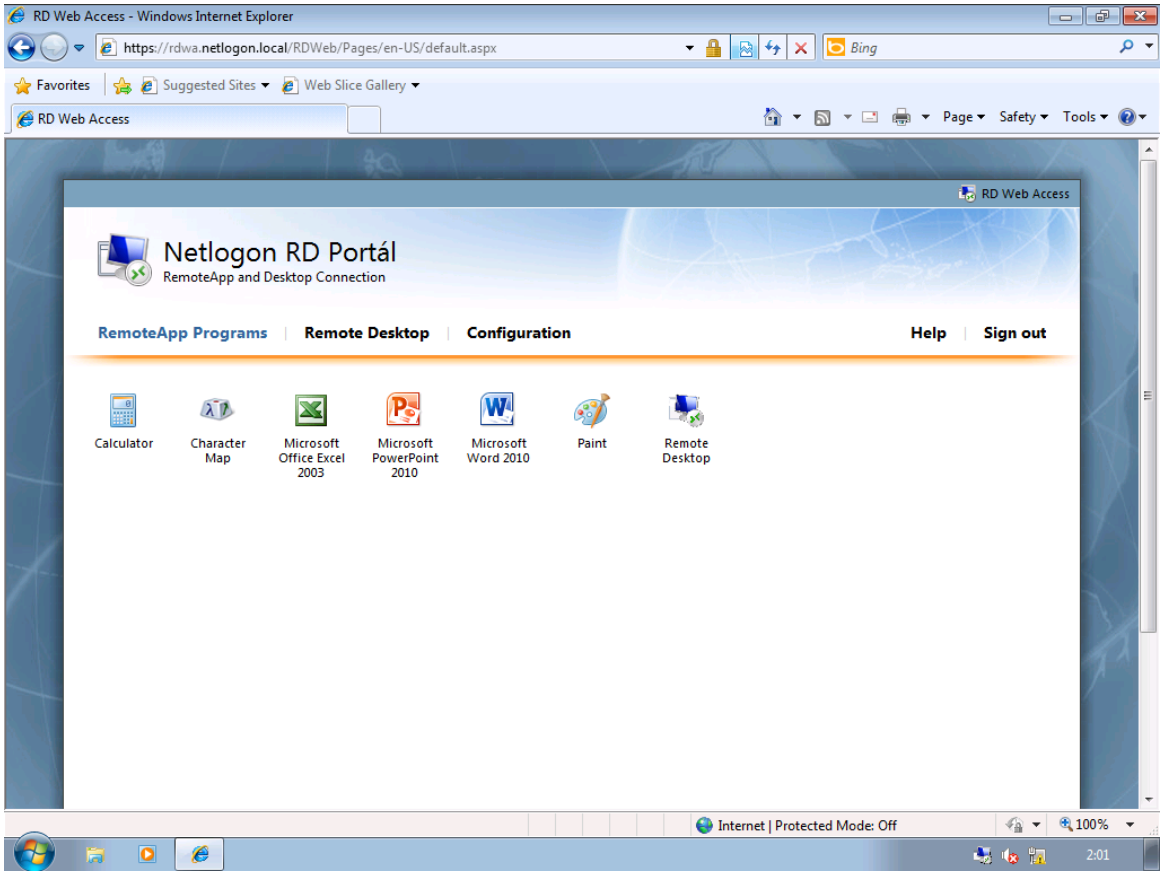


8.26 ÁBRA ÚJABB ELŐRELÉPÉS (A PORTÁL NÉVBŐL MÁR KIDERÜL VALAMI)

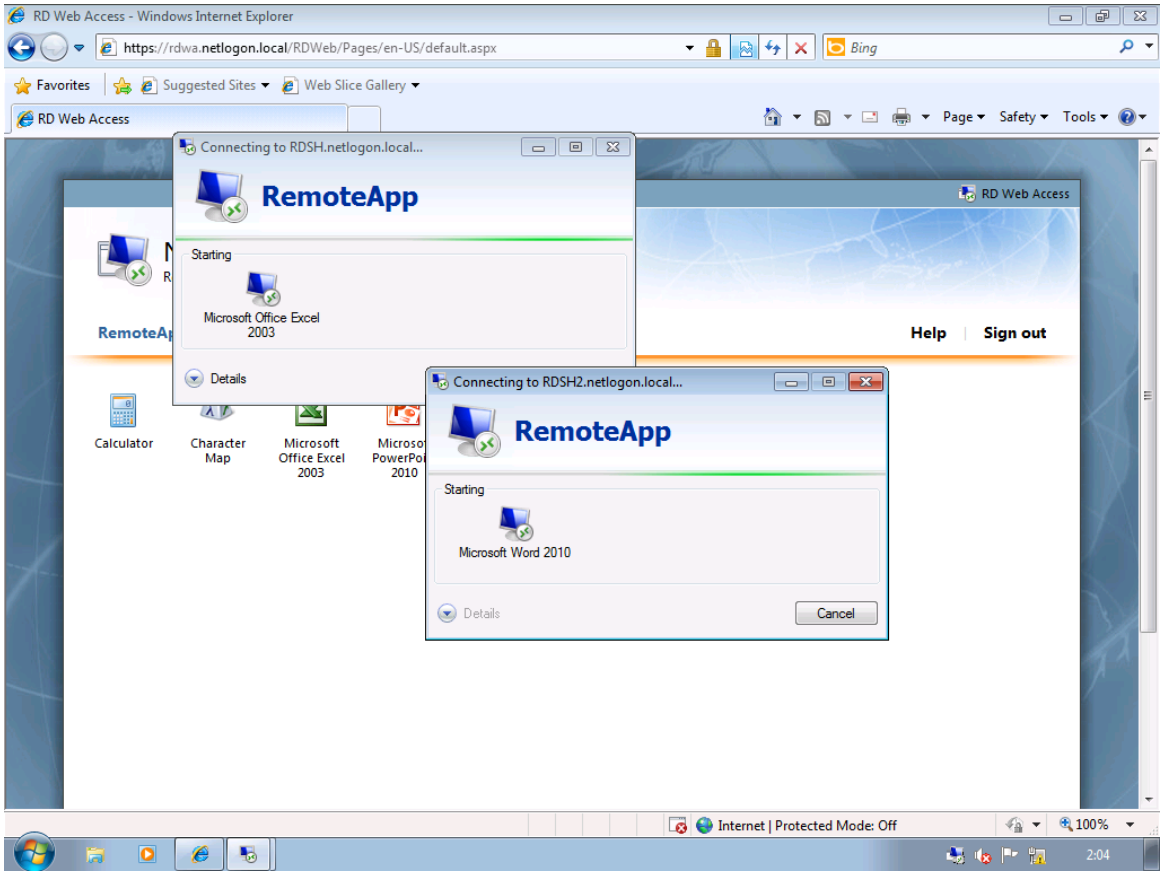
Ezután a kliensben tallózzuk be az RDWeb oldalt, a siker teljes ragyogása miatt. Ha megnézzük a következő képet, akkor a korábbi portálhoz képest van pár új ikon, pl. az Office 2010-es alkalmazások. Nos, erre is jó a két RDSH, a példában az egyikről publikáltam az Excel 2003-at, a másikról meg a 2010-es verziókat[126].

Ráadásul a felhasználó nem is veszi észre a különböző forrásokat, persze miért is venné észre, nem ez a dolga, és amúgy is természetes, hogy ilyen szintű problémákat megoldunk. Sima ügy.

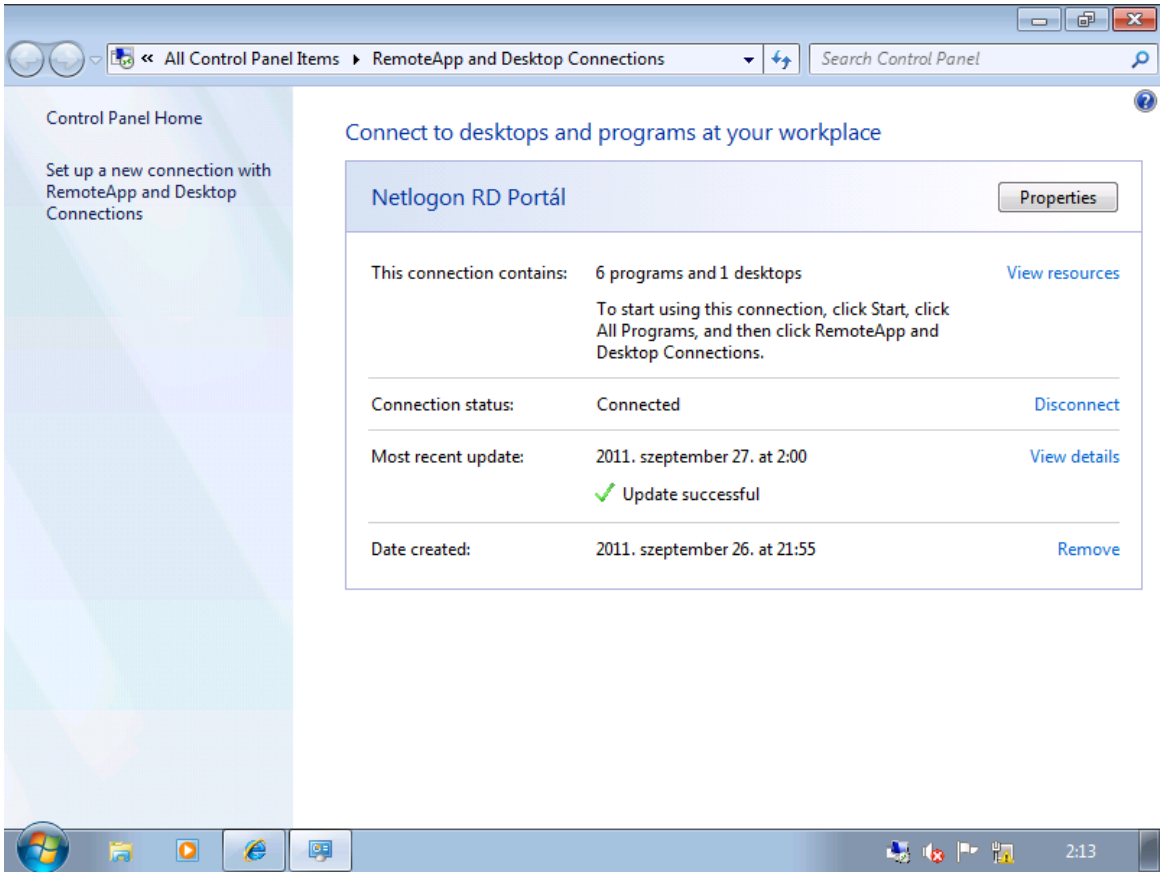
[126] Az már csak hab a tortán, hogy van a rendszeremben 2007-es Office is, plusz az egyik család App-V-vel, pontosabban App-V for RDS-sel van előkészítve.



8.27 ÁBRA NYERTÜNK



8.28 ÁBRA SASSZEMMEL ÉSZREVEHETJÜK AZ ABLAKOK FEJLÉCÉT: AZ EGYIK RDSH, A MÁSIK RDSH2.



8.29 ÁBRA EGY UTOLSÓ KÉP: A REMOTEAPP W7 CP-BE INTEGRÁLT RÉSZE, IMMÁR AZ RDCB-N KERESZTÜL

8.5 VDI

Tovább szárnyalunk.

Az R2 előtt nem volt lehetőség arra, hogy a Virtual Desktop Infrastructure (VDI) egy külső gyártó megoldása nélkül működhessen a rendszereinkben. Most már van, ergo ideje megismerkedni vele, de egyébként is ajánlom a felfedezést - annak is, aki nem akarja, vagy nem tudja bevezetni -, mert a téma nagyon érdekes és izgalmas, és működik, szépen.

> Ebben a fejezetben egy egypéldányos RD Virtualization Host környezetet építek fel, de már most megjegyzem, hogy a több RDVH-s rendszer kialakítása is hasonló módon történik, bár ebben az esetben célszerű lesz olyan felügyeleti eszközt választanunk, mint például az SCVMM (System Center Virtual Machine Manager)[127].

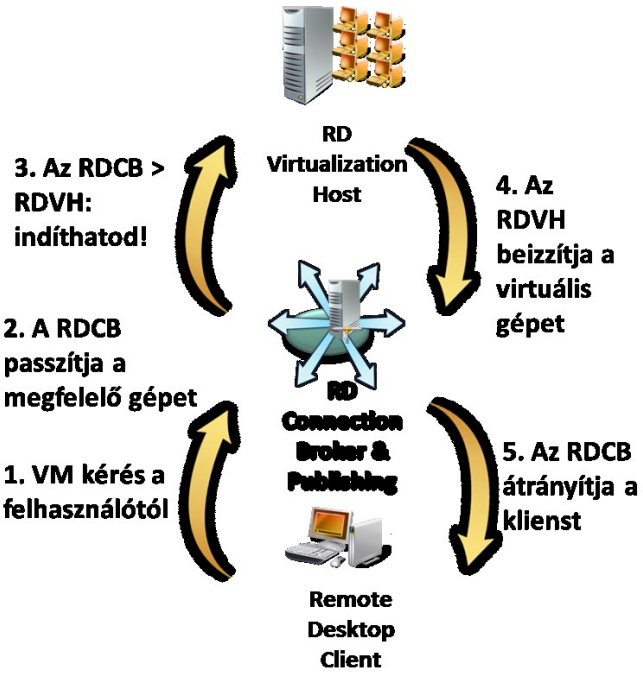
De mi is az a VDI?

127 http://www.microsoft.com/en-us/server-cloud/system-center/virtual-machine-manager.aspx

A válasz egyszerűen, teljesen a saját szavaimmal: egy olyan környezet, ahol a felhasználók a fizikai gépek helyett/mellett virtuális gépeken (is, vagy csak) dolgoznak, teljesen hétköznapi módon, és mindezt az RDS infrastruktúrán keresztül érik el.

Persze úgy, ahogy bármikor máskor, ha a virtualizáció bejön a képbe, már variálhatunk is egyből (és ez az, ami *imho* a plusz izgalmat hozza egy szakembernek [128]), így természetesen itt is, mert rögtön kétféle géptípus is létezik:

1) Minden felhasználónak van egy saját, nevesített, személyes virtuális gépe (Personal Virtual Desktop), amely csak az övé, ő eteti, akár rendszergazda jogosultságot is kaphat rajta, és persze a változásokat mentjük is a .vhd fájlba.
2) Noname, közös gépek, amelyek egy ún. pool-ban várakoznak arra, hogy valaki általános célokra és nem mentve a változásokat (azaz minden változás törlődik, vagyis inkább az eredeti állapot „visszaíródik") használja ezeket a gépeket, és tipikusan nem is emelt szintű joggal.



8.30 ÁBRA A VDI MŰKÖDÉSE, ELÉGGÉ EGYSZERŰSÍTVE

Műszakilag azért persze ennél lényegesen bonyolultabb a dolog, és ami a fontos, nem is egyetlen összetevőn múlik, hanem egy összjátékon. És van egy új elem is, ez

[128] Őszintén szólva az én esetemben nem volt ez mindig így, 6-7 éve még egyáltalán nem győzött meg a virtualizáció, és abban a mondásban találtam örömet, hogy *„…szerver az, amit nem bírok felemelni"* ☺, de hát ez már régen elmúlt, ma már elképzelhetetlen az az élet, amikor még nem volt Hyper-V, és az a fajta hihetetlen rugalmasság, amit a virtualizáció ad hozzá a lehetőségeinkhez.

az RD Virtualization Host rész-szerepkör, de a korrekt működéshez szükség van az RDWA-ra, különösen nagy szükség van az RDCB-re és az RDSH-ra, no és persze a Hyper-V-re. És akkor még a címtárszolgáltatásról nem is beszéltünk.

De merüljünk el a részletekben kicsit, tehát szükségünk lesz a következő alkotóelemekre:

- Egy publikációs felületre, ami az RDWA lesz, azaz a felhasználó a Web Access felületen látni fogja a saját virtuális gépét szimbolizáló ikont, vagy a pool-t szimbolizáló másik ikont.
- Egy kapcsolat kezelő eszközre (RDCB), ami átirányítja a kérést a megfelelő virtuális gép felé.
- Egy Redirector-ra (ez az RDSH egyik üzemmódja is lehet) hogy el tudja küldeni a felhasználótól érkező kérést az RDCB-nek. Ez a két szerep a Microsoft ajánlása szerint ugyanaz a gép, tehát egy RDSH + RDCB lesz a lelke a folyamatnak.
- Egy VM ügynökre, ami preparálja (elindítja, felébreszti, leállítja, stb.) az RDVH szerepkört futtató gépen a virtuális gépeket.
- A Hyper-V-re (együtt az RDVH-val), mint a virtuális gépeket üzemeltető eszközre.
- Az AD DS-re a személyes virtuális gépek felhasználói fiókokhoz történő hozzárendelésére és tárolására[129], mert így a felhasználó SID-je alapján történhet meg az RDWA-ban a megfelelő személyes virtuális gép ikonként történő megmutatása.

Egy felhasználó szemszögéből a hétköznapi használat viszont nem túl bonyolult, a böngészőjéből a Web Access felületen kattint a személyes gépére, vagy a pool-ra (csak egy ikonja lesz a pool-nak, hiszen elvileg teljesen mindegy, hogy melyiket kapja meg innen), a gép elindul, belép, mint egyébként és látja a desktopot, és elkezd dolgozni. Ilyenkor viszont a következő folyamatok történnek a háttérben (feltételezve, hogy most a pool-t használja, és egy új kapcsolatot indít):

1) Tehát a felhasználó a VM pool ikonra kattint, erre az ikon „mögötti” RDP fájl megnyitásával az msts.dll azonnal a Redirector-hoz fordul.
2) A Redirector azon nyomban továbbküldi a kérést az RDCB-nek.
3) Az RDCB kideríti (az msts.dll-től kapott infókötegből), hogy a felhasználó egy virtuális géphez akar kapcsolódni, és hogy ez egy a közös pool-ban lévő gép. Így aztán az RDCB aktiválja a VM bővítményét, megnézi a kapcsolatokat tartalmazó adatbázisát, mégpedig azért, hogy kiderüljön, hogy ez egy teljesen új munkamenet lesz, vagy esetleg egy szétkapcsolt.
4) Ha új kapcsolat lesz, és ha megtalálja a Hyper-V-t futtató gépet, akkor az RDCB kapcsolatba lép az RDVH-val, és megtudakolja, hogy megy-e a gép?

[129] Emiatt nem szükséges sémát bővíteni.

5) Az RDVH megrugdossa a poolban lévő egyik virtuális gépet, felkelti, ha alszik, stb., majd kideríti az IP címét.
6) Ezt a címet elküldi az RDCB-nek, ami továbbküldi a Redirector-nak, ami pedig ezt elküldi a felhasználó fizikai gépének.
7) A felhasználó gépe szépen csöndben kilép a Redirector felé menő eddigi RDP kapcsolatból, és átugrik a virtuális gépre a kapott IP alapján.

Nos, ilyen egyszerű ez.

De még nincs vége. Ha viszont arról van szó, hogy egy szétkapcsolt állapotból indul a felhasználó, akkor a folyamat a harmadik lépésig azonos, ott viszont elválik az eddig megismerttől. Mivel az az RDVH gépen lévő VM ügynök folyamatosan jelzi az RDCB-nek a virtuális gépek állapotinfóját, ezért az RDCB tudni fogja, hogy nem egy új, hanem egy szétkapcsolt esetről van szó, ezért rögtön „rájön", hogy nem kell a pool-t böngésznie, nem választhat tetszőlegesen, hanem csak azt a gépet akarjuk, amelyikkel eddig is megvolt a kapcsolat. Így a VM ügynök csak finoman rugdossa meg a gépet, hogy kiderítse, hogy bevethető-e, és ha igen, akkor máris mehet az IP cím a szokásos módon a felhasználó gépéhez.

Most viszont beszéljünk a konkrét összetevőkről, illetve mivel már van egy királyul működő RDS infrastruktúránk, csak az új elemekről! Igazából egy gépen fogunk sokat dolgozni, aztán pedig az RDCB-n véglegesítjük a konfigot (tudjuk, zöldítünk újból), majd leteszteljük.

Szóval az RDS rendszer mellé kell egy Hyper-V gép is, célszerűen ugyanabban a tartományban, és minimum két virtuális gép (csak hogy lássuk a különbséget a két típus között, de nekem azért most is 6 darab lesz a példában), és persze mind kliens lesz, mivel ezek desktopját akarjuk a felhasználónak odaadni. Vegyük úgy, hogy a Hyper-V és a virtuális gépek telepítése és beléptetése a tartományba már megoldott feladat és az RDVH komponensé is (8.2 ábra), mivel ez eléggé next-next-finish[130] művelet, képet sem érdemel.

Ezután viszont van dolog bőven, először is preparálnunk kell az összes virtuális gépet, amelyeket rabigába fogunk majd, és mindezt majdnem teljesen függetlenül attól, hogy melyik VDI típusba tartoznak majd.

A preparálás a következő műveleteket tartalmazza:

- A Remote Desktop engedélyezése és a megfelelő felhasználói csoport hozzáadása Remote Desktop Users csoporthoz
- Az RPC (Remote Procedure Call) engedélyezése

[130] A RemoteFx képesség ehhez a megoldáshoz nem követelmény, de természetesen jól jön (de ez csak az R2 SP1-gyel érkezik), lásd következő fejezet.

- Tűzfal kivételszabályok az RDS és a Remote Service Management miatt
- RDP protokoll engedélyek beállítása az RDVH számára
- RDS szerviz restartja (XP esetén a gép restartja)

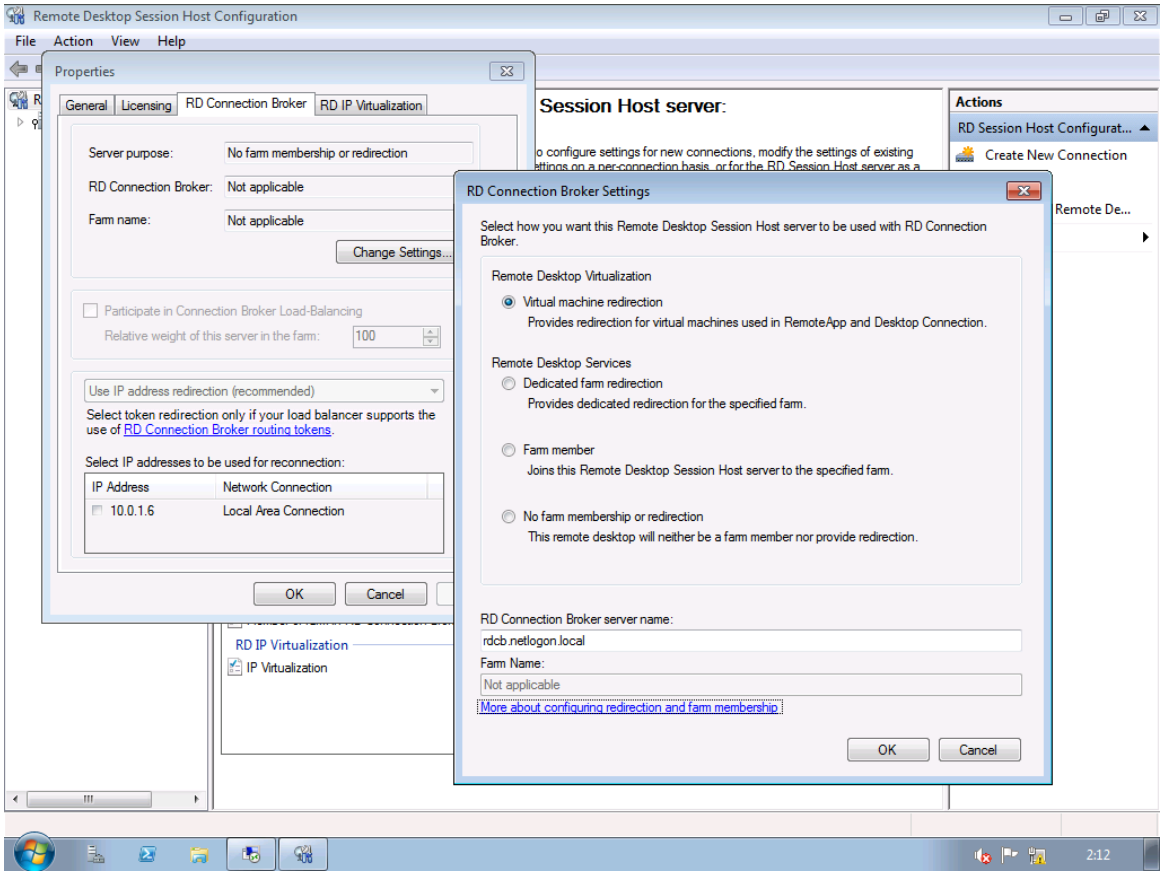
> Szerencsére van segítségünk ehhez, mégpedig egy a Microsofttól származó Powershell (na mégis, mi más? ☺) szkript formájában, mégpedig itt: http://gallery.technet.microsoft.com/ScriptCenter/bd2e02d0-efe7-4f89-84e5-7ad70f9a7bf0
>
> Ha megvan a szkript, mentsük el az ajánlás szerint, aztán a virtuális gépenként külön-külön kiadandó PS parancsok jönnek, először is:
> Set-ExecutionPolicy remotesigned –force
>
> Majd:
> Configure-VirtualMachine.ps1 -RDVHost tartomány_neve\Hyper-V_gep_neve -RDUsers tartomány_neve\csoport_neve

Plusz van még két darab érdekes feladatunk is: a virtuális gépeink nevének a Hyper-V konzolon ugyanúgy kell kinézni, mint a gépen belül, tehát FQDN névvel. Nem így szoktuk, de egyszerűen csak nevezzük át.

Illetve, és ezt viszont csak a pool gépekkel kapcsolatos feladat: ha mindent beállítottunk, feltelepítettünk, stb. a virtuális gépeken, akkor minden pool tagnak kiválasztott gépen készítsünk egy pillanatképet (snapshot), és nevezzük el, *kötelezően* erre a névre: „RDV_Rollback”. Ugyanis ez lesz a kívánt, indító állapot, és erre fogja az adott pool gépet visszaállítani minden alkalommal a Hyper-V, ha kilép a felhasználó. Így valósul majd meg a mentés és változtatás nélküli állapot, ami ugye a pool-ban tartózkodó gépek egyik fontos tulajdonsága.[131]

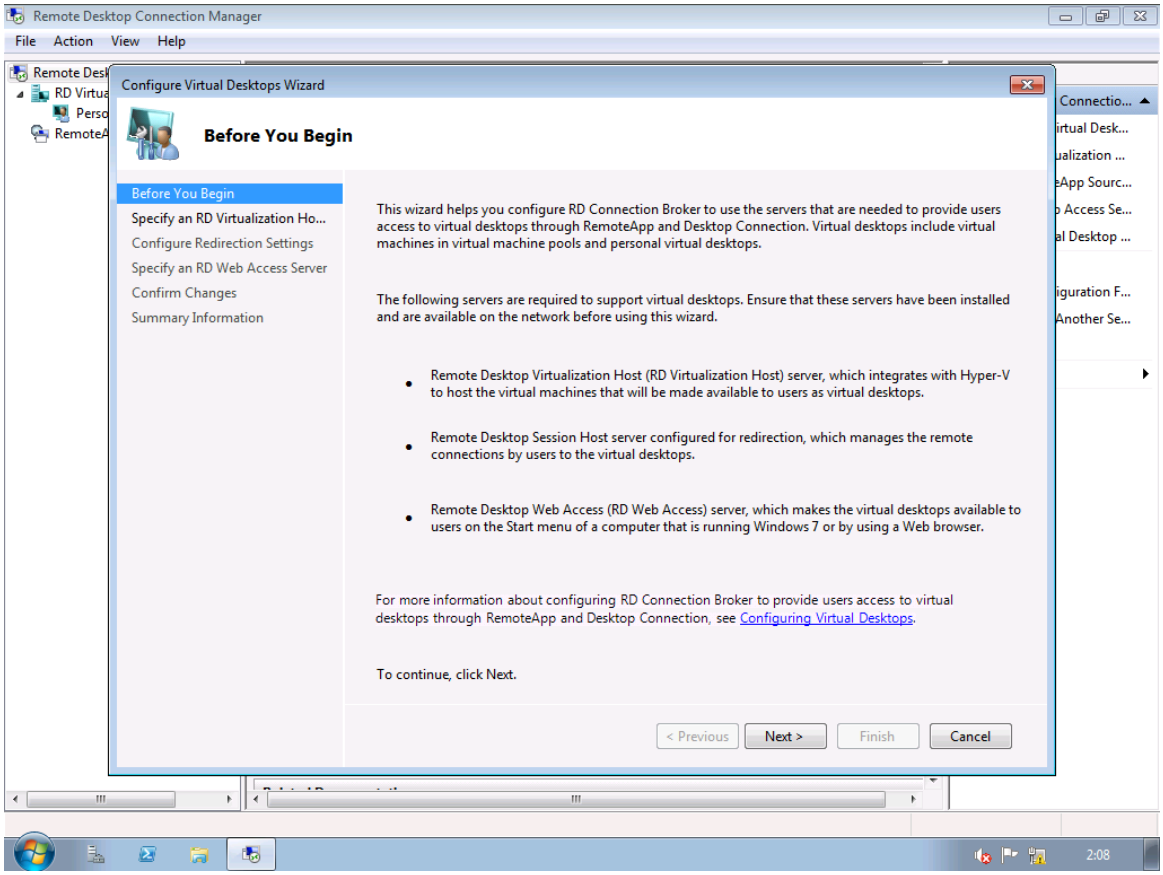
Ha ez mind rendben van, akkor jöhet az RD Connection Broker konfigurálása, immár képes beszámoló formájában. De nem is, először kezdjük mégis az RDSH-val, és a már ismert „Edit Settings”-ből bármelyik részre kattintva keressük meg az „RD Connection Broker” fület, és válaszuk a „Change Settings”-et!

[131] De célszerű gondoskodni a vándorló profilokról vagy pl. a mappa átirányításról, különben a nevesített felhasználóknak érdekes élményei lesznek mondjuk egy, a pool gépen elkészített dokumentumról ☺.

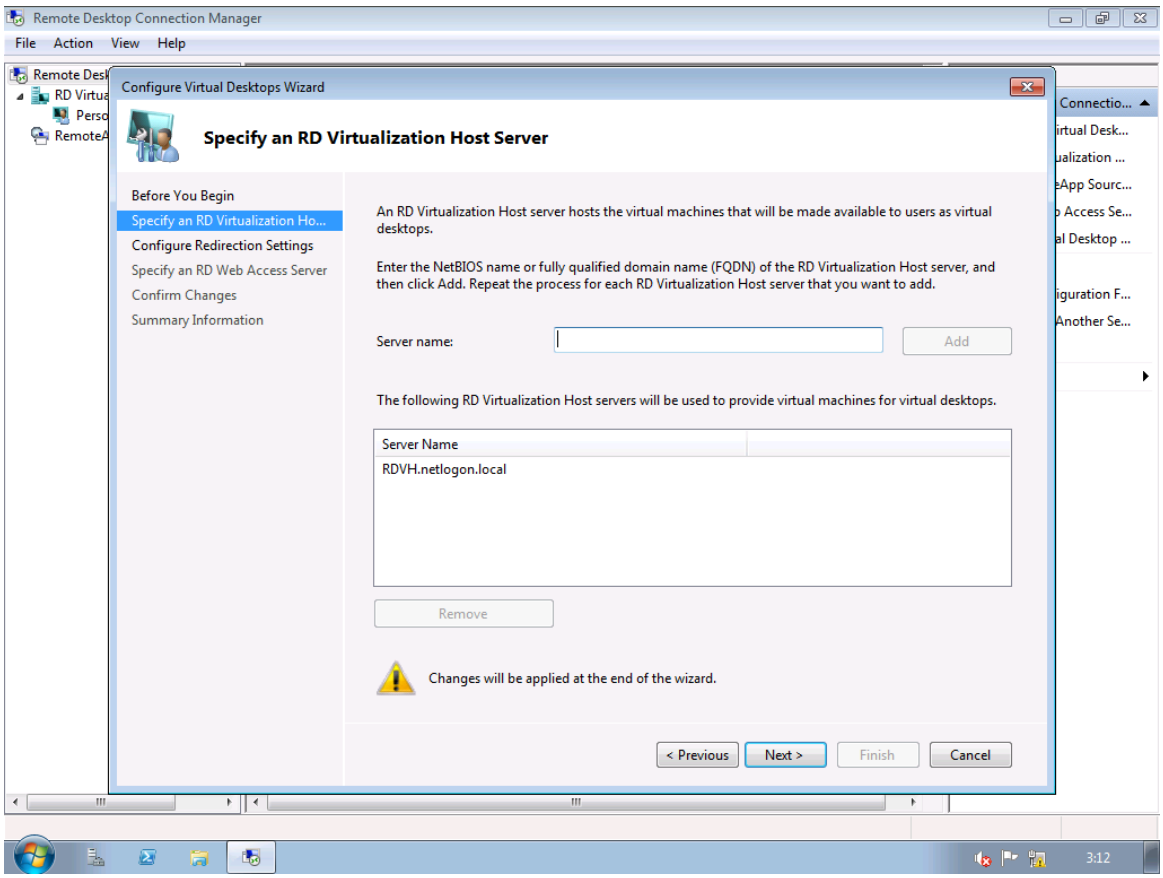


8.31 ÁBRA LEGYEN EZ EGY VM REDIRECTION RDSH, ÉS NE FELEJTSÜK EL A CB NEVÉT MEGADNI

Ezután az RDCB-ben startoljunk a legfelső sorban, azaz válasszuk a „Configure” hivatkozást az „RD Connection Broker is not configured…” szöveg mellett!

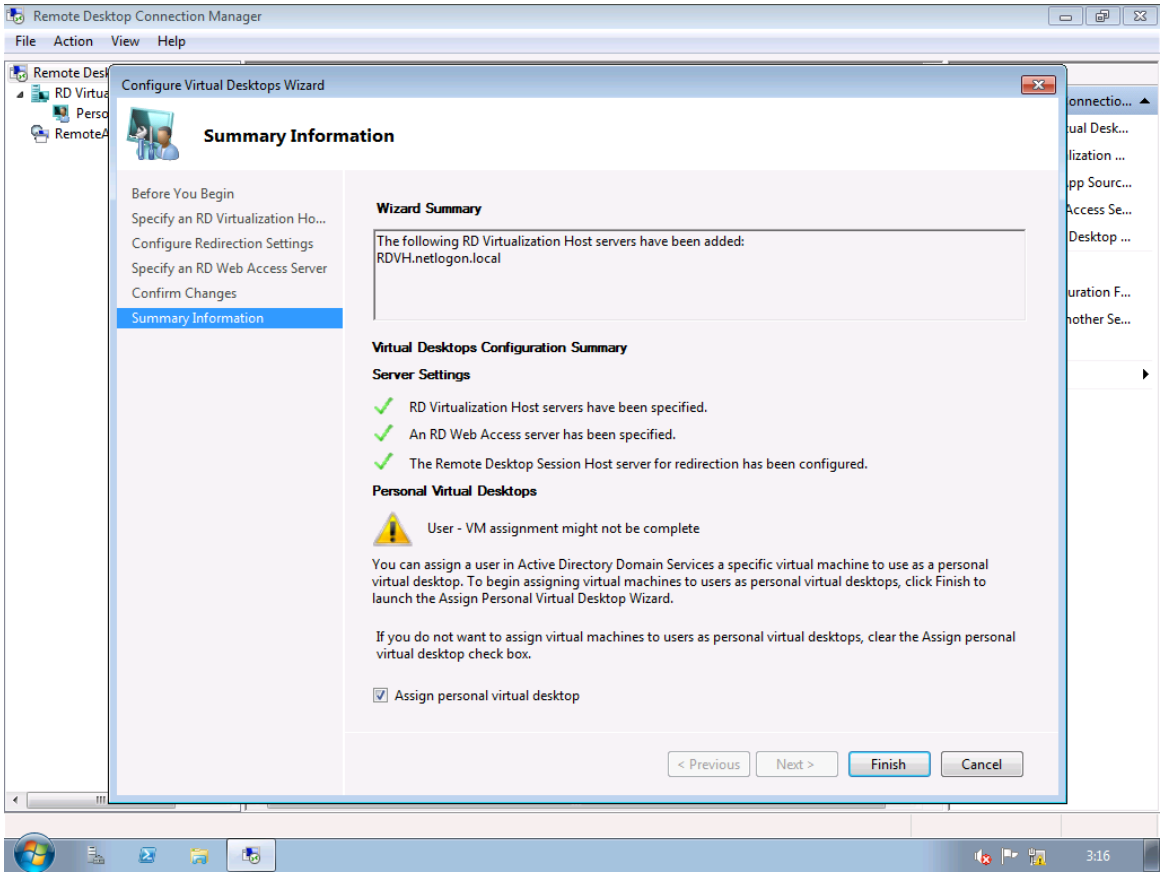


8.32 ÁBRA 3 SZERVERT KÉR, MEGKAPJA.

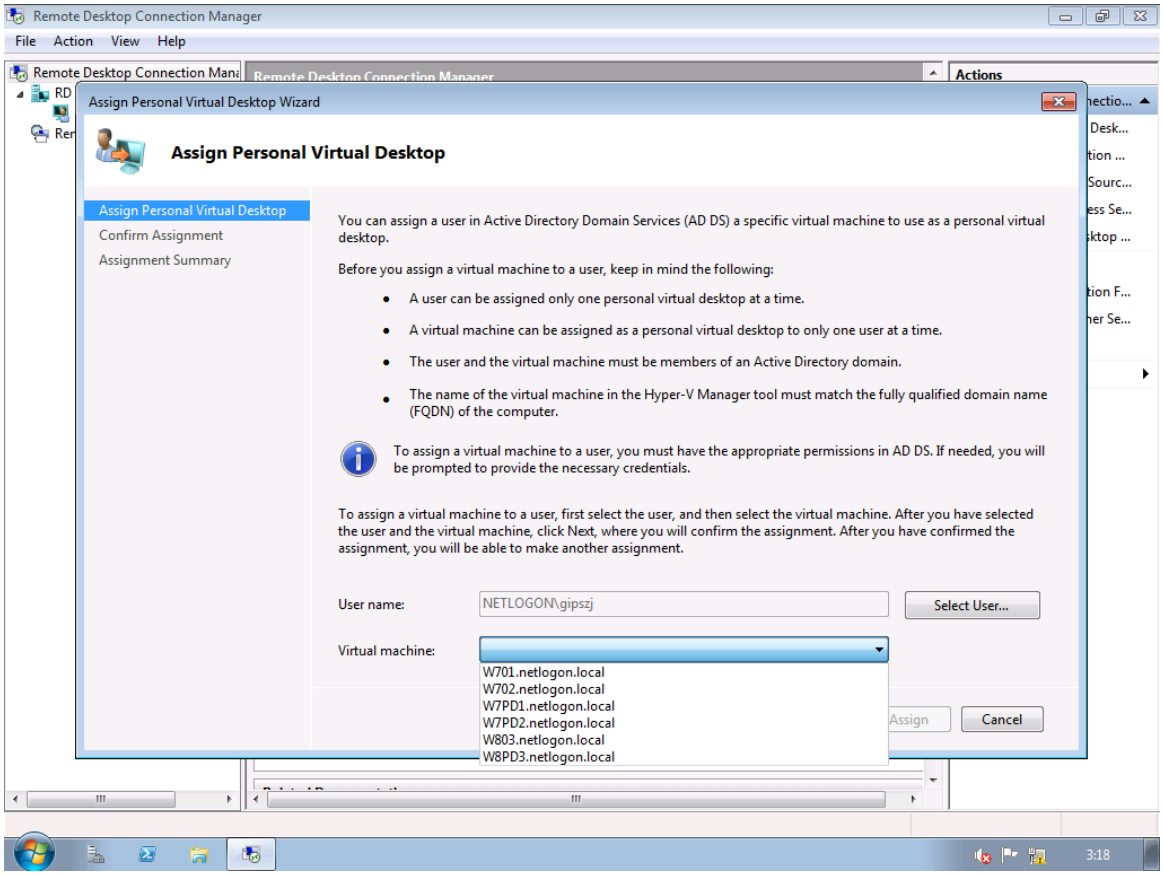


8.33 ÁBRA ELŐSZÖR ADJUK MEG AZ RDVH GÉPÜNK NEVÉT, HA ELFOGADJA, AZ FÉL SIKER

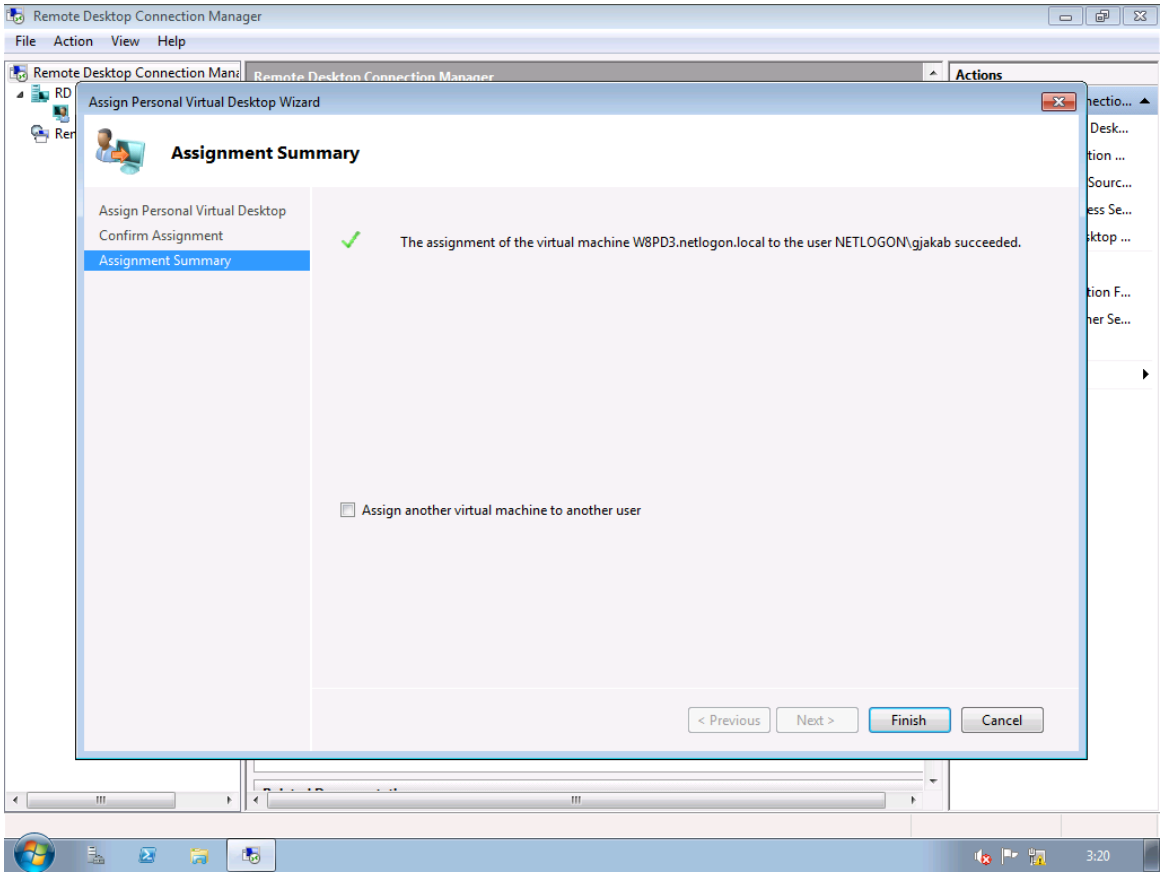
És igazából a következő két ablak is kimaradhat, ha már korábban beállítottuk az RDSH-ban a Redirector-t, és még régebben a Web Access szerverünket. Ezután az összegzés jön, majd nincs vége, az alkalmazás még csak most jön, ellenőriz mindent, és a végén 3 zöld pipát kell kapnunk. Ha így történt, akkor viszont mehet a varázslás tovább, az ablak alján már látható, hogy a személyes virtuális gépek hozzárendelése innen is indítható.



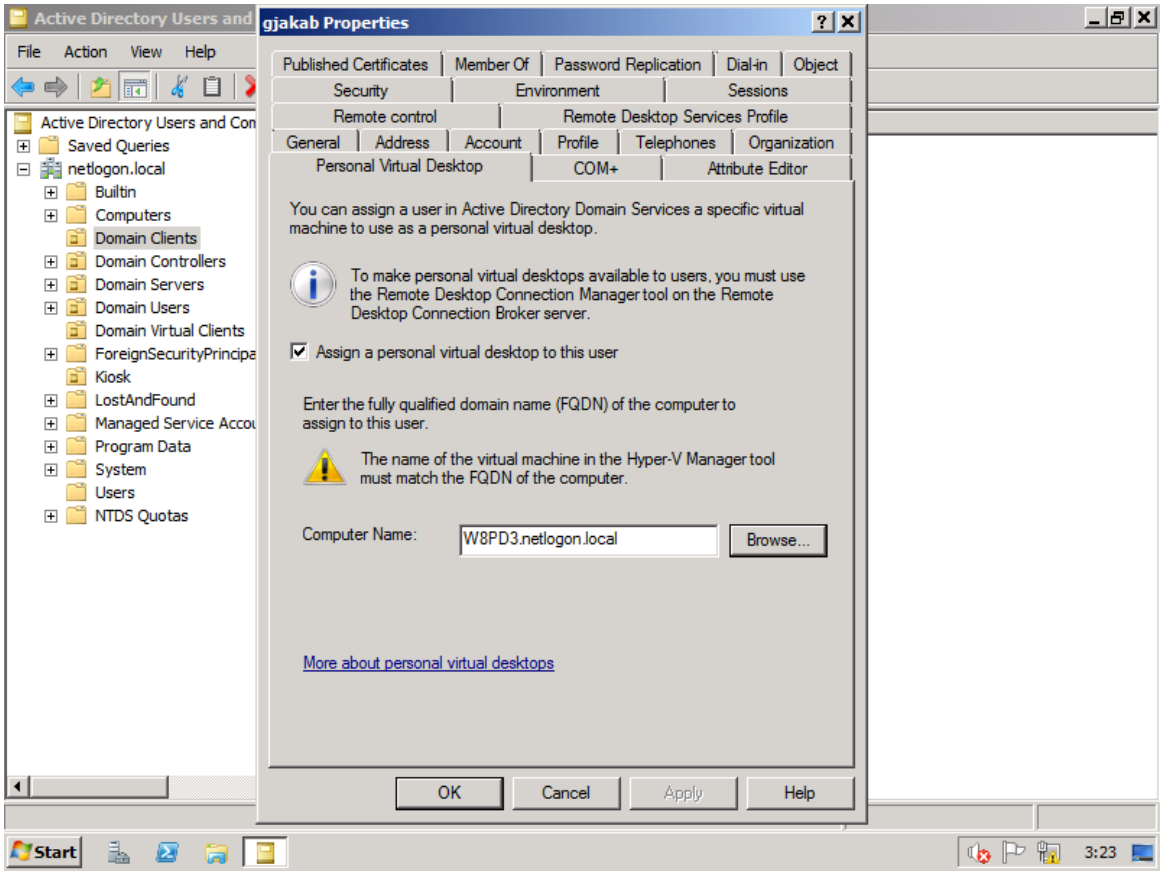
8.34 ÁBRA EDDIG OK, DE FOLYTATJUK



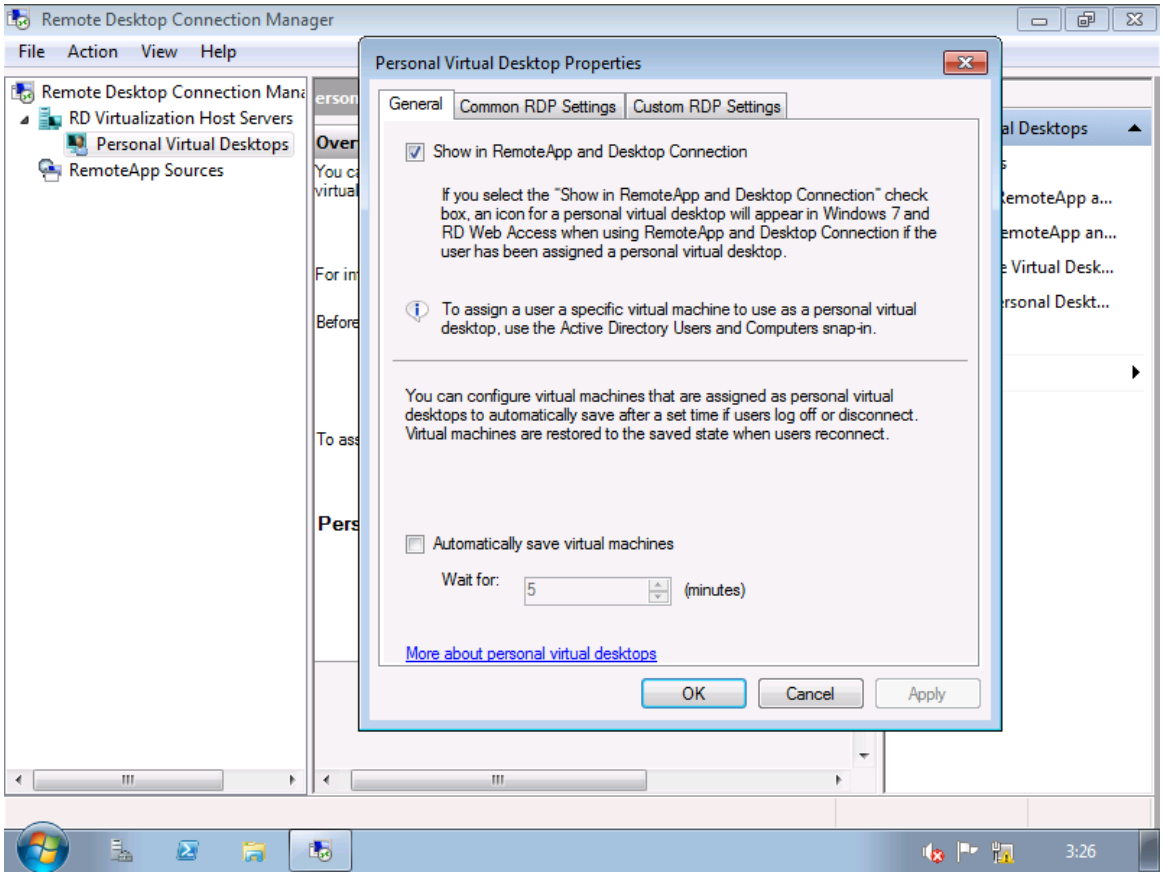
8.35 ÁBRA GIPSZJ MEGKAPJA ÉLETE ELSŐ VIRTUÁLIS GÉPÉT, ÉS HA LÁTJUK AZ ÖSSZESET, JÓL DOLGOZTUNK EDDIG



8.35 ÁBRA KÖZBEN GJAKAB IS KAP EGYET, DE Ő MÁR EGY WINDOWS 8-AT ☺

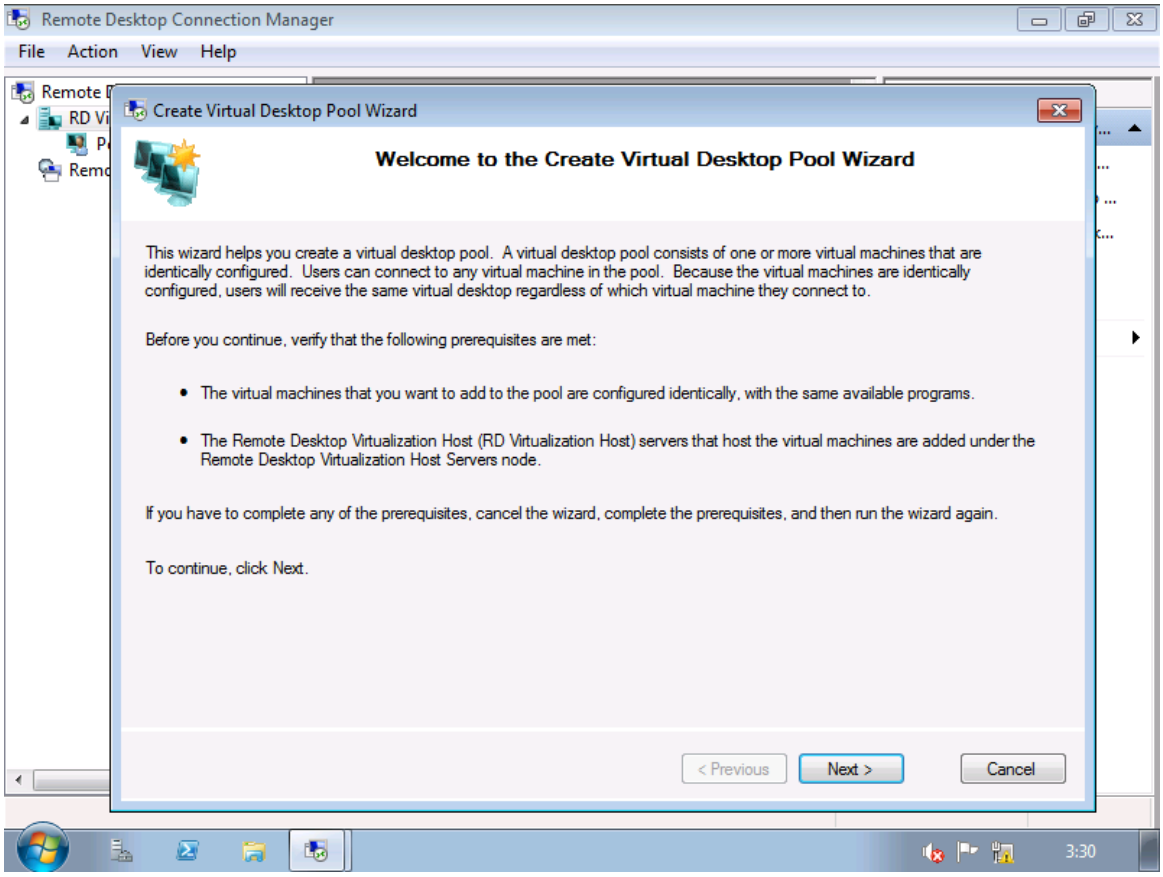


8.36 ÁBRA GJAKAB SZEMÉLYES WINDOWS 8-AS GÉPE LÁTSZIK AZ AD-BAN IS

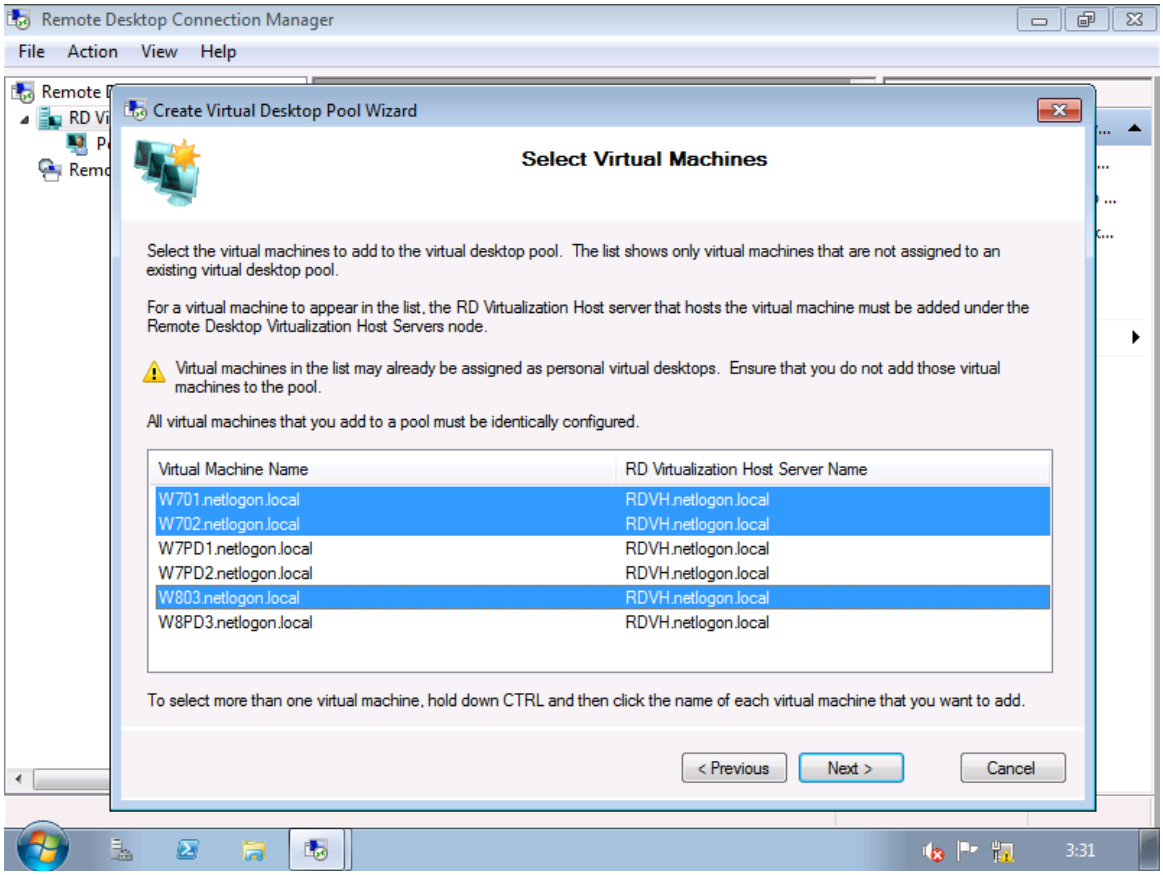


8.37 ÁBRA A SZEMÉLYHEZ RENDELT GÉPEKNEK VAN MÉG 1-2 EXTRA TULAJDONSÁGA IS

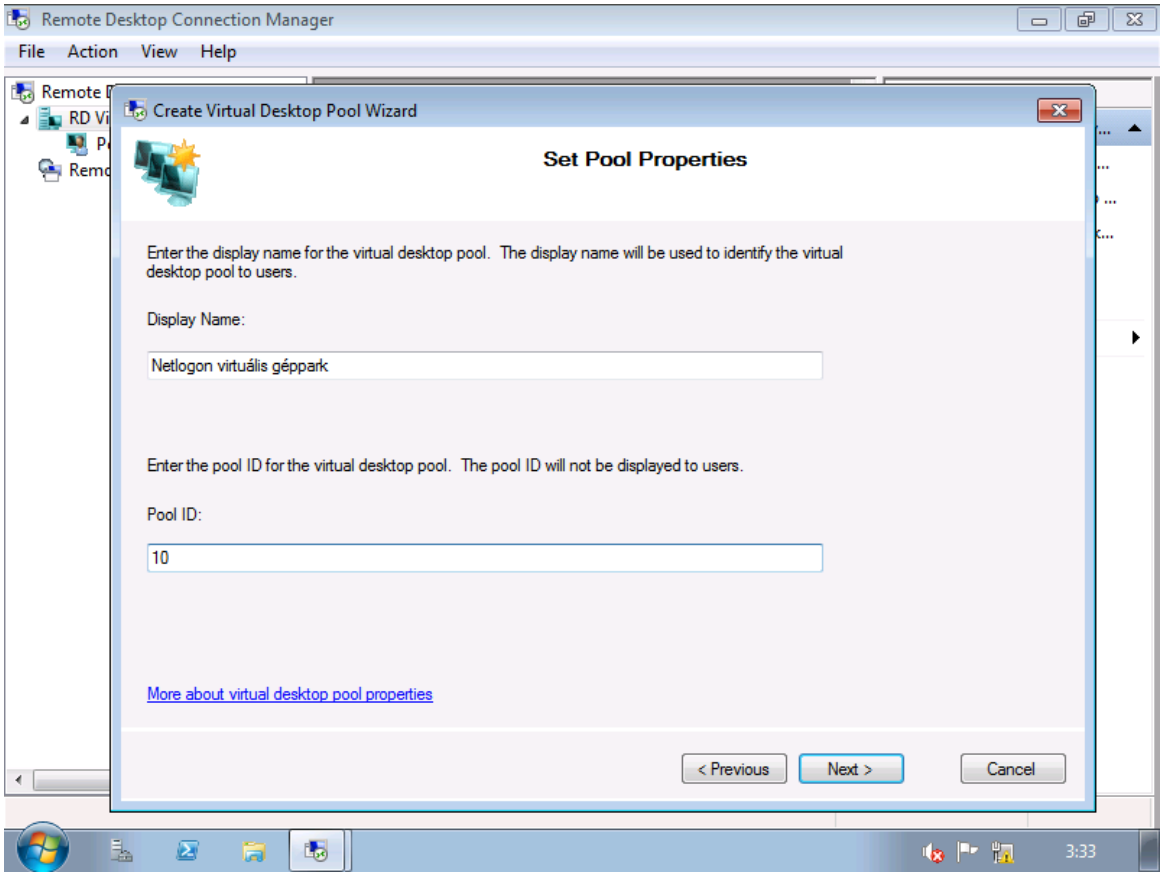
Már csak egyetlen dolgunk maradt, a pool elkészítése, azt pl. a bal oldali keretből, az „RD Virtualization Host Servers” pont helyi menüjéből indíthatjuk. Új képek jönnek.



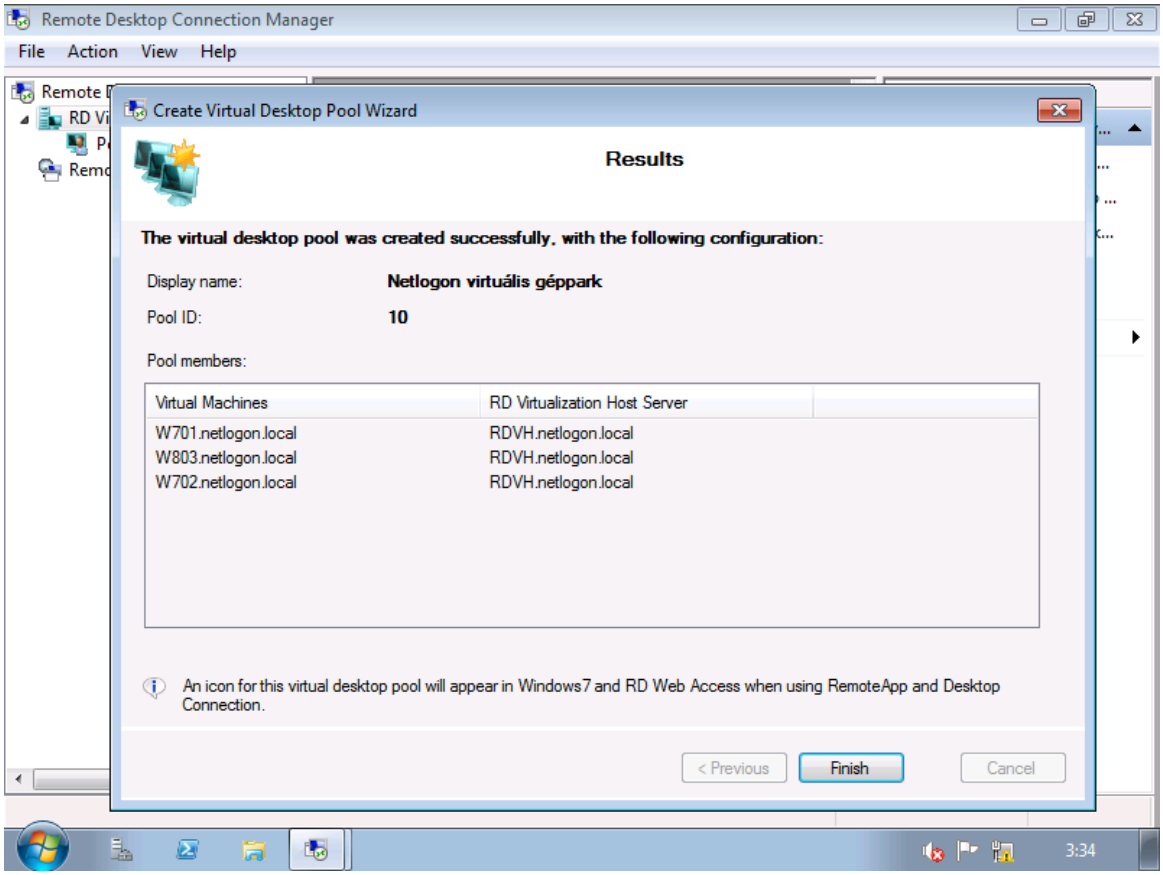
8.37 ÁBRA HALADUNK A POOL FELÉ



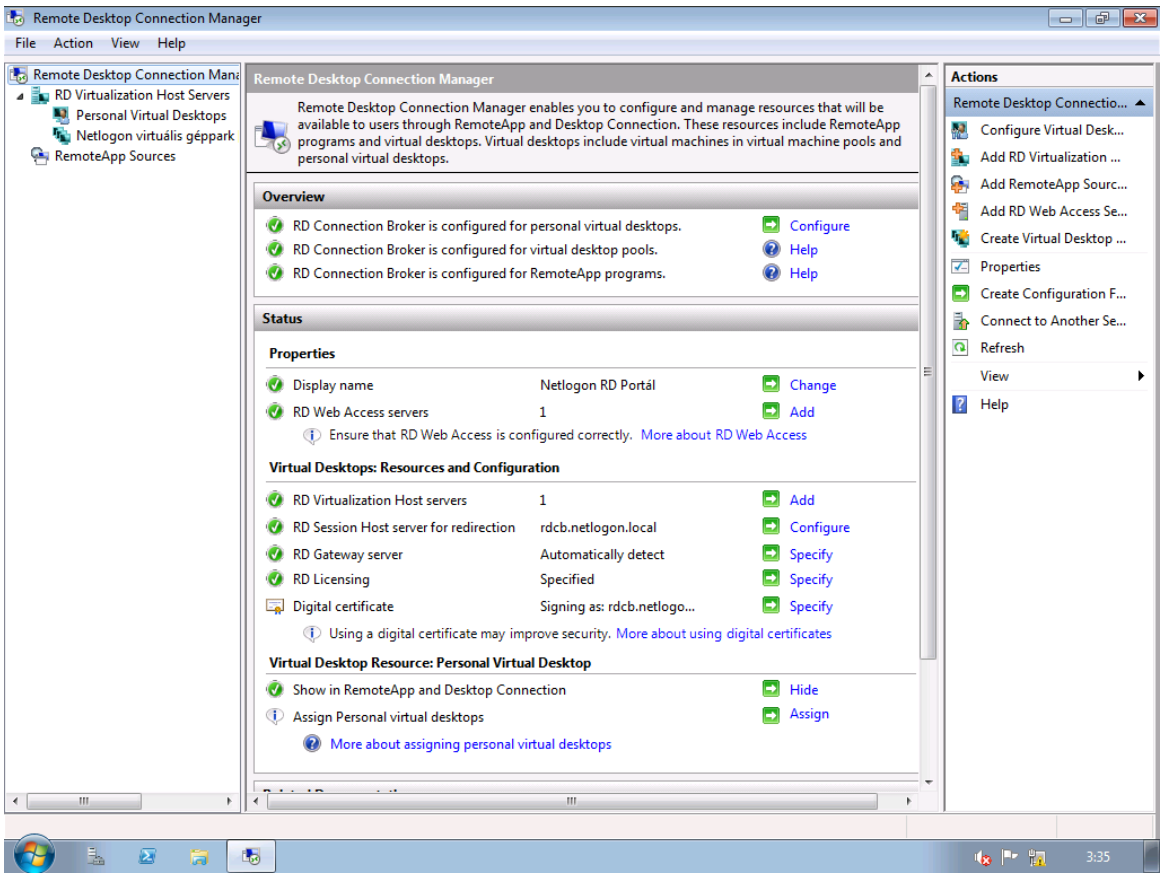
8.38 ÁBRA KÉT WINDOWS 7 ÉS EGY WINDOWS 8 LESZ POOL TAG (ÉLESBEN AZONOS LEGYEN)



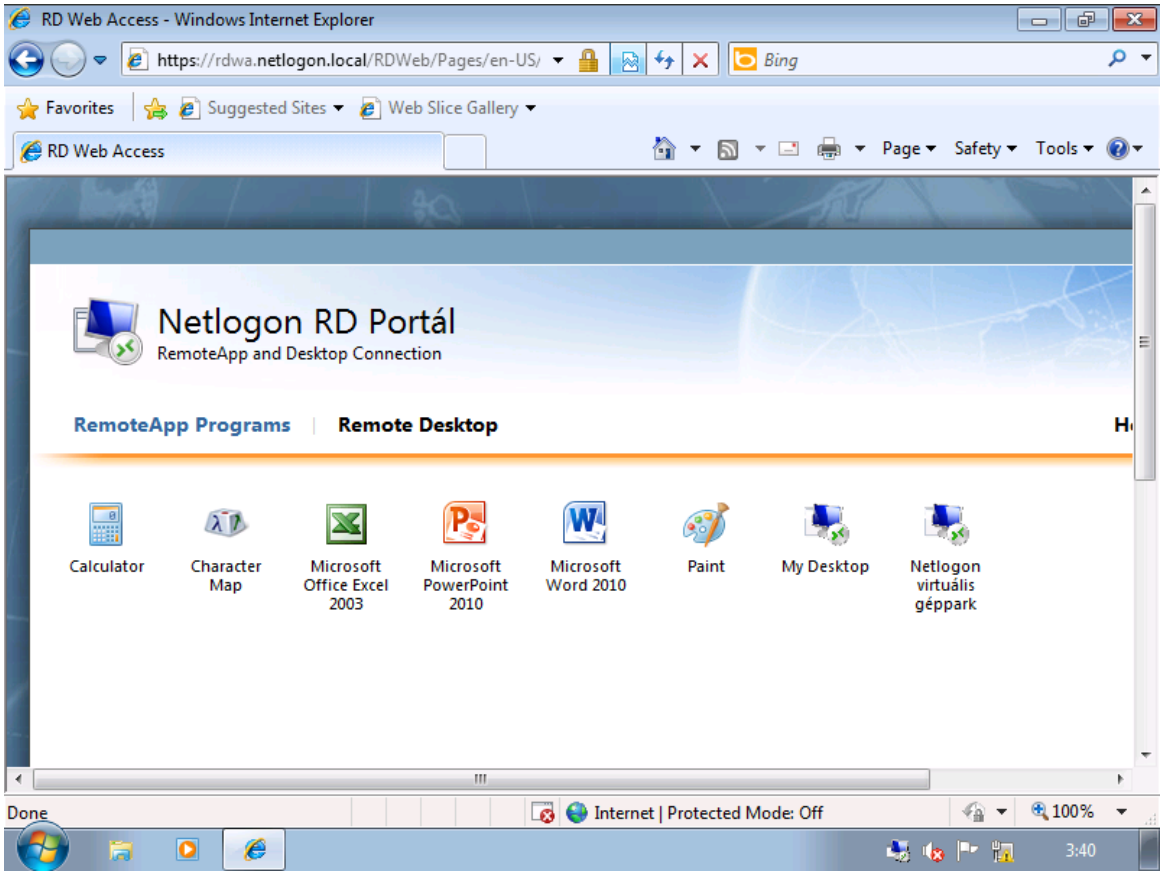
8.39 ÁBRA BÁRMILYEN NÉV ÉS AZONOSÍTÓ MEGFELEL



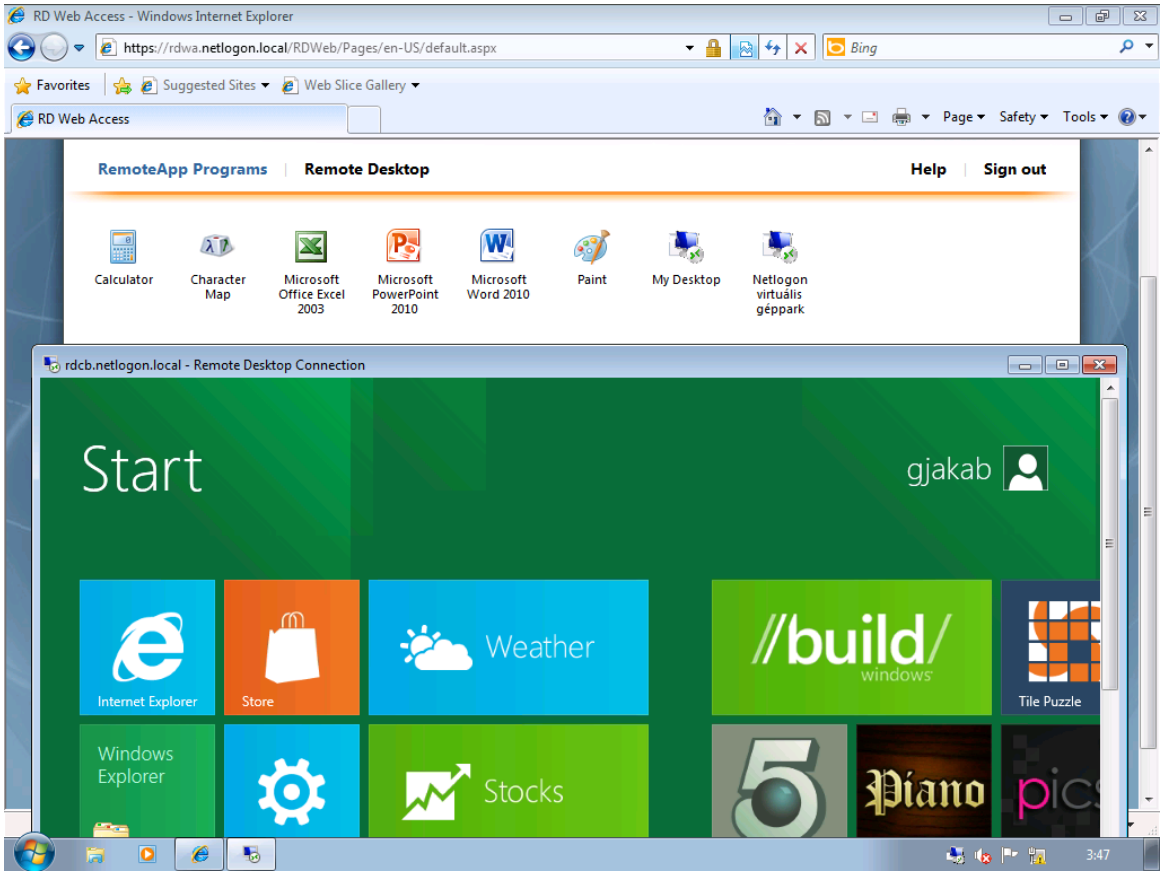
8.39 ÁBRA FELÁLLT A NETLOGON VIRTUÁLIS GÉPPARK



8.40 ÁBRA OLLÉ, MINDEN ZÖLD!



8.41 ÁBRA A KÉT UTOLSÓ IKONÉRT ROBOTOLTUNK EDDIG



8.42 ÁBRA GJAKAB SAJÁT WINDOWS 8-A MEGÉRKEZETT

8.6 RemoteApp for Hyper-V

Még egy megoldásról illik beszélni, ha már az RDS-VDI témakörnél vagyunk. Míg a VDI egy komplett desktop-ot ad a felhasználó kezébe, a RemoteApp for Hyper-V (innentől RAH) csak az alkalmazást.

Azaz a felhasználó egy (vagy több) RemoteApp ikont kap, amit a saját fizikai gépéről indít, viszont az alkalmazás egy virtuális gépen fut. Ebből persze a felhasználó semmit nem vesz észre, nem is kell, ne zavarjuk össze!

> Ha ismerjük a Windows 7 egyik kellemes újdonságát, az XP Mode-ot, akkor érteni fogjuk, hogy a RAH működési elve ugyanaz[132], csak egy távoli gépen és Hyper-V alatt. Ugyanis az XP Mode az egy alkalmazás kiajánlás, helyi desktop virtualizációval, míg a RAH szintén alkalmazás kiajánlás, csak éppen távoli desktop virtualizációval.

Van még egy komoly oka a RAH használatának, és az az alkalmazás kompatibilitás. Ugyanis az a gép, amiről majd indítjuk az alkalmazást, csak Windows 7 lehet, de a célgép akár egy XP is, IE6-tal és más őskövületekkel – amelyekre sajnos még mindig szükség van.

Ha a RAH-ot óhajtjuk, a következő előfeltételeknek kell megfelelni:

- A virtuális gép csak XP SP3 vagy Vista SP1 vagy Windows 7 (Enterprise vagy Ultimate) lehet.
- A guest gépekre egy frissítést fel kell tennünk (csak XP[133] és Vista[134] esetén), és némi registry variálásra is szükség lesz.
- A kliensen az RDC 7 az alapfeltétel, és a RemoteApp alapjául szolgáló .rdp fájlt kicsit korrigálnunk kell.
- Csoportházirenddel célszerű lesz a munkamenet szétkapcsolási beállításokat is konfigurálni, ezen a helyen:
    - Computer Configuration | Policies | Administrative Templates | Windows Components | Remote Desktop Services | Remote Desktop Session Host | Session Time Limits | Set the time for disconnected sessions.

Ezután jöhetnek a konkrét teendők, mégpedig most egy XP SP3 esetén, és egy Notepad-ot fogunk elsőként futtatni erről az OS-ről.

---

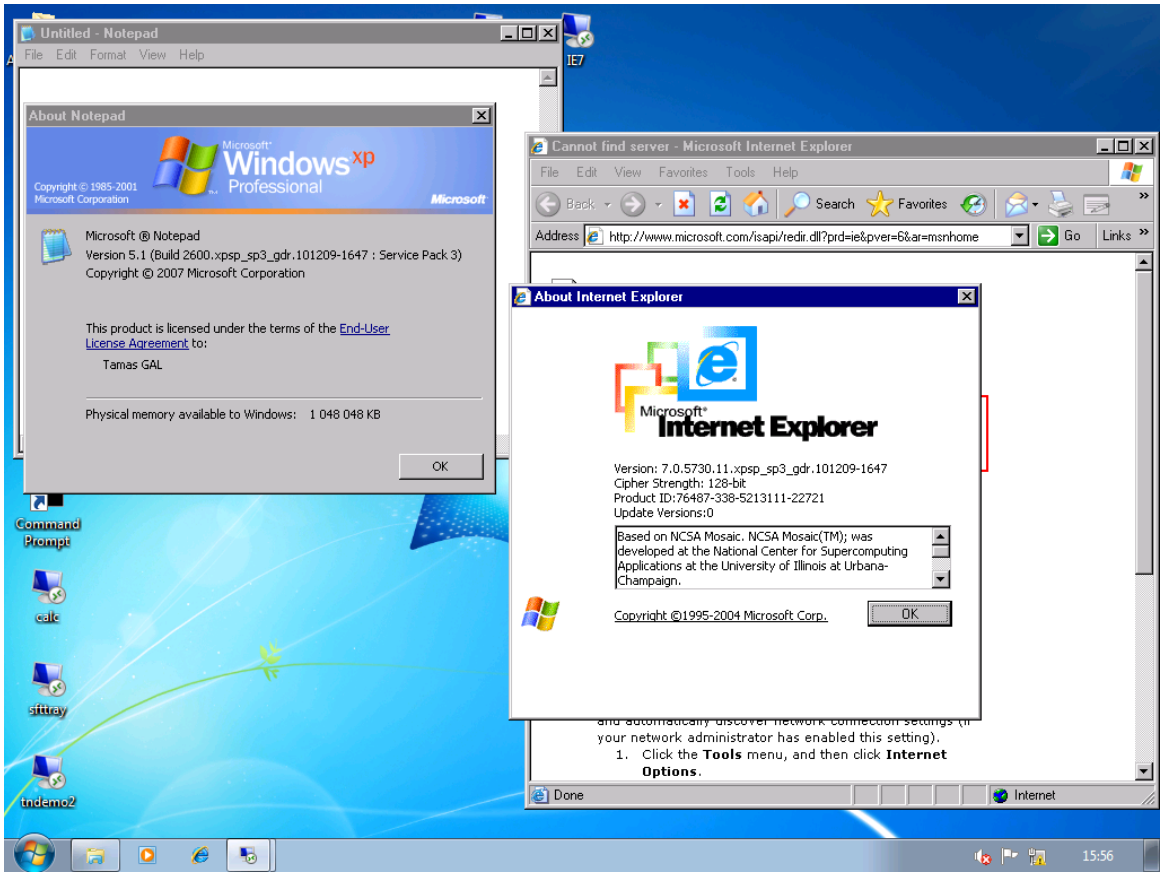
[132] Sőt, ugyanaz a hotfix teszi lehetővé ezt a működést! Ha ezt a hotfixet egy Windows Virtual PC-n futó Vistá-ra tesszük fel, akkor a helyi gépünkön egyszerre lehet IE7 és IE8/9 (a lektor megjegyzése).

[133] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=4465

[134] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=10007

- Telepítsük fel a frissítést!
- Registry: HKLM/Software/Microsoft/Windows NT/CurrentVersion/Terminal Server/TsAppAllowList/fDisabledAllowList = 1

- Lépjünk át a Windows 7-es kliensre, majd indítsunk el egy mstsc.exe-t, mentsük el az .rdp fájlt, pl. RemoteNotepad néven, majd zárjuk be.
- Nyissuk meg pl. Notepad-dal az .rdp fájlt, és javítsunk bele:
    - remoteapplicationmode:i:1
    - alternate shell:s:rdpinit.exe
- Majd adjuk a végére a következő sorokat:
    - RemoteApplicationName:s:Remote Notepad
    - RemoteApplicationProgram:s:%windir%/system32/notepad.exe
    - DisableRemoteAppCapsCheck:i:1
    - Prompt for Credentials on Client:i:1



8.43 ÁBRA EGY KLASSZIKUS NOTEPAD ÉS IE7 – WINDOWS 7-RŐL

Ez így szépen megy is, egy dolgot ne felejtsünk el: a kliensre csatlakozunk, és nem szerverre, azaz összesen egyetlen egy RDP kapcsolat áll rendelkezésre.

8.7 RD GATEWAY

Méltatlanul a végére került ez az összetevő, de csak azért, mert talán a kedves Olvasó is észrevette, hogy fokozatosan építőkockáról, építőkockára raktam össze egy

komplex RDS + VDI rendszert, és eddig az RDGW nem igazán fért bele a képbe. Azért nem, mivel erre az összetevőre tipikusan akkor van szükségünk, ha nemcsak a belső hálón, hanem kívülről is szeretnénk elérni az RDS+VDI infrastruktúránkat.

Ekkor viszont nagyon jól jön.

Ugyanis az RD Gateway nagyon tűzfalbarát megoldás. Lehetővé teszi a távoli felhasználóknak, hogy a belső hálózati RDS szerver(ek)hez való kapcsolódást HTTPS-en keresztül (RDP over HTTPS) valósítsák meg. Persze mindezt önmagában, azaz pl. VPN nélkül, a távoli felhasználónak csak egy RDP kliensre lesz szüksége a biztonságos kapcsolódáshoz. Mert hát aki próbált már vadidegen helyekről, szállodákból, stb. kapcsolódni a szervereihez, annak biztosan ugyanúgy ökölbe szorult már a lábujja, mint nekem szokott, amikor az RDP tiltásával találkozom. De ha megy HTTPS-ben, hát hadd menjen, éljen a megbonthatatlan tűzfalbarátság! ☺

Szerveroldalon ehhez szükséges egy minimum Windows Server 2008 (de az R2-vel most is sokkal jobban járunk) kiszolgáló, ami akár a tűzfal is lehet (a TMG-vel is remekül képes együttműködni), de nem muszáj, lehet a DMZ-ben is és lehet a privát hálózatban is. Így vagy úgy, a lényeg, hogy a távoli kliensnek ehhez a szerverhez kell kapcsolódni SSL-el, hogy aztán ez a szerver végezze a konverziót a klasszikus, belső, csak az RDP-vel operáló RDS szerver(ek) felé. De még egyszer hangsúlyozom: nem VPN vagy DirectAccess helyett használjuk, a hatása kizárólag az RDP/HTTPS forgalomra irányul.

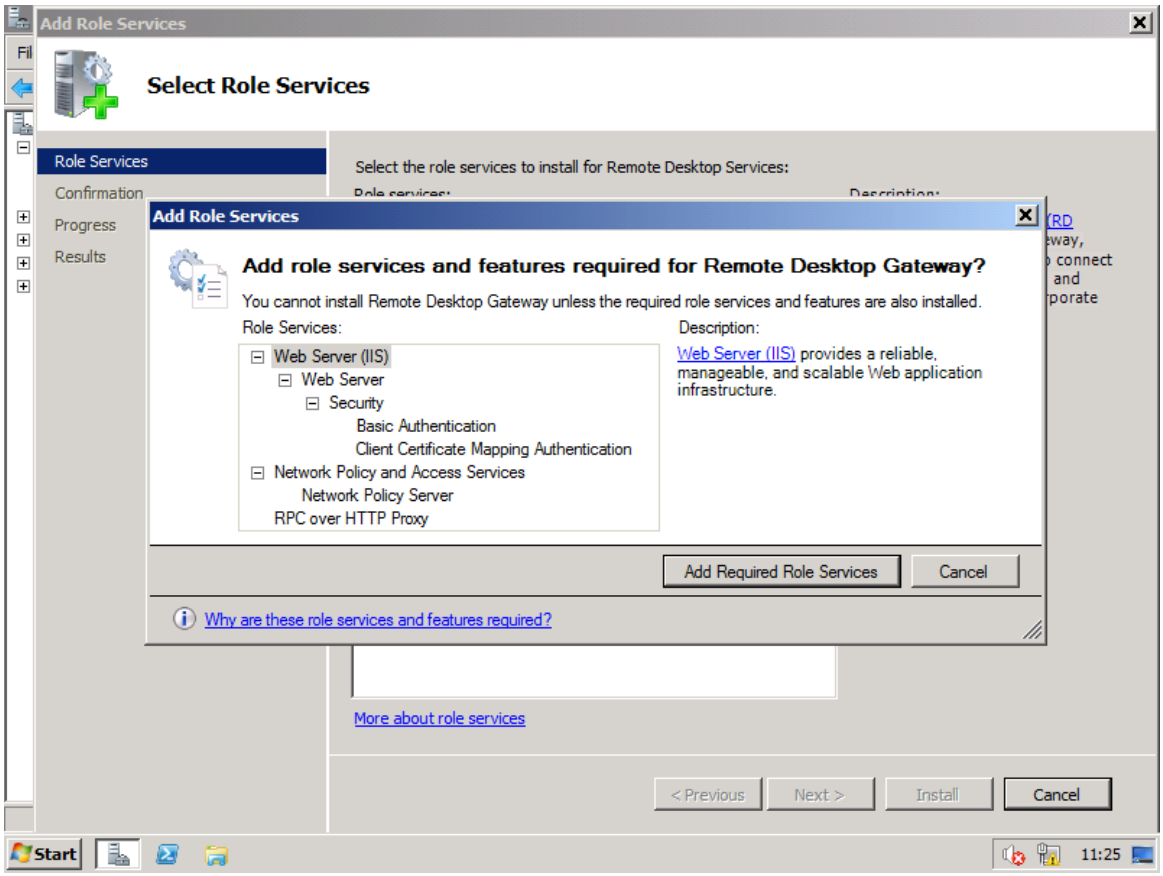
De nemcsak a RDP/HTTPS konverziót teszi hozzá az RD Gateway a lehetőségeinkhez, hanem azért pluszban hozzáférés-szabályzást illetve erőforrás-elérést is képes ellátni. Nézzük tehát a kétfelé oszló szabályozás lehetőségeit kicsit részletesebben:

- Kapcsolat engedélyező házirendeket (RD CAP = Connection Authorization Policies) gyárthatunk a RD Gateway Manager MMC-ben - vagy akár már a komponensek telepítése közben -, melyekkel felhasználóknak, csoportoknak adhatunk kapcsolódási lehetőséget a RD Gateway-hez. Mindehhez a helyi felhasználói adatbázisból vagy az AD-ból is vehetünk fiókokat, illetve ezek hiányában akár teljesen saját készítésű fiókokkal is képes megoldani. Olyan CAP házirendet is készíthetünk, melyben azokat a belső hálózati erőforrásokat (gépeket) jelöljük meg, melyeknek adunk hozzáférést, de a különböző eszközök (meghajtók, vágólap, nyomtatók, stb.) átirányítását is elvégezhetjük a CAP házirendekből.
- Készíthetünk erőforrás engedélyező házirendeket is (RD RAP = Resource Authorization Policy), amelyekkel szabályozható, hogy a hálózaton belül mely gépeket (számítógép csoportokat) érhetik el távoli felhasználók (akik szintén szelektálhatóak itt is). Szintén lehetséges a meglévő helyi vagy AD csoportok,

vagy a helyben, az RD Gateway Managerrel létrehozott csoportok használata, vagy akár úgy is beállíthatjuk, hogy ne legyen semmilyen korlátozás.

1-2 további extrát is feljegyezhetünk a neve mellé:

- Az R2-es verzió már NAP integrációval is rendelkezik.
- Állandó belépési üzeneteket, illetve admin és/vagy rendszer (instant) üzeneteket is publikálhatunk.
- A külső biztonságos eszközátirányítás is megvalósítható (R2 RDSH és RDP7 esetén).

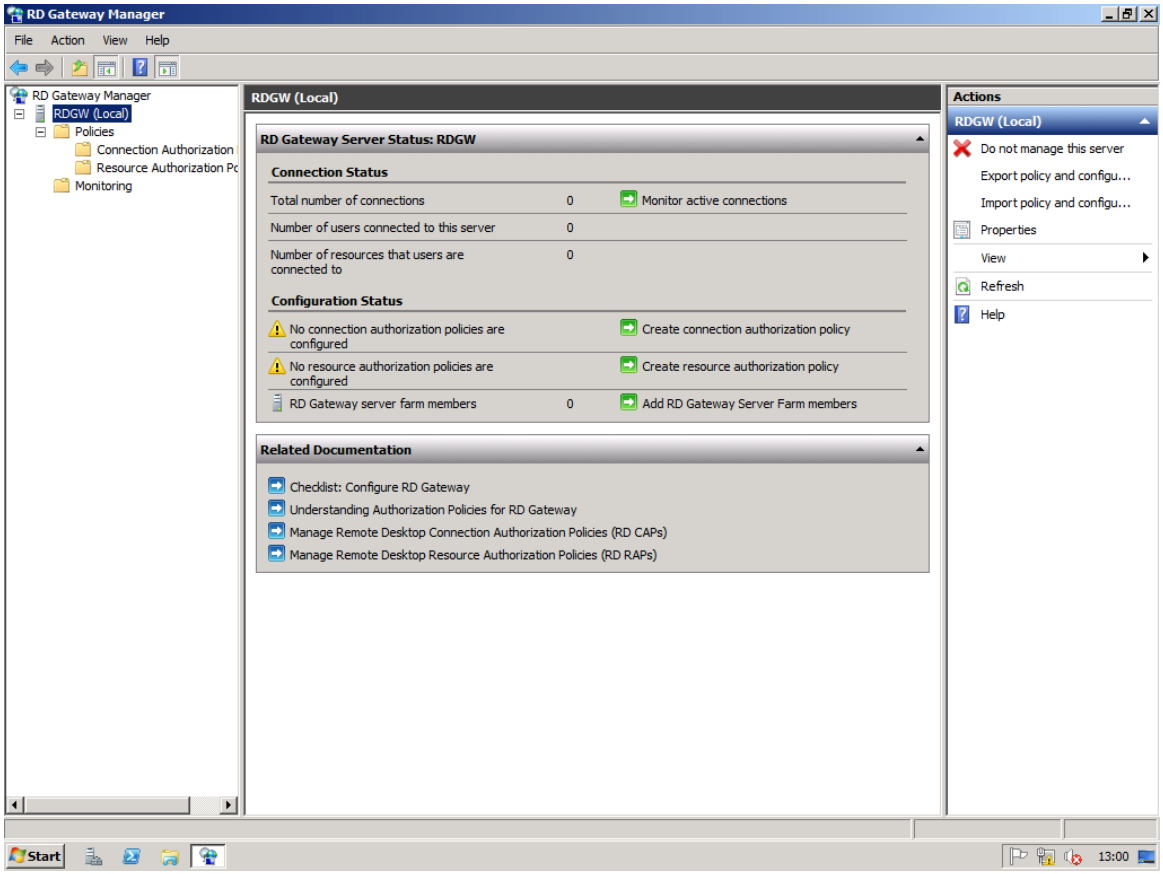


8.44 ÁBRA AZ RD GATEWAY SZEREP TELEPÍTÉSÉHEZ KÖTELEZŐ ELEMEK

A telepítése során az első fontos kérdés a tanúsítvány használat lesz, ami lehet önaláírt, belső és külső tanúsítványkiadótól származó, és el is odázhatjuk a kérdést, de a lényeg, hogy legyen tanúsítvány (az önaláírtat azért hagyjuk ki, ha lehet). A telepítő felajánlja az azonnali házirend gyártást is, de ezt egyelőre hagyjuk ki!

Illetve még egy szerepkörhöz ragaszkodik, mégpedig az NPS telepítéséhez, no vajon miért is? Nos, a NAP támogatás miatt.

Ha felment, akkor keressük fel az RD Connection Manager-t, és kezdjük el nézegetni!

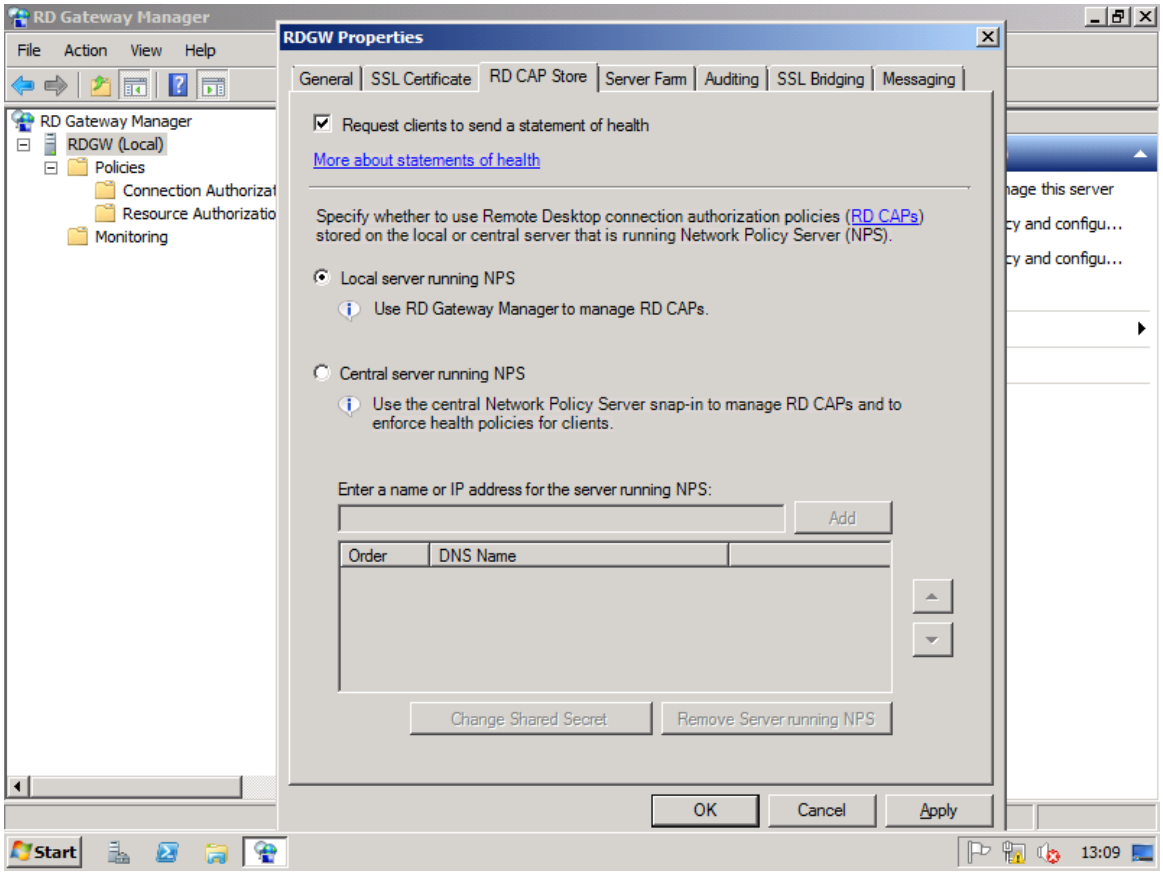


8.45 ÁBRA AZ RD GATEWAY MANAGER

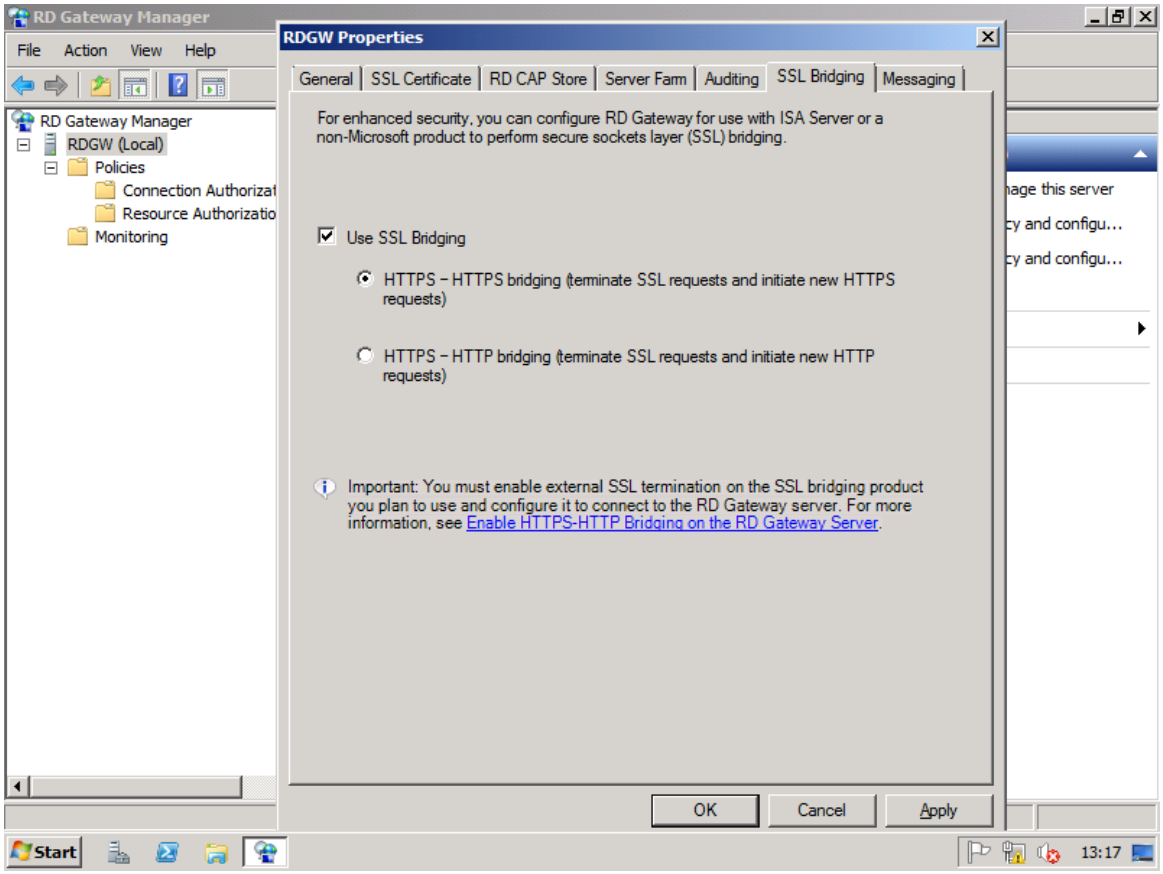
Kezdjük a globális beállításokkal, a gépünk tulajdonságai között. Az első három fülön a kapcsolatok számának korlátozását, majd a tanúsítványunk beállítását, illetve a NAP beállításokat (ahol például a RD CAP-jaink – központilag is – megtalálhatóak lennének) találjuk.

Azután – mivel a rendelkezésre állás ebben az esetben is fontos - az esetleges RDGW farm tagsági beállításait kapjuk meg. Az „Auditing” alatt a naplózás részletességét állíthatjuk be, míg az „SSL Bridging”-nél az ISA vagy TMG, vagy más publikáló eszközzel történő kapcsolódás szabályzása látható. Ha használjuk, két eset lehetséges:

- HTTPS-HTTPS: Annak ellenére, hogy pl. a TMG terminálja majd a HTTPS kapcsolatot (azért, hogy az összes szűrési képességét be tudja vetni), azért legyen a TMG és az RDGW között is SSL csatorna.
- HTTPS-HTTP: Ne legyen két SSL tunnel (az első ugye a külső user gépe és a TMG külső lába között van), a TMG és a RDGW között elég nekünk a HTTP is.



8.46 ÁBRA NAP VAGY NEM, HA IGEN HELYI VAGY TÁVOLI?



8.47 ÁBRA A VISZONY A TŰZFALHOZ

Egyetlen dolog maradt a globális beállításoknál, mégpedig egy R2-es újdonság, az üzenetek, amelyeket majd csatlakozó felhasználók kapnak meg. Van ideiglenes rendszer üzenet, és van állandó belépési üzenet, és keménykedhetünk is, azaz olyan felhasználók számára letilthatjuk az összes kapcsolódási lehetőséget, akiknek az RDP kliensei nem képesek ezeket az üzeneteket fogadni (lásd közvetkező táblázat).

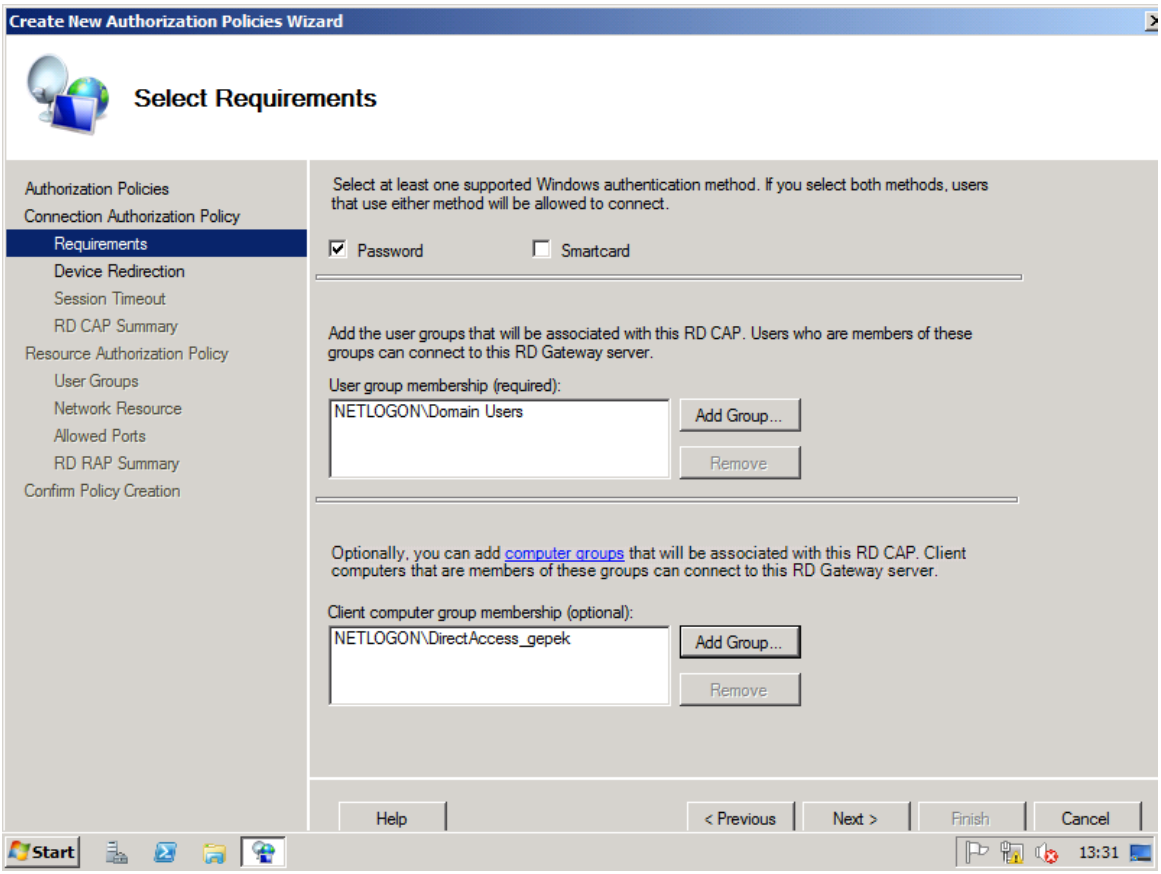
	Win7/ R2	Vista SP+	Vista SP+	XP SP3	XP SP3	XP SP2	XP SP2
	RDC 7.0	RDC 7.0	RDC 6.1	RDC 7.0	RDC 6.1	RDC 6.1	RDC 5.2
Felhasználónkénti szűrés a RemoteApp alkalmazásoknál	igen	igen	igen	igen	igen	igen	-
Web SSO	**igen**	**igen**	nem	**igen**	nem	nem	nem
Webes űrlap alapú hitelesítés	igen	igen	igen	igen	igen	igen	nem
RD Gateway alapú eszközátirányítás	igen	igen	igen	igen	igen	igen	nem
RD Gateway rendszer- és bejelentkezési üzenetek	**igen**	**igen**	nem	**igen**	nem	nem	nem
RD Gateway autentikáció és autorizáció – a háttérben	**igen**	**igen**	nem	**igen**	nem	nem	nem
RD Gateway időtúllépések (inaktív és session)	**igen**	**igen**	nem	**igen**	nem	nem	nem
NAP vizsgálat az RD Gateway-en keresztül	**igen**	**igen**	nem	**igen**	nem	nem	nem

8.48 ÁBRA A BIZTONSÁGI MÁTRIX – AZ RD GATEWAY KAPCSÁN KÜLÖN ÉRDEKES LESZ

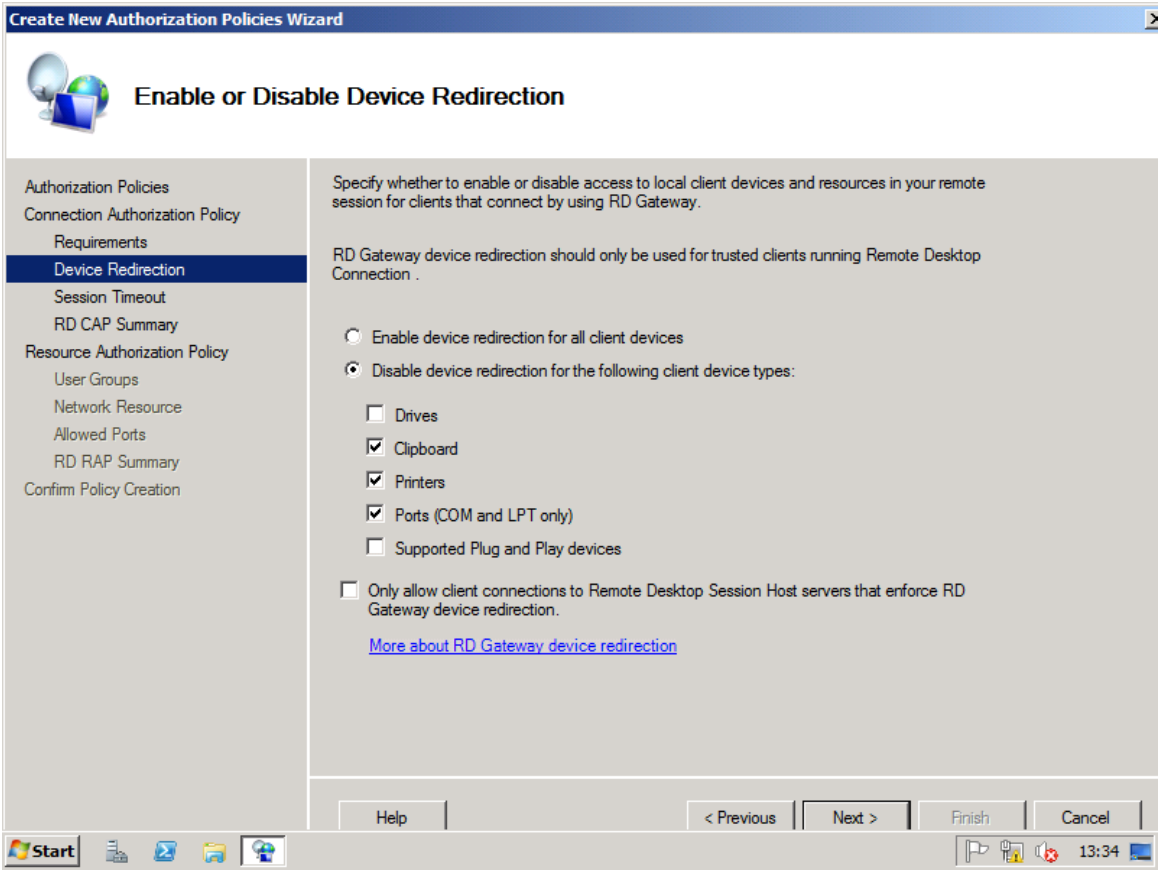
És akkor hozzuk végre létre a házirendeket, mert ez a lényeg, a bal oldali keret faszerkezetében látjuk is már ezek tárolóit, persze jelenleg még üresek. Ha mondjuk a CAP-pal kezdjük, akkor látszik, hogy az NPS szerveren lévő CAP-ok is használhatóak lennének, de mi inkább helyit készítünk most, és a varázslóval. Ebben az a jó, hogy egyből meg is adhatjuk, hogy a CAP mellett legyen egy RAP-unk is, válasszuk most ezt, és akkor egy menetben túl leszünk rajta.

Adjunk egy nevet először a CAP-nak[135], majd jöjjön az első restrikciós panel! Itt a legalsó csoport az érdekes, azaz a gépek domain tagsága szerint is szelektálhatunk a kliensek közül. Én például csak és kizárólag a DirectAccess laptopoknak engedtem meg, hogy belépjenek az RDGW-n keresztül (és ezeken a gépeken is csak a „Domain Users” csoport tagjai).

[135] Tetszőleges mennyiségű CAP és RAP házirendünk lehet, lesz majd sorrend is, az elnevezésnél ezt esetleg vegyük számba.



8.49 ÁBRA HITELESÍTÉS, FELHASZNÁLÓI CSOPORT, GÉP CSOPORT

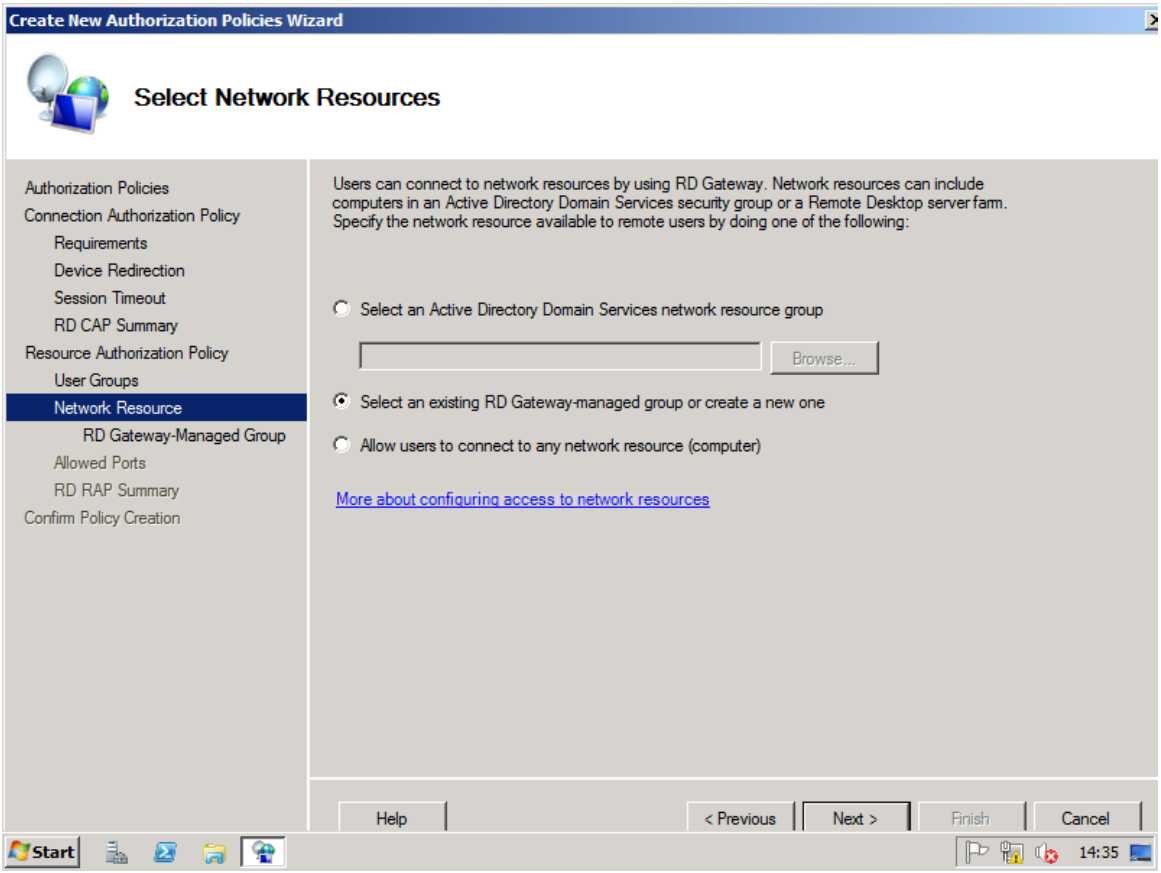


8.50 ÁBRA A MEGHAJTÓK ÉS A PNP ESZKÖZÖK TILTÁSA

Az alsó képen - az eddigi összes eszközátirányításos beállítással szemben - itt és most a tiltásokat kell bepipálnunk. A kicsit különálló „Only allow client…” négyzet az RDP 7.0 vagy újabb használatát teszi kötelezővé. A következő panelen a „nyugalmi állapot” (idle) és a munkamenetek időtúllépési beállításait láthatjuk, de ez most érdektelen. Ha ez mind megvan, jön a szumma képernyő, majd térjünk át az RD RAP gyártásra.

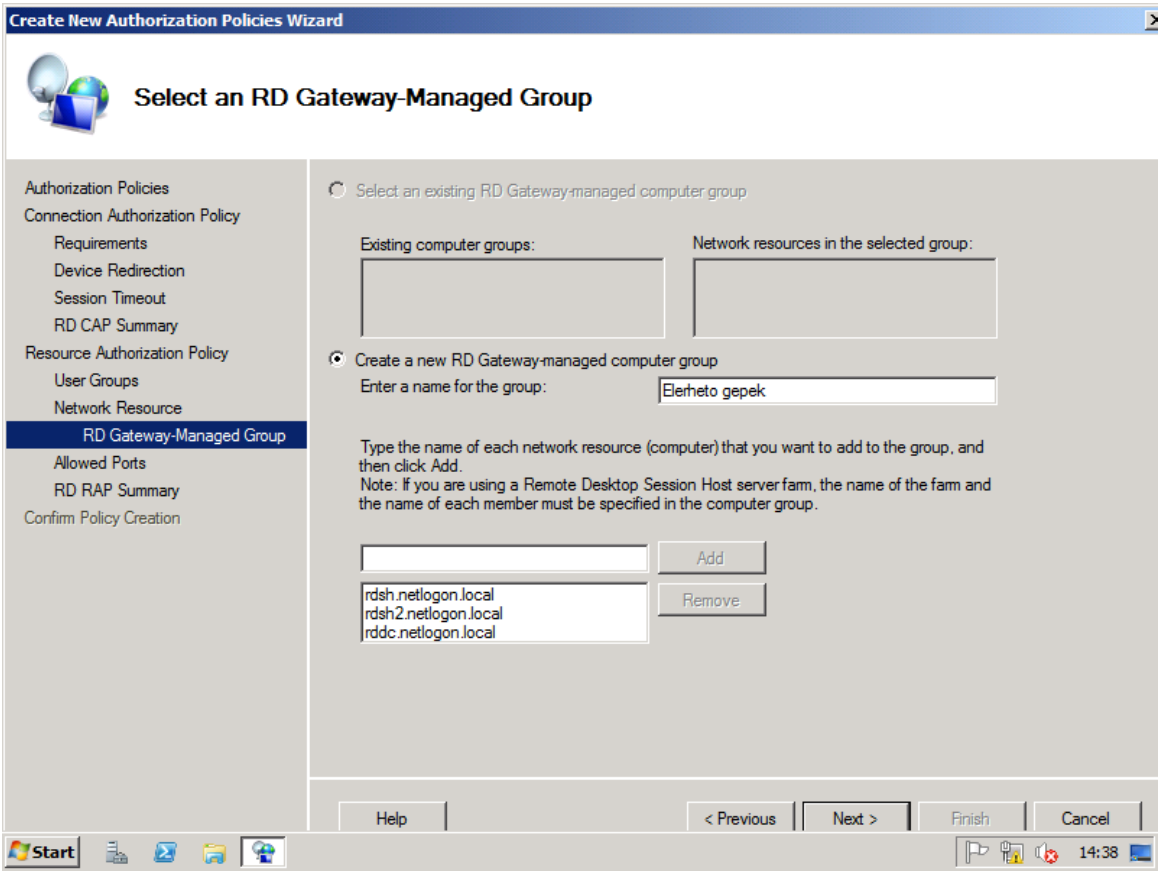
Újra csoporto(ka)t kell kijelölnünk, de ezek már nem a kapcsolódáshoz, hanem az erőforrások eléréséhez lesznek majd szükségesek. Ezután azokat az adott gépeket, gépcsoportokat jelöljük majd ki (tipikusan a szerverek), amelyekhez a korábban megadott felhasználók hozzáférhetnek az RDP kapcsolat során. Azaz ha az RDGW-n keresztül jönnek, akkor bármelyik szervert nem érhetik majd el, csak és kizárólag a kijelölteteket. Három variáció van:

1) AD csoport
2) Az RDGW-n kattintgatunk össze egy csoportot, vagy választunk egy már legyártottat
3) Nincs erőforrás-hozzáférés korlátozás, legalábbis az elérhető gépek szerint nem csinálunk ilyet



8.51 ÁBRA HOVA ENGEDJÜK BE?

Ha a középsőt választjuk, akkor nekünk kell a gépek, vagy pl. egy RDSH farm esetén a farm nevét (is!) megadni, de az is lehet, hogy szélsőséges esetben IP címeket kell beírni a listába.



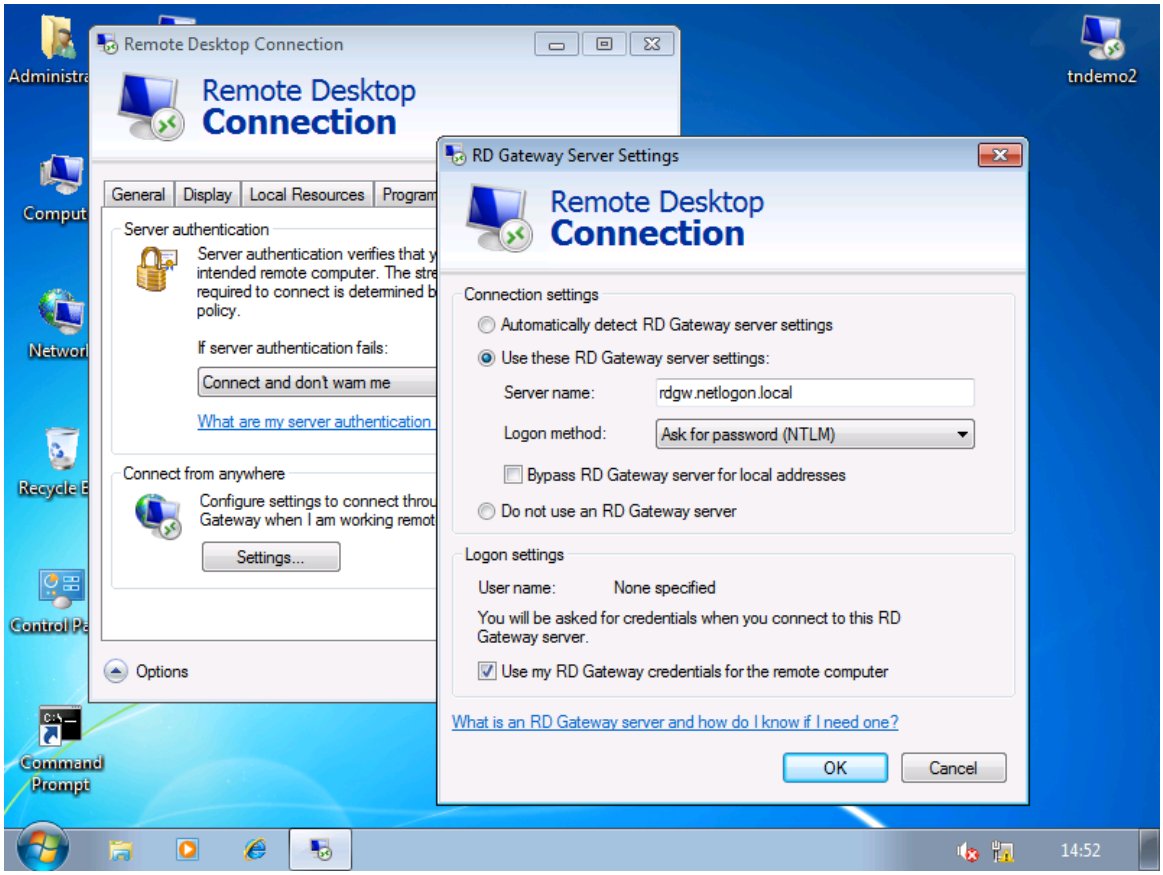
8.52 ÁBRA VIGYÉTEK A DC-T IS!

Most már tényleg csak egy elem van hátra a varázslóból, mégpedig a TCP port szűkítés vagy éppen a bármilyen port megadásának a lehetősége. Ezután ismét szumma, majd végeztünk, immár rendelkezünk hozzáférési és erőforrás házirend szabályokkal is.

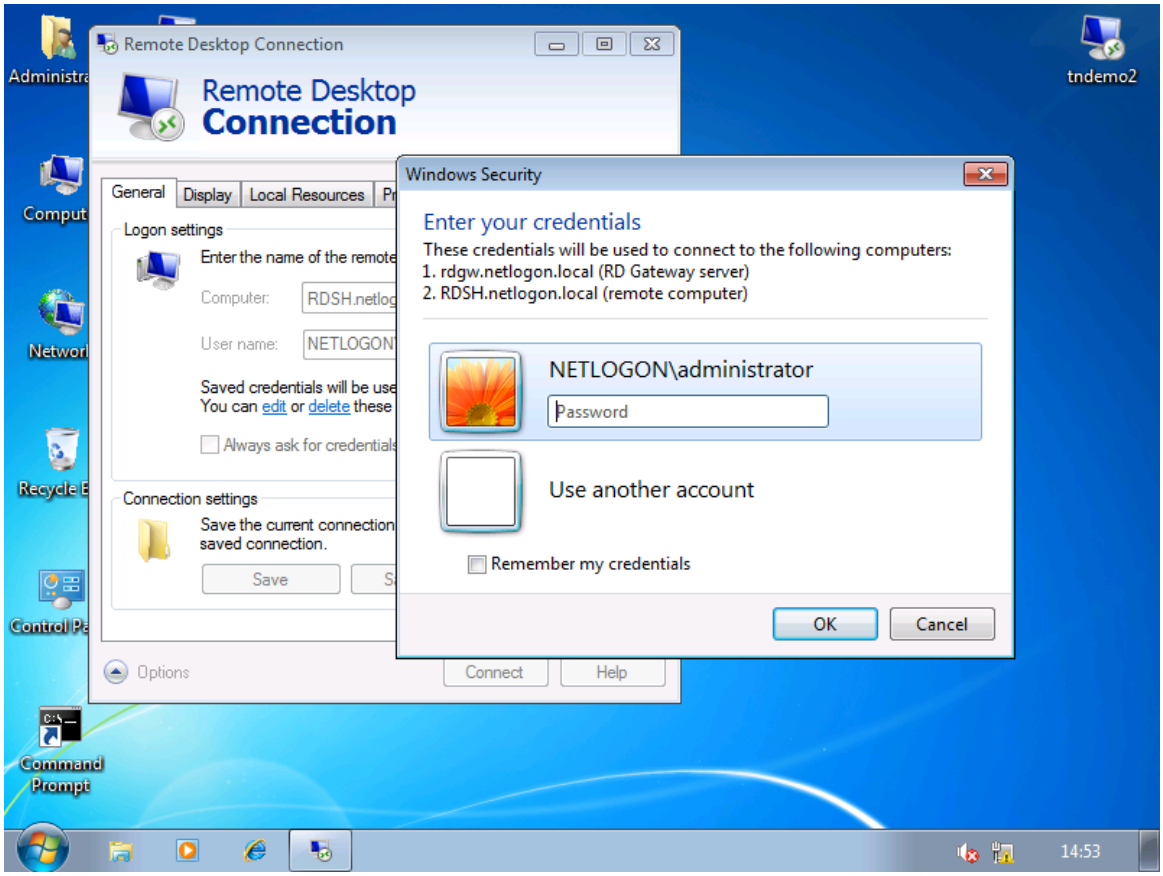
> És ne felejtsük el, amíg ezeket nem gyártjuk le, addig nincs átmenő forgalom az RDGW-n, azaz ha csak feltelepítjük, és az RDSH vagy a RDCB szervereken megjelöljük, hogy használja pl. a RemoteApp a Gateway-t, de nem csinálunk CAP/RAP objektumokat, addig coki!

Az RDGW szerveren végeztünk, most jöhet az RDSH / RDCB szervereken a Gateway konfigurálás, majd sétáljunk el a kliensre, merthogy ezt is fel kell készítenünk! No nem nagyon (és persze tartományi környezetben Csoportházirend is van), de azt azért meg kell mondanunk a Windows 7-nek például, hogy van ám RDGW szerver is.

A következő képen az is látszik, hogy hol.

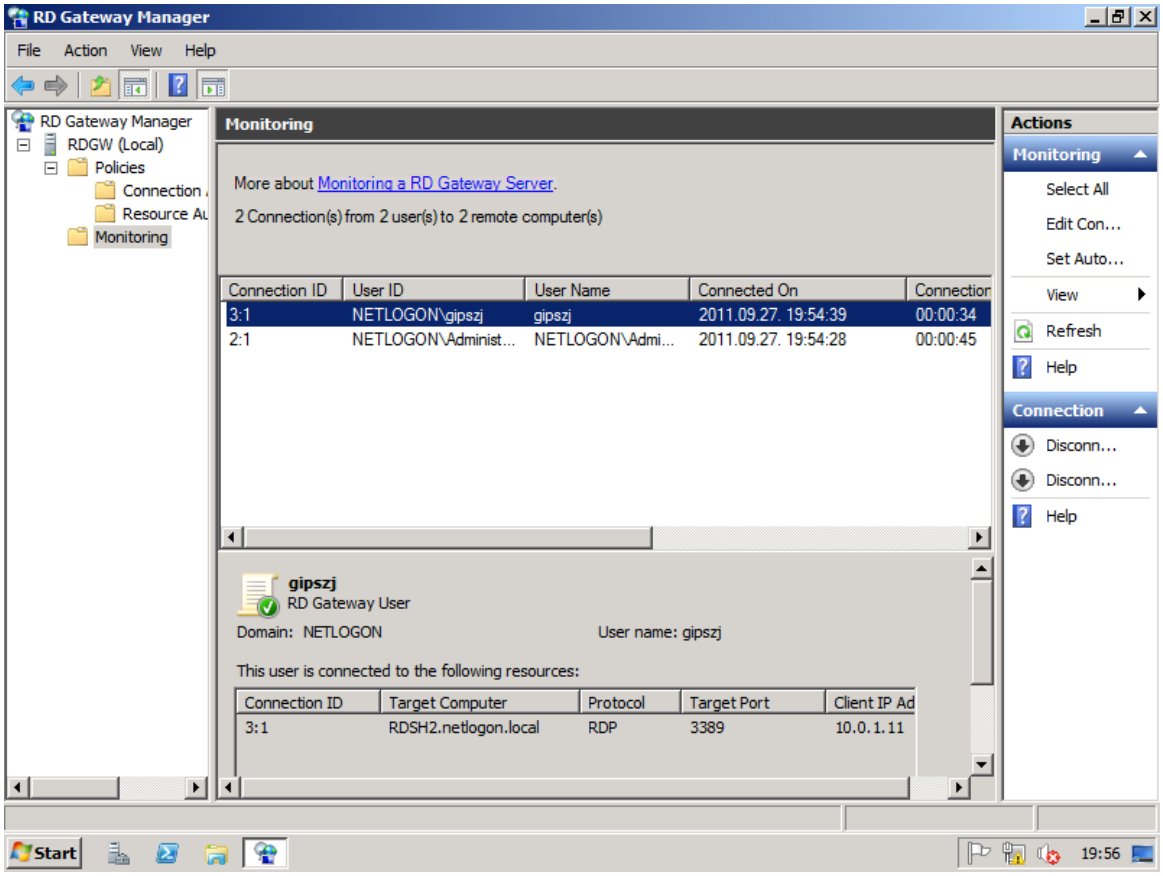


8.53 ÁBRA BEJÖN A KÉPBE AZ RDGW...



8.54 ÁBRA ...ÉS MÁR HITELESÍTÜNK IS ÁLTALA.

Szóval a kliensünk RDP kapcsolatában a legutolsó fülön kell megadnunk, hogy hogyan, milyen jellemzőkkel óhajtunk az RDGW-n keresztül kapcsolódni. Felhívnám a figyelmet a legalsó négyzetre (Use my RD Gateway credentials for the remote computer), amellyel az SSO, azaz az egyszeri/egyszerű belépés áldásos hatása alá kerülhetünk. Ez gyönyörűen látszik a második képen, mikor is megmutatja nekünk a hitelesítő ablak, hogy ezekkel az adatokkal először az RDGW-re, majd aztán a célszerverre fogunk belépni. Ha ehhez minden feltételt megteremtettünk, akkor működni is fog, ahogyan ez a következő képen látszik is az RD Gateway Manager Monitoring menüpontja alatt.



8.55 ÁBRA A 2 DARAB ÁTMENŐ KAPCSOLAT ADATAI

Nem hiszem el, hogy vége ennek a fejezetnek, pedig mégis.

De egy kicsit azért rokon rész következik, hiszen a VDI vagy RAH miatt már úgyis érintettük, és egyébként itt a fejezet végén jól el is árulom, hogy az RDS is egyfajta virtualizáció, mégpedig az ún. prezentáció virtualizáció.

9 Hyper-V

Egy korábbi lábjegyzetben már megemlítettem a virtualizációval kapcsolatos pozitív irányba történő véleményváltozásomat, de az igazsághoz hozzátartozik, hogy annak ellenére, hogy végigütögettem - a Virtual PC-től kezdve, a Virtual Serveren át, a Hyper-V-n keresztül az SCVMM-ig -, az elmúlt sok-sok év rengeteg termékét, mégis ez az a témakör, amit inkább csak *használok*, mint értek. Illetve ez azért nyilván kissé túlzás, de a mélyvízben azért néha kapálódzok kicsit.

> Szóval, aki ettől a fejezettől azt várja, hogy a Hyper-V működésének legmélyebb bugyraiban turkálva, a sarki zöldséges számára is tökéletesen érthetőre fordítom a lényeget (mint remélhetőleg általában), az lehet, hogy csalódni fog. Inkább a gyakorlati dolgokra szeretnék fókuszálni, azaz leginkább az üzemeltetésre, persze azért lesz elmélet is bőven, és kivételesen - és persze engedéllyel[136] – nagyobb tudású szakemberektől is „lopok" néha ebben a fejezetben.

9.1 Mit tud, mire való és mi kell hozzá?

Egy biztos, akár tervező rendszermérnökök vagyunk, akár kreatív fejlesztők, akár kézműves rendszergazdák, akár IT vezetők, e téma mellett elmenni nem lehet és nem is érdemes. Ha több operációs rendszert, több alkalmazást, több gépet akarunk működtetni és mindezt flexibilisen, időt és erőforrást spórolva, és meglehetősen nagy szabadsággal, akkor a virtualizáció tökéletes alternatíva. Ráadásul több területre is átnyúlunk, mivel a virtualizáció a Microsoft egy halom megoldásában is jelen van. Ebben a fejezetben a szerver-virtualizációról (Hyper-V) fogunk megemlékezni, de a téma kapcsán gondolhatunk az alkalmazás-virtualizációra (pl. App-V), a desktop-virtualizációra (Med-V), vagy akár az előző részben emlegetett RDS-re is.

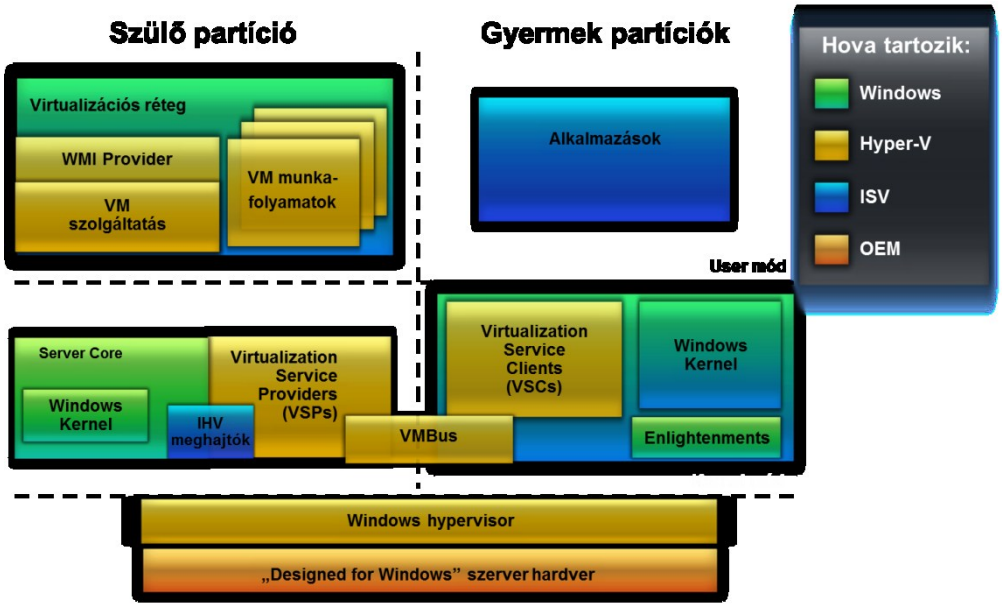
A Hyper-V egy teljesen 64 bites, mikrokerneles hypervisor-alapú virtualizációs megoldás, amely a Windows Server 2008-ban indult el (az RTM-hez képest némi késéssel, ha emlékszünk) az 1.0-ás verzióval. Az R2-ben már 2.0-ás változat van, több komoly újdonsággal, és még mielőtt a 3.0-ás verziót a Windows 8 Server[137]-ben elérnénk, az R2 SP1 is lökött a funkcionalitáson egy kicsit, vagy nem is kicsit.

[136] Bár így tennének mások is, de sajnos nem tesznek így, nincs erkölcs a neten, nekem például kilométeres online hivatkozási jegyzékem lehetne, de csak 10 méteres van ☺.

[137] A könyv írásakor még béta, sőt még az sem (ún. Developer Preview), úgyhogy a név is csak kódnév, később bármi más is lehet.

Viszont a virtualizációval kapcsolatban általában sok a homályos kifejezés is, és kicsit máshogy is kell gondolnunk a gépekre, a hardverre vagy az alkalmazásokra, épp ezért oszlassuk el kicsit a ködöt pár definícióval[138]:

- Hypervisor: A hypervisor egy vékony szoftverréteg[139], ami közvetlenül a hardver és a rajta futó operációs rendszerek között foglal helyet. A feladata, hogy elkülönített futtatási környezeteket biztosítson az összes operációs rendszer számára (ezek lesznek a „partíciók"). Minden partíció csak a saját hardver erőforrásaival rendelkezik (memória, eszközök és a CPU adott időszeletei). A hypervisor ellenőrzi és koordinálja a partíciók hozzáférését a tényleges hardverhez.
- Partíció (Partition): ez a hypervisor által biztosított elkülönítés alapegysége; egy fizikai címtartományból és egy vagy több virtuális processzorból épül fel. A partícióhoz meghatározott hardver erőforrások rendelhetők és az erőforrások eléréséhez szükséges jogosultságok is.



9.1 ÁBRA A HYPER-V FELÉPÍTÉSE

- Szülő partíció (Parent partition): Az a partíció, amelyben dolgozva a gyerek partíciókat létrehozzuk és felügyeljük. Ha nagyon le akarnánk egyszerűsíteni, akkor azt mondhatnánk hogy ez a host gép, de azért nem, mivel a szülő partíció is egy virtuális gép.
- Gyerek partíció (Child partition): A szülőből létrehozott bármely további partíció. A gyerek partíció gyakorlatilag egy virtuálisan definiált hardver.

[138] A szótár eredeti verziója *Somogyi Csaba* cikkéből származik: http://www.microsoft.com/hun/technet/article/?id=2014e837-c995-4025-895e-1d4ca578fb69&media=printer

[139] A hypervisor mérete kicsi: AMD platformon 519KB, Intelen 536 KB.

Általunk megszabott méretű RAM, adott mennyiségű CPU időszelet és virtuális eszközök összessége, és maga a definíció egy darab XML állomány.

- Vendég operációs rendszer (guest): A gyerek partícióban futó operációs rendszer szoftver. A vendég rendszer lehet teljes kiépítettségű (pl. bármely Windows rendszer), vagy akár egy speciális célú kernel is. A hypervisor közömbös a vendég rendszer iránt, csak az erőforrásokat adja számára.
- Eszköz emuláció (Device emulation): Olyan eszköz virtualizációs megoldás, ahol a virtualizált hardver nem különböztethető meg a tényleges fizikai hardvertől (1:1-es megfelelés).
- Szintetikus eszközök (Synthetic devices): Olyan virtuális eszközök, amelyeknek nincs közvetlen fizikai megfelelőjük. Az ilyen eszközök a VMBus segítségével kommunikálhatnak akár más partícióban lévő fizikai eszközökkel is.
- Worker processz: Ebből egy darab minden működő virtuális géphez létrejön a gazda operációs rendszeren. Ez a processz kapcsolja össze a virtuális hardver elemeit, mintha egy virtuális alaplapba rakosgatnánk az alkatrészeket. Ezen felül kapcsolatot épít fel a gazda gép és a virtuális gép között, biztosítva, hogy a gazdagépről irányítani tudjuk a virtuális gép működését. Az irányítás WMI parancsokon keresztül történik, a megjelenítést pedig az RDP protokoll segíti. A Worker processz tartja a kapcsolatot minden szereplővel, figyeli a hardver konfiguráció változását, így ha menet közben átkonfiguráljuk azt, akkor azokat igyekszik érvényre juttatni a hypervisor-on keresztül.

Mi mindenre van szükségünk Hyper-V működéséhez? Nem sok tételből áll a lista:

- Egy 64 bites CPU-ra. Már a Windows Server 2008 esetén is csak a 64 bites változatnál használhattuk a Hyper-V-t, az R2-nél pedig nincs is ugye más.
- Windows Server 2008 / R2 Standard, Enterprise, Datacenter
- A CPU-nál a hardveres virtualizáció támogatás (Intel VT/AMD-V)
- Engedélyezett és bekapcsolt, hardveres Data Execution Protection (DEP) - (Intel XD bit / AMD NX bit)

És amit nyújt, technikai szemmel, felsorolásszerűen és persze az R2-vel számolva:

- 32 és 64 bites virtuális gépek párhuzamos működése
- Egy- és több processzoros (magos) virtuális gépek használata
- 64 processzormag (akár 8x8 mag), SLAT és CPU Core Parking támogatás
- 1 TB fizikai memóriatámogatás
- Maximum 384 futtatható virtuális gép és maximum 512 virtuális processzor
- 256 TB lemezterület LUN-onként
- Pass-through[140] lemeztámogatás 256 TB LUN-ig
- 16 node-os fürt, maximum 1024 virtuális géppel
- Cluster Shared Volumes (CSV) használat, Quick és Live Migration támogatás

[140] Ez az a helyzet, amikor egy fizikai diszket dedikálva adunk oda egy virtuális gépnek, ami a leggyorsabb diszk sebességet jelenti.

- Multipath IO támogatás
- Virtuális hálózati kapcsoló (switch) használata, 10 GBitE támogatás
- Virtuális gépek pillanatnyi állapotának mentése (snapshot), és visszaállítása
- MMC 3.0 felügyeleti eszköz, WMI interfész (szkriptelés, felügyelet)

És most koncentráljunk egy kicsit a szerver-virtualizációra és nem felsorolásszerűen az előnyökre, azaz pontosan milyen helyzetekben lehet hasznos a Hyper-V nekünk?[141]

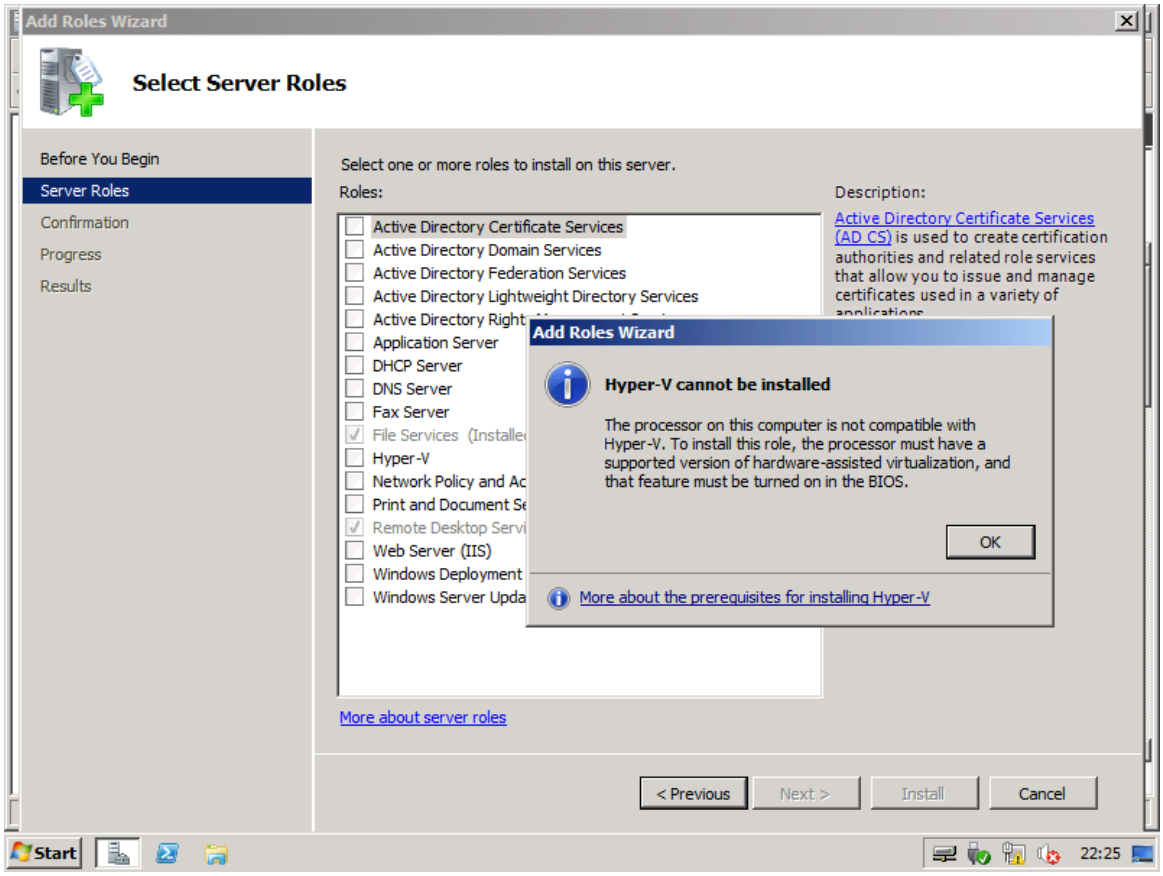
- Szerverkonszolidáció: a szerver hardverek a legritkább esetben vannak folyamatosan kiterhelve a lehetőségeik határáig. Minden szolgáltatás máskor és eltérő mennyiségű számítási teljesítményt illetve erőforrásokat igényel. Érdemes ezeket a különféle szolgáltatásokat minél kevesebb fizikai vasra központosítani, és azok skálázhatóságát és rendelkezésre állását biztosítani.
- A szolgáltatások folyamatos működésének biztosítása: a cél itt igencsak egyszerű: szeretnénk minimalizálni mind a tervezett, mind a be nem tervezett rendszerleállások idejét. Minél kevesebbszer álljon le a rendszer, de ha le is áll, gyorsan helyre tudjuk azt állítani! Virtualizációval mindez könnyen megvalósítható, hiszen mind a fürtözésre, mind a virtuális lemezek és gépek replikációjára és mozgatására is számtalan megoldás áll rendelkezésünkre, amihez egészen kényelmes rendszerfelügyeleti megoldások is elérhetőek már.
- Dinamikus adatközpont: lehetőségünk van arra is, hogy az egy vasra konszolidált operációs rendszerek, illetve szolgáltatások között rugalmasan mozgathassuk az erőforrásokat, például a rendelkezésre álló memóriát, illetve a számítási kapacitást. Ha több szerverünk van, igény szerint másolhatjuk, mozgathatjuk köztük a virtualizált gépeinket is.
- Fejlesztési és tesztkörnyezet: könnyen építhetünk olyan virtuális tesztkörnyezeteket, amelyekkel bármilyen tesztelési célokat megvalósíthatunk. Ezek a virtuális környezetek nem kell, hogy külön fizikai szerverekre kerüljenek – elférhetnek a már használatban lévő szervereken is, és mivel csak a teszt idejére van rájuk szükség, így erőforrásigényük is csak ideiglenes. A virtualizációnak köszönhetően tökéletesen izolálhatjuk ezeket a tesztrendszereket a valódiaktól (egy hardveren belül is!), de ha pont ennek az ellenkezőjére van szükségünk (például egy migráció tesztelésekor szeretnénk elérni az aktuális rendszert is), az is könnyen megvalósítható.

Nos, ennyi a bevezetéshez szükséges adat és elmélet után nézzük meg a Hyper-V kezelésére mindennaposan használt eszközünket, a Hyper-V Manager-t!

9.2 A KONZOL ÉS A VIRTUÁLIS GÉPEK KEZELÉSE

[141] A következő négy bekezdés *Budai Péter* műve, egy régi-régi Technet Magazinból.

Ha Hyper-V-t szeretnénk használni, és megfelel a gépünk a követelményeknek, akkor szokásosan a Server Manager-ben kezdünk, mivel a Hyper-V egy szerepkör.
A telepítés nem bonyolult, rész-szerepkör vagy egyéb képesség nem kell hozzá, magányos farkas. Ugyan a hálózati interfészre vonatkozóan kapunk egy kérdést, de ezt bőven ráérünk elhalasztani.



9.2 ÁBRA EZ ÍGY NEM OK (ÉRTELEMSZERŰEN VIRTUÁLIS GÉPRE NEM RAKHATOK HYPER-V-T)

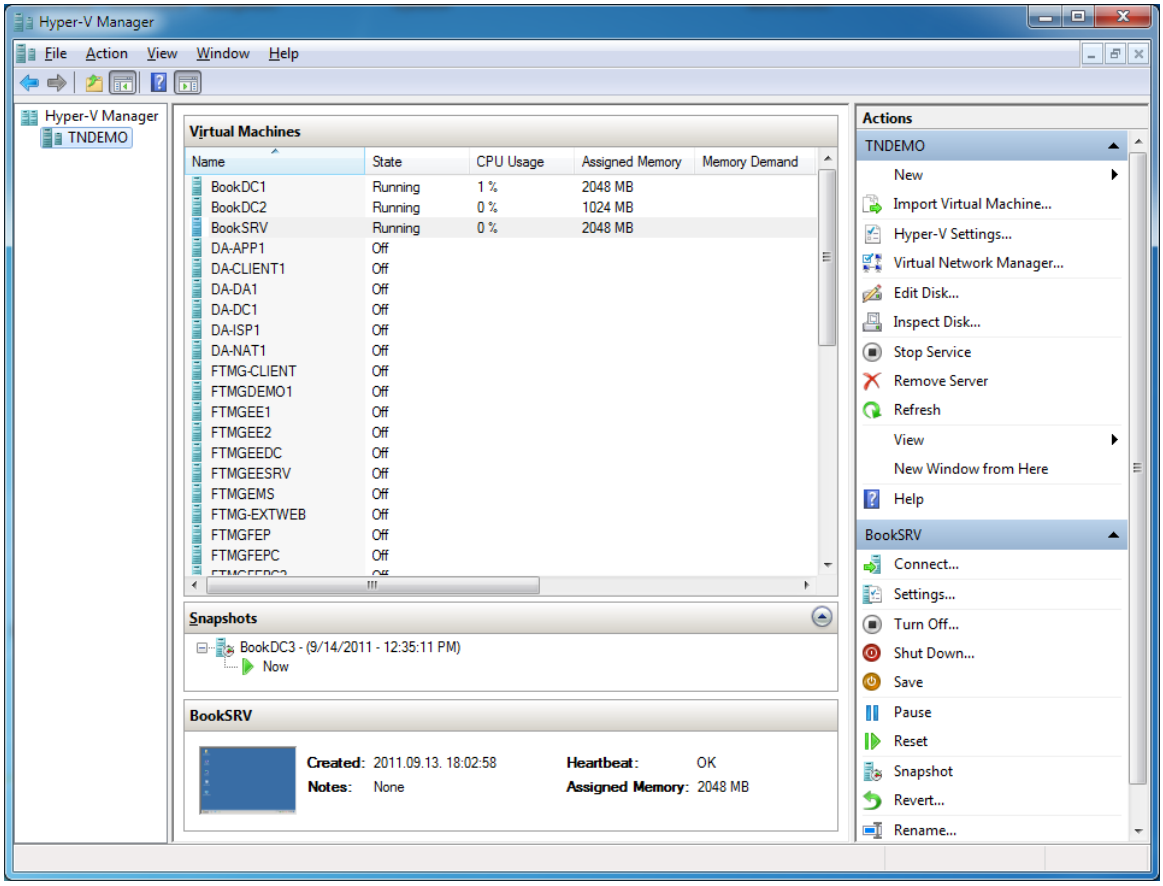
A szerepkör a teljes GUI-s kiszolgálóra történő telepítésekor a kezeléshez szükséges eszköz, a Hyper-V Manager egyből felkerül, viszont Server Core vagy a Hyper-V Server esetén nem, és nem is lehet. De távolból igen, mindhárom szerver üzemmód esetén és erre 2 megoldásunk is van, tipikusan mindkettő tartományban egyszerűen elérhető, munkacsoportos környezetben már kevésbé, mivel a jogosultságok delegálása kissé körülményes[142]:

1) A Server Manager-ben a képességek között találunk egy Hyper-V Tools-t, így ha az egyik szerverről a másikra szeretnénk a kezelést megoldani, akkor ezt kell telepíteni és használni.

142 http://blogs.technet.com/b/jhoward/archive/2008/03/28/part-1-hyper-v-remote-management-you-do-not-have-the-requested-permission-to-complete-this-task-contact-the-administrator-of-the-authorization-policy-for-the-computer-computername.aspx

2) És erre a célra szolgál az RSAT csomag pl. egy Windows 7-en, amelynek szintén van egy Hyper-V Tools MMC-je.

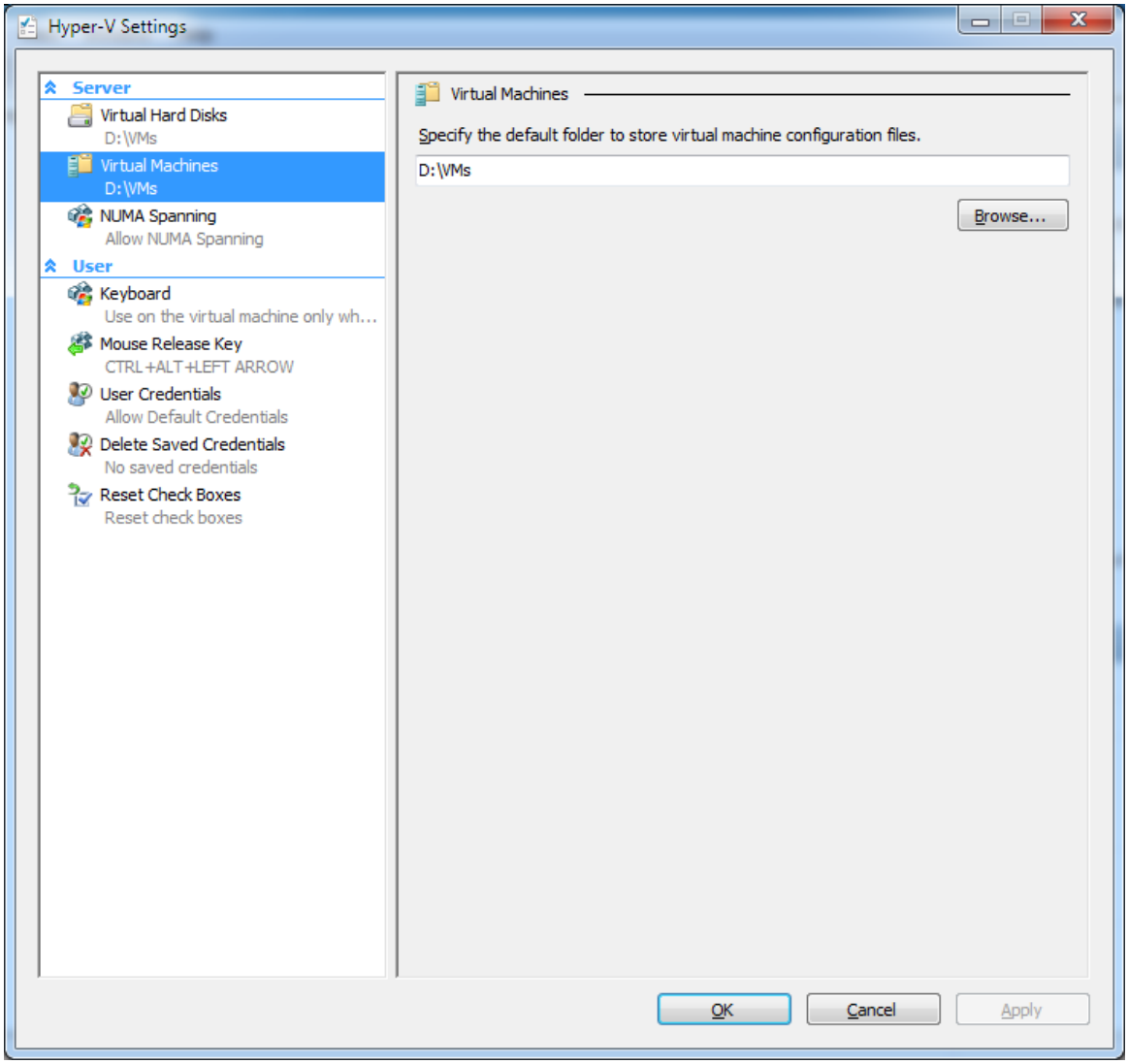
> No és persze méretesebb környezetben, több Hyper-V szervert felügyelve és irányítva, központosított feladatokat ellátva az SCVMM-nek nem lesz párja.



9.3 ÁBRA A HYPER-V MANAGERBEN IS LEHETNE TÖBB KISZOLGÁLÓNK IS, A BAL OLDALI KERETBEN

A Hyper-V Manager-rel a szülő partíció operációs rendszeréből kezelhetjük a gyermek partíciókat (a guest-eket, azaz a virtuális gépeket). Itt hozhatjuk létre ezeket, itt törölhetjük, állíthatjuk be a jellemzőiket. A középső, domináns keretben a virtuális gépeket és pillanatnyi állapotukat, a memória és CPU fogyasztást, stb. látjuk. A teendők a jobb oldali keretben jelennek meg, egyrészt felül a komplett Hyper-V-re vonatkozóan, másrészt alul az adott virtuális gép viszonylatában.

Az első leselkedés után nézzünk be a globális tulajdonságok közé, ezt az adott Hyper-V szerver helyi menüjében a Hyper-V Settings-et kiválasztva érhetjük el.



9.4 ÁBRA KEZDJÜK ITT

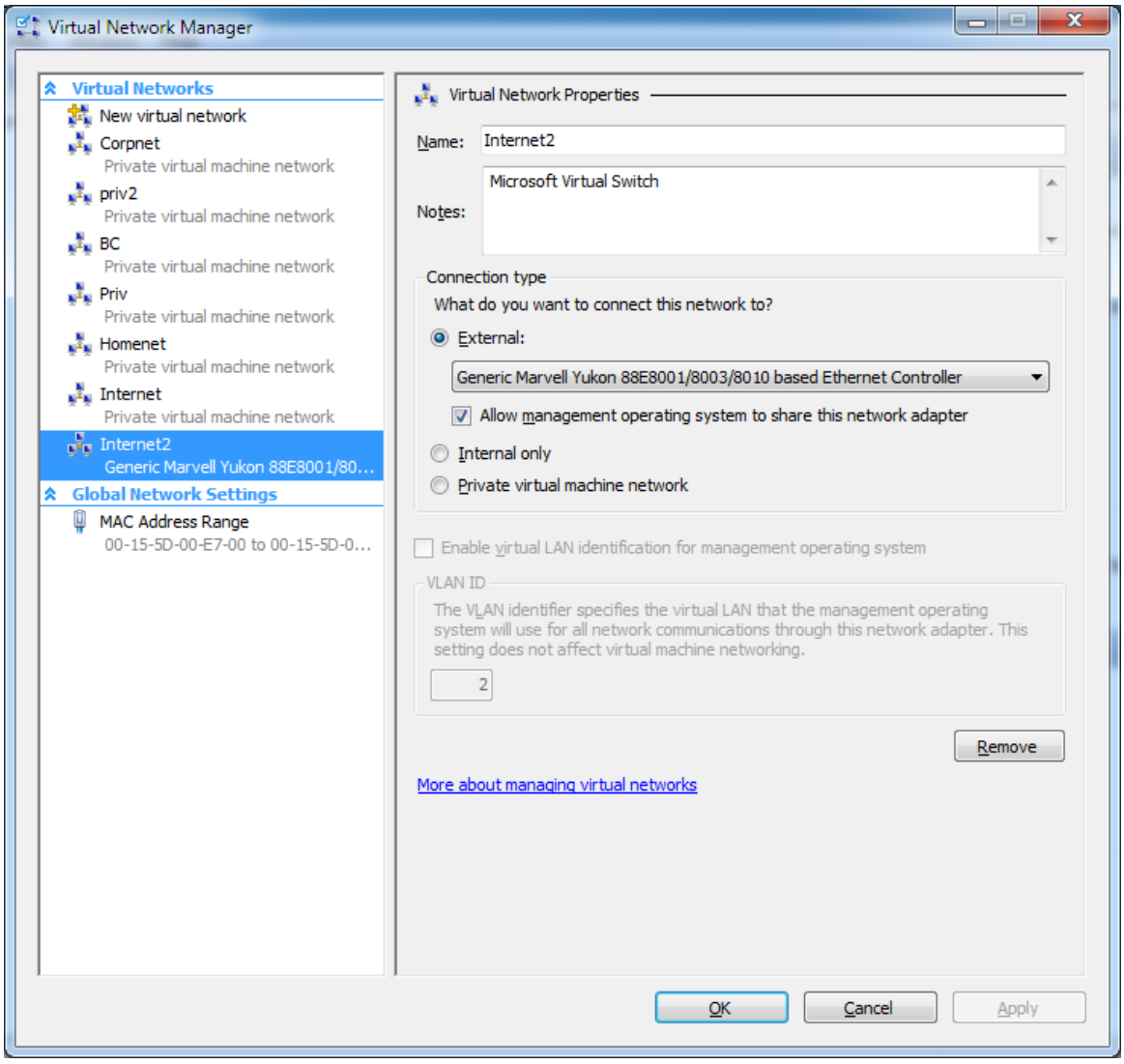
Az elején a kiszolgálóra vonatkozó beállítások jönnek szembe, pl. a leendő virtuális gépek .vhd fájljainak és konfigurációs fájljainak alapértelmezett helyét tudjuk módosítani, illetve a NUMA Spanning (Non-Uniform Memory Architecture [143]) engedélyezése is itt található. Aztán pedig kisebb jelentőségű beállítások jönnek, mint pl. a billentyű kombinációk használatának körülményei vagy az egérkurzor elengedése[144] (ha nincs integrációs komponens telepítve).

Ellenben egy ezeknél lényegesen fontosabb részt is célszerű még a virtuális gépek létrehozása előtt konfigurálni,mégpedig a virtuális hálózatokat. Az ún. virtuális

[143] Bizonyos (igen komoly) kiszolgáló hardver esetén Hyper-V alatt egy virtuális gépnek meg lehet adni, hogy mely NUMA node-on működjön. Ti a NUMA egy olyan spéci memória architektúra, amely a multiprocesszoros rendszerekben használatos, és a CPU-knak saját, a közös rendszer memóriától elkülönített memória területe is lehet.

[144] Ezt annyira nem nevezném apróságnak, egy rosszul konfigurált egérkurzor képes az őrületbe kergetni az admint (a lektor megjegyzése).

switchek konfigurációja szintén az adott Hyper-V szerver helyi menüjében található (Virtual Network Manager). Itt három, egymástól teljesen eltérő virtuális hálózat típus áll rendelkezésünkre, amelyek egyik közös jellemző viszont az lesz, hogy akár többet is létrehozhatunk belőlük (lásd következő kép).



9.5 ÁBRA A MEGFELELŐ HÁLÓZATI BEÁLLÍTÁS A KULCS MINDENHEZ

- Private: kizárólag a virtuális gépeink közötti hálózati kapcsolatok kialakítására nyújt lehetőséget, se a szülő felé, sem egy külső kapcsolat felé nem lehetséges kapcsolódni. Így lehet például kellemesen szeparálni egymástól akár teljesen ugyanolyan IP konfigurációval tesztrendszereket (persze ha nincs szükség külső kapcsolatra).
- Internal: Az adott Hyper-V szerver gépei és a szülő operációs rendszer, valamint az ugyanazon a fizikai szerveren futó virtuális gépeink közötti hálózati kapcsolat kialakítására szolgál.
- External: Ezen a virtuális switch-en keresztül csatlakoztathatjuk a virtuális gépeinket a rendszerünk nem virtualizált részébe. Az ilyen típusnál a virtuális hálózathoz kötelező hozzárendelni fizikai gép egyik hálózati kártyáját.

- Az „Allow management operating system to share this network adapter” bepipálása azt teszi lehetővé, hogy ugyanazon a hálózati kártyán „lásson ki” a szülő partíció és a virtuális gépek is. Tehát, ha pl. egyetlen egy hálózati kártyánk van, akkor ha ezt az opciót levesszük, akkor csak a virtuális gépek látják majd ezt a hálózati kártyát, a host OS nem, tehát pl. a felügyelet kissé körülményes lesz[145]. Épp ezért legyen több hálózati interfészünk egy Hyper-V esetén, mivel az ajánlás pont azt mondja, hogy dedikáljunk a virtuális gépeknek külső interfészt a fizikai hálózat felé, és ne kapcsoljuk be ezt az opciót.
- Amennyiben nem lehetséges a fizikai hálózati interfész szintjén elválasztani egymástól a fizikai gép és a virtuális gépek hálózatát, akkor használjunk több VLAN-t, és adjuk meg annak az azonosítóját (VLAN ID), amelyet a fizikai OS elérésére szeretnénk használni.
- Több ilyen külső hálózatot is létrehozhatunk, de egy adaptert, kizárólag egyetlen external virtuális hálózathoz rendelhetünk hozzá.

> A hálózati beállítások legalján (és csak az R2-ben) látható a választható MAC Address tartomány (MAC Address Range), amelyből majd a virtuális gépeink számára kerülnek - dinamikusan - kiosztásra a címek.[146]

Van még 1-2 menüpont az adott Hyper-V kiszolgáló helyi menüjében, de ezek vagy később lesznek majd igazán aktuálisak (Edit/Inspect Disk), vagy magától értetődőek (pl. Remove Server vagy a View). Úgyhogy haladjunk tovább, és nézzük meg, hogy hogyan hozhatunk létre egy virtuális gépet!

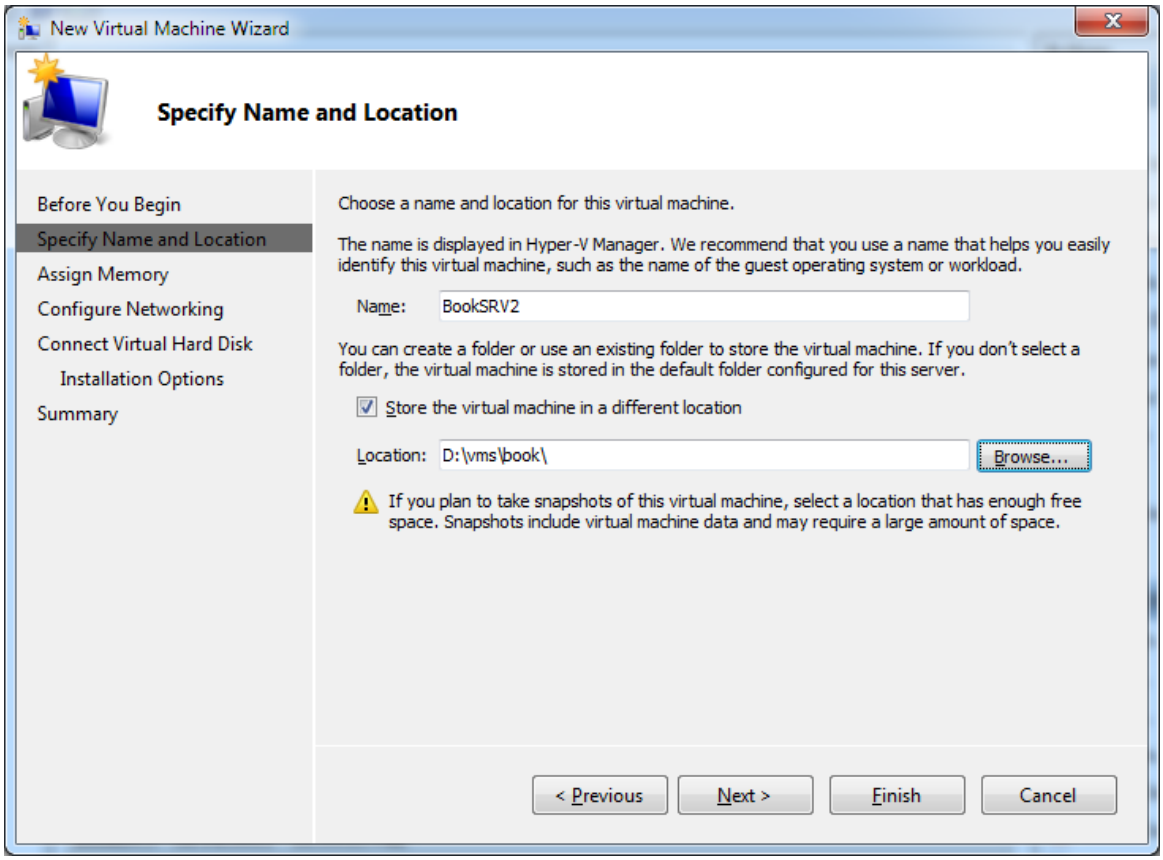
9.3 Egy virtuális gép létrehozása

Legalább háromféle módon juthatunk új virtuális gép birtokába:

1. Telepítünk egy teljesen új virtuális gépet, egy teljesen új virtuális lemezzel, a szokásos OS telepítési módszerrel
2. Rendelkezünk egy másik Hyper-V „alól” kiexportált géppel (amelyhez egy konfigurációs fájl és egy vagy több diszk is tartozik), és ezt beimportáljuk
3. Rendelkezünk egy sysprep-elt lemezképpel, és ebből (ha okosan akarjuk csinálni) egy differenciális lemezzel hozunk létre telepítés nélkül egy vagy akár több új virtuális gépet

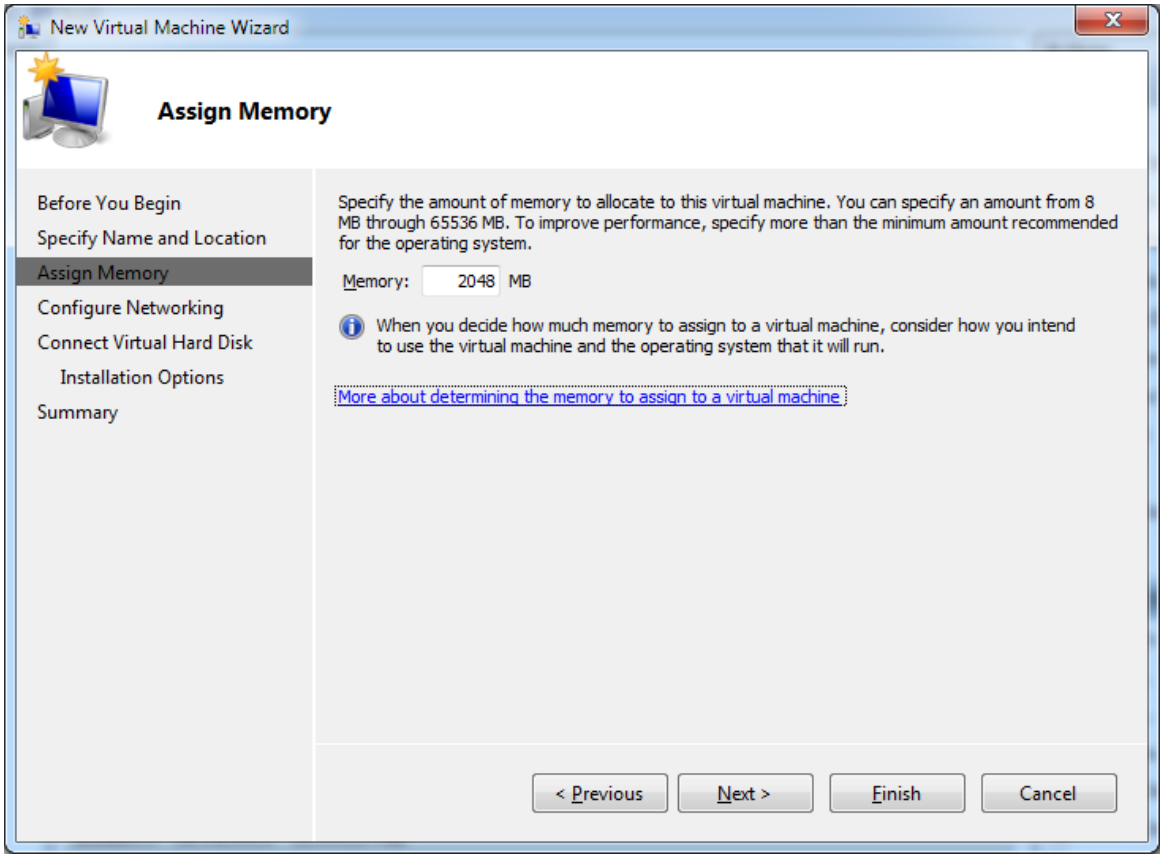
[145] Az ilyen környezetet „headless” környezetnek nevezzük. Szerverekbe beépített rendszerfelügyeleti kártyával működtethető (a lektor megjegyzése).
[146] Több Hyper-V host esetén (SCVMM nélkül) átfedések lehetnek. Azonos MAC című gépek nem kommunikálhatnak egymással, több host esetén, de SCVMM hiányában nekünk kell gondoskodnunk a MAC címek hostokon átívelő egyediségéről (a lektor megjegyzése).

Nézzük sorban! Az egyes módszer a legegyszerűbb, de pl. sok gép esetén nagyon fárasztó, és semmilyen könnyebbséget nem hordoz magában. E módszer szerint egy új virtuális gépet és egy vagy több új virtuális diszket fogunk létrehozni, és aztán megkezdjük az OS telepítését. A folyamatot az adott Hyper-V szerver helyi menüjében, a „New” pontra kattintva kezdeményezhetjük (itt az új virtuális gép mellett akár egy új virtuális diszket, vagy éppen egy virtuális floppy is létrehozható egyébként).

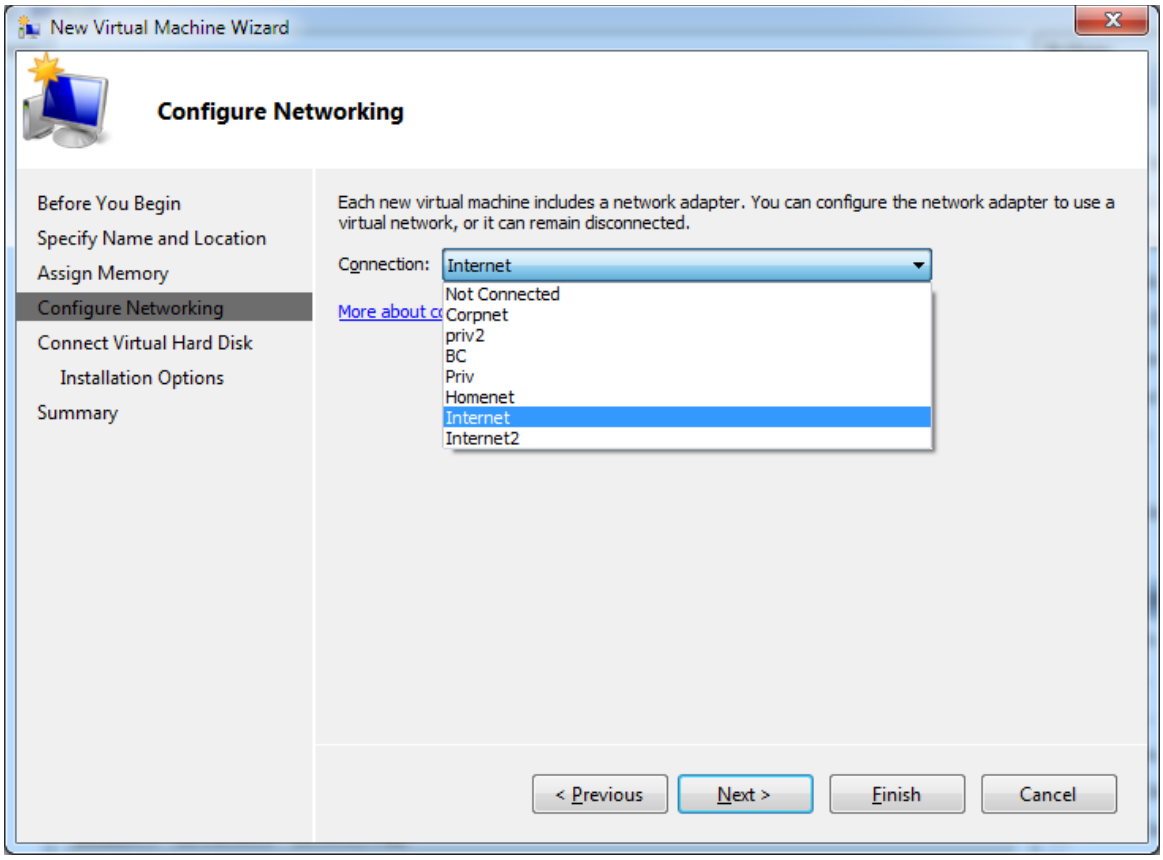


9.6 ÁBRA NEVEZZÜK ÉS HELYEZZÜK EL A GÉPÜNKET

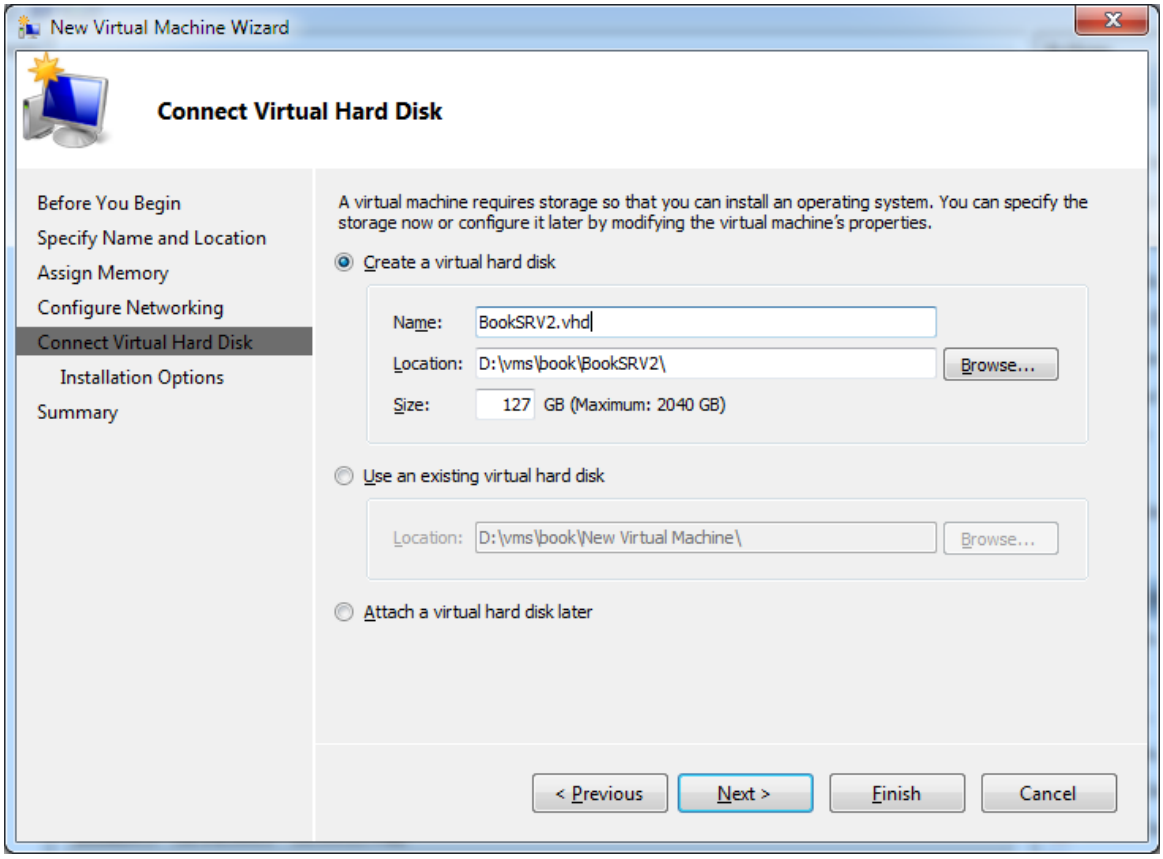
Ezután jönnek sorban a hardveres jellemzők, RAM, hálózat, diszk, stb., viszont a CPU konfigurációt az új virtuális gép varázslóban nem módosíthatjuk, alapértelmezetten egyet kap a gépünk, de ahogy minden mást, amit eddig beállítottunk, természetesen ezt is megváltoztathatjuk – majd a varázsló befejezése után.



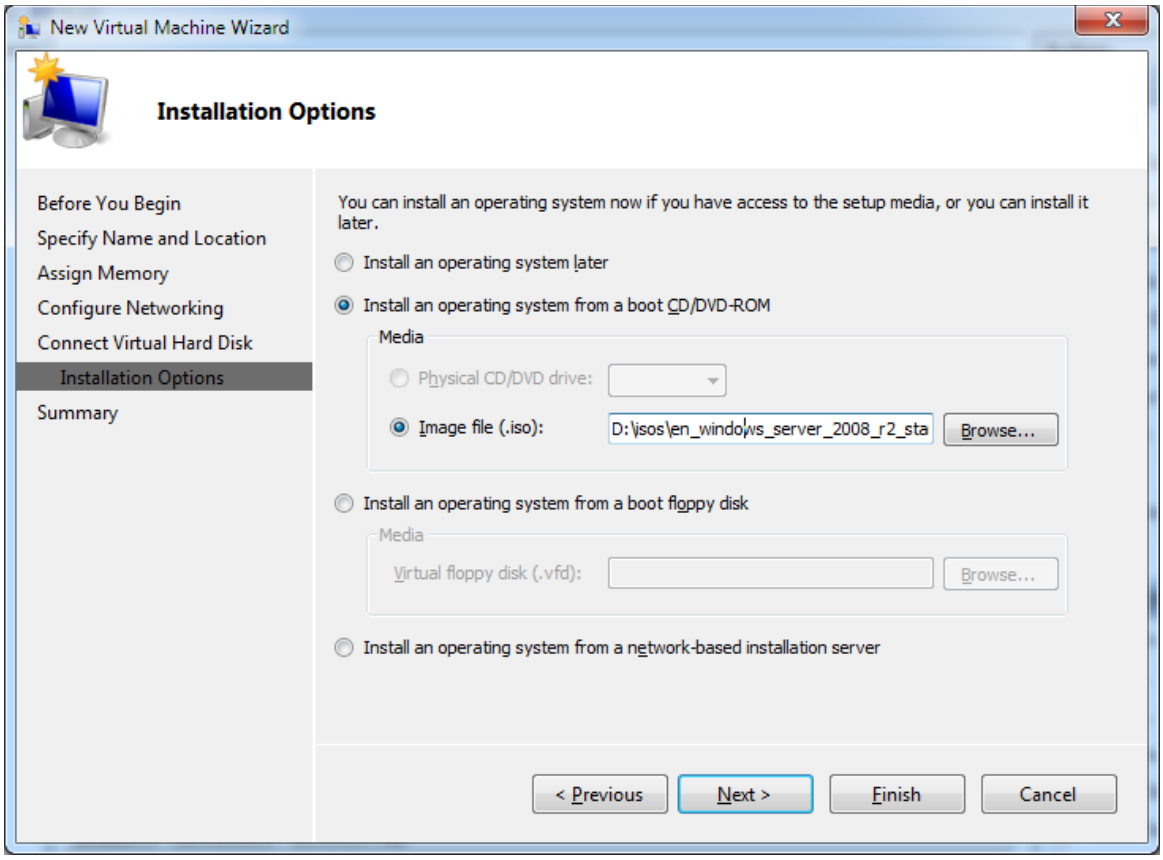
9.7 ÁBRA A RAM HOZZÁRENDELÉSE



9.8 ÁBRA A SWITCHEK



9.9 ÁBRA LEMEZKEZELÉS



9.10 ÁBRA ADJUK MEG A TELEPÍTŐ MÉDIÁT, MAJD A FINISH-RE KATTINTVA VÉGEZTÜNK IS

A lemezek kiválasztásánál (9.9 ábra) álljunk meg egy kicsit, mivel itt több lehetőségünk van: új .vhd-t hozunk létre, vagy egy létezőt használunk (mert már korábban csak a diszket létrehoztuk), vagy egyelőre lemez nélkül hozzuk létre a virtuális gépet. Most mi az alapesetet választjuk, mert teljesen szűz lesz a gép, de pl. semmi akadálya nincs annak, hogy a későbbiekben további diszkeket is csatlakoztathassunk.

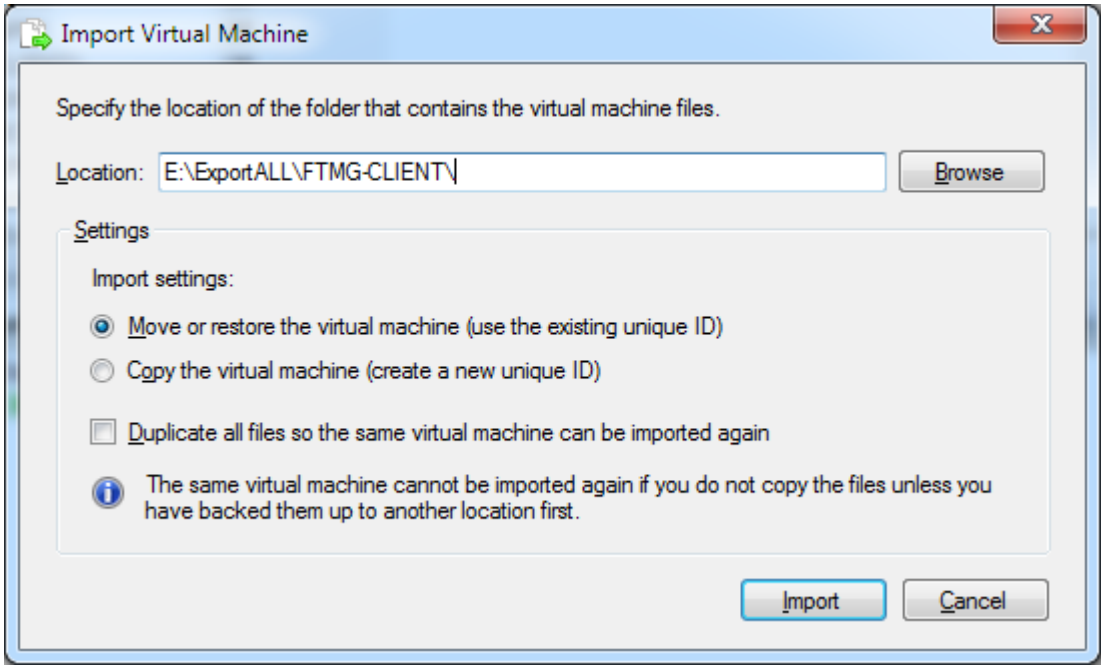
A következő ablakban (9.10 ábra) a telepítő média megadása a feladat. Ez lehet egyrészt egy később eldöntendő dolog, másrészt lehet egy fizikai CD/DVD meghajtó, vagy lehet egy .iso fájl is (én ezt választottam). Szélsőséges esetben tolhatjuk egy floppyról is a telepítőt, illetve PXE boot-tal egy hálózati telepítést is megvalósíthatunk[147].

Nos, ez volt az első módszer, és ha elindítjuk a virtuális gépet, elindul egy normális, hétköznapi operációs rendszer telepítés.

A másodikhoz viszont merüljünk el kicsit az export/import lehetőségekben. Ezt a virtuális gépek másik fizikai Hyper-V szerverre, másik diszkre történő áthelyezésére, esetleg egy adott állapot hosszabb távú lementésére (archiválás) használhatjuk. Vegyük figyelembe, hogy csak és kizárólag leállított állapotú gépet tudunk exportálni! Viszont ekkor már egyszerű lesz, a virtuális gépen jobb gomb és Export, majd adjuk meg a célhelyet, és a virtuális gép diszk méretétől függően pár perc alatt készen is vagyunk (minden virtuális gép állapotsorának az utolsó eleme a „Status”, ebben látjuk az export százalékos állapotát).

Az importnál azért már van több lehetőségünk is. Ehhez megint csak a Hyper-V szerver helyi menüjében keressük meg az „Import Virtual Machine” menüpontot!

[147] De csak egy „Legacy” típusú hálózati adapterrel (a lektor megjegyzése).



9.11 ÁBRA A MAPPÁT KELL BELŐNI

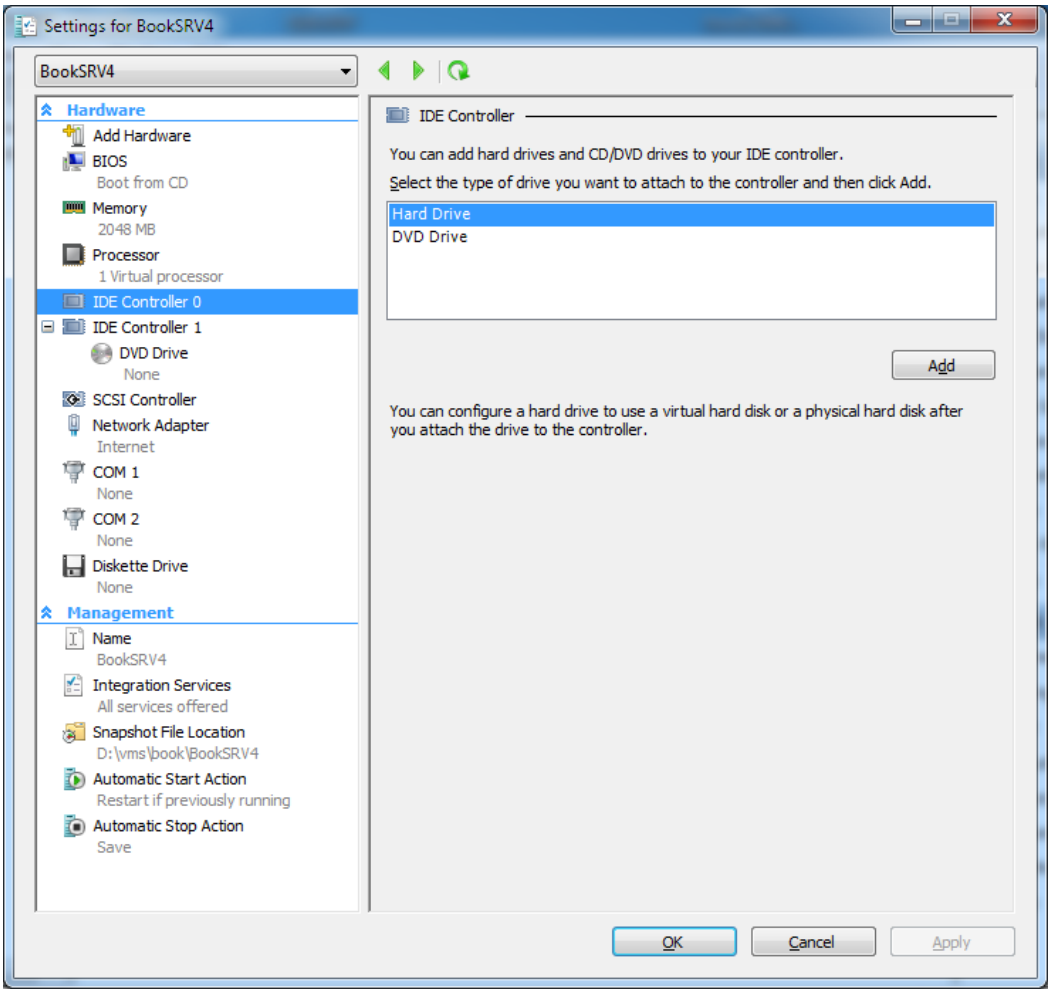
Ha betallóztuk a mappát, akkor el kell döntenünk, hogy ez egy egyszeri import lesz-e vagy esetleg egyfajta sablonként akarjuk használni a korábban kiexportált gépet.

A csak és kizárólag az R2 alatt megjelenő „Duplicate all files…" opció kiválasztása esetén (és persze a „Copy the virtual machine (create a new unique ID") használata mellett) lehetőségünk nyílik egy korábban exportált gép többszöri importálására. Ezen új opció segítségével egy előre definiált, konfigurált, előkészített és exportált virtuális gépet (master image) többször is felhasználhatunk, így egy új kiszolgáló néhány percen belül a rendelkezésünkre állhat. Ha nem ezt a lehetőséget választjuk, akkor az import folyamat az echte exportált fájlokat használja fel a virtuális gépünkhöz, és ezt a vhd-t fogja elindítani, tehát ezt az exportot összesen egyszer tudtuk beimportálni.

> Az exportnál elvileg minden jellemzőnek és tulajdonságnak passzolnia kell az export és az import Hyper-V gépek tekintetében. Természetesen egy az eredeti gépbe becsatolt, de az új helyen nem létező .iso fájl, vagy egy eltérő nevű hálózati switch esetén nem fog meghiúsulni az export, viszont egy figyelmeztető hibaüzenetet kapunk erről. Sajnos a konkrét hibát nem írja bele a Hyper-V ebbe az üzenetbe, viszont az Eseménynaplóban, az „Applications és Services Logs\Microsoft\Windows" naplók között a Hyper-V-VMMS naplófájlban konkrétan meg fogjuk találni, hogy mi fáj neki.

A harmadik módszer kicsit hasonlít a kettes végéhez, és ugyanúgy azt a célt szolgálja, hogy egyszerűbb legyen sok gépet létrehozni. Egy korábban létrehozott (és írásvédetté tett) sysprep-elt .vhd fájlt fogunk használni, ráadásul helytakarékos

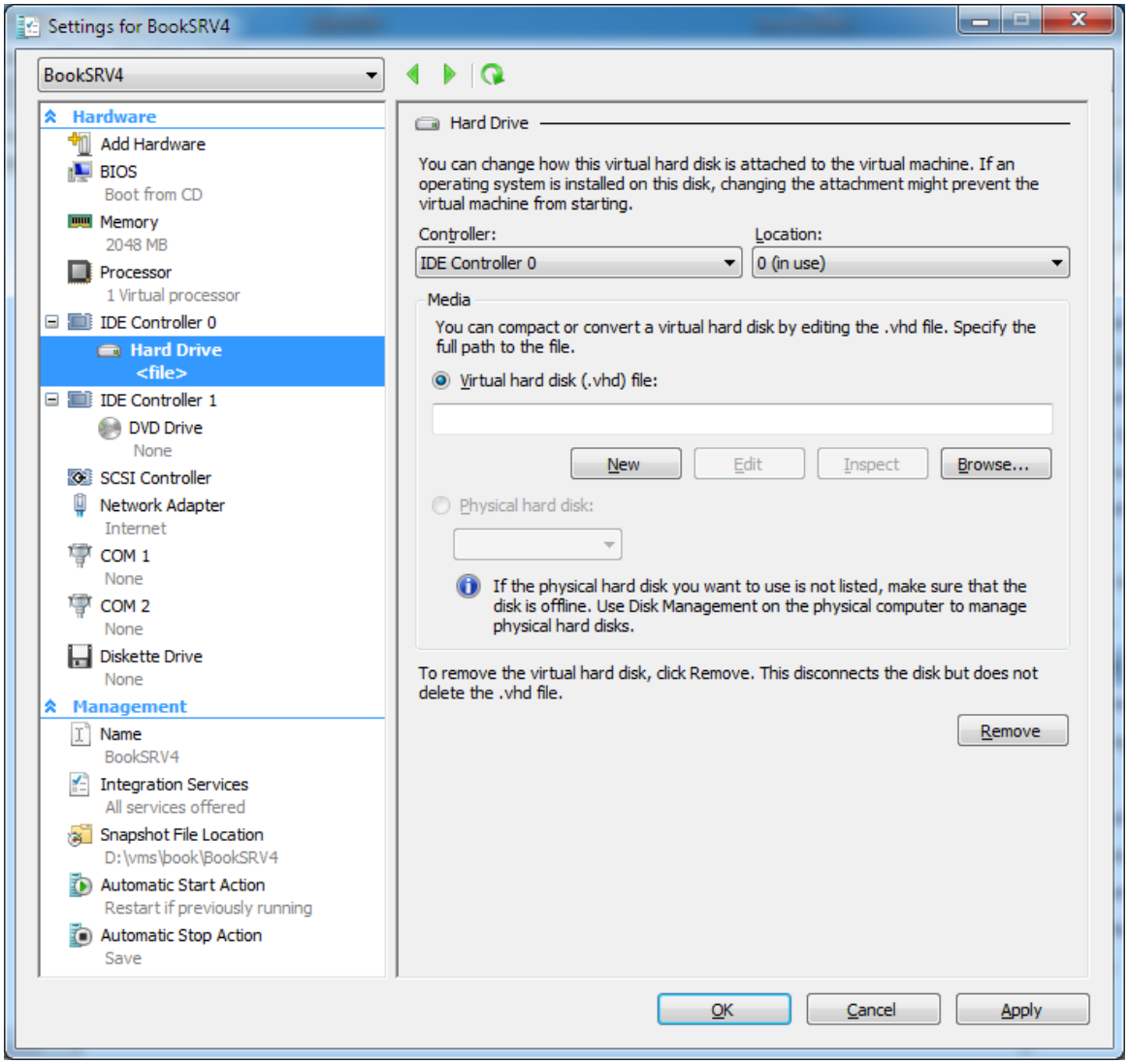
módon, tehát mint különbségi (differencing) diszket. Így aztán ha 10 gépet akarunk létrehozni, akkor 11 db .vhd fájlunk lesz: 1 nagy méretű szülőlemez (ez a sysprep-elt image) és 10 db különbségi lemez (valószínűleg egészen kicsik). Ezzel a módszerrel rengeteg helyet spórolunk meg, igaz, mivel *„ingyenebéd nincs”*, ez kissé a sebesség rovására megy majd, illetve hosszútávon a differenciális lemezre gyűjtött változások mérete mégiscsak meghaladhatja a dinamikus/fix méretű lemezek méretét.



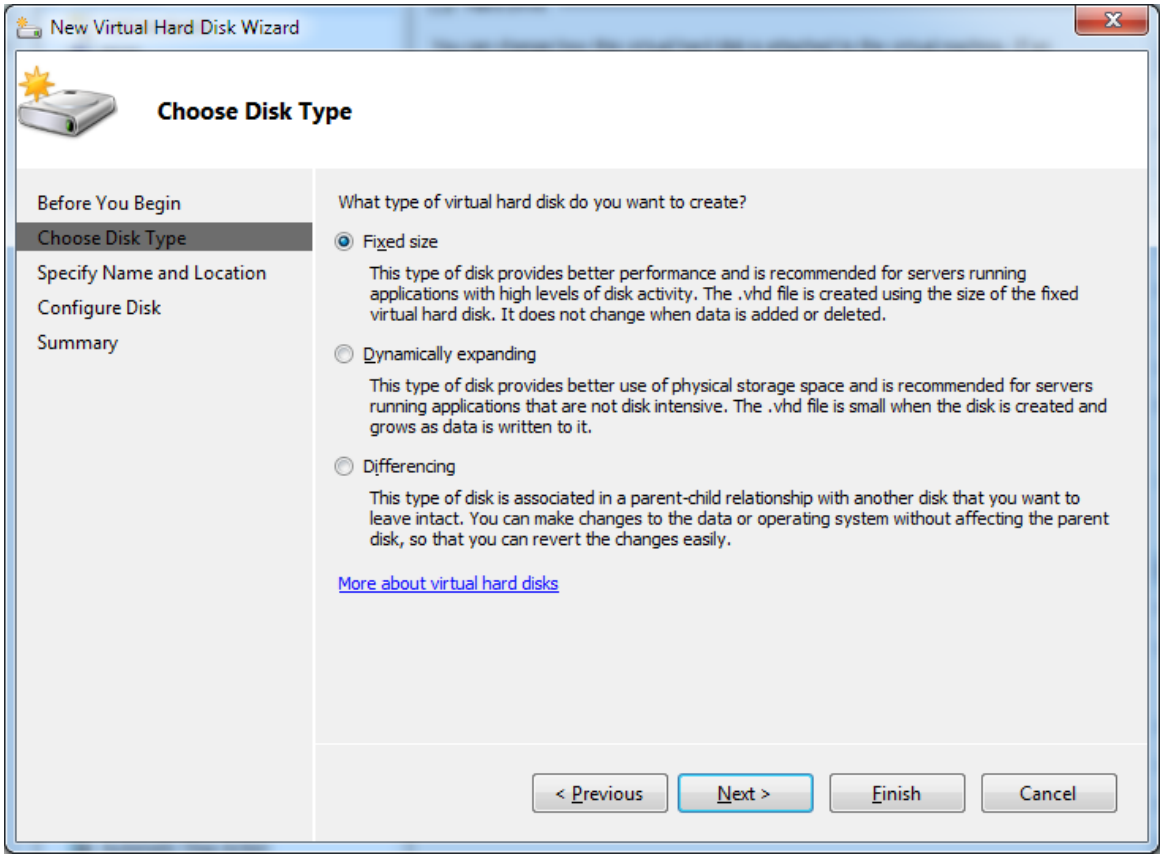
9.12 ÁBRA VÁLASSZUK AZ ÚJ HDD-T

Ezt viszont az új gép varázslóban nem tudjuk bevinni (9.9), ezért ilyenkor válasszuk nyugodtan a döntés elhalasztását („Attach a virtual disk later”)! Így akkor lesz csak lemezünk, ha már kész a gép, de még „üres”.

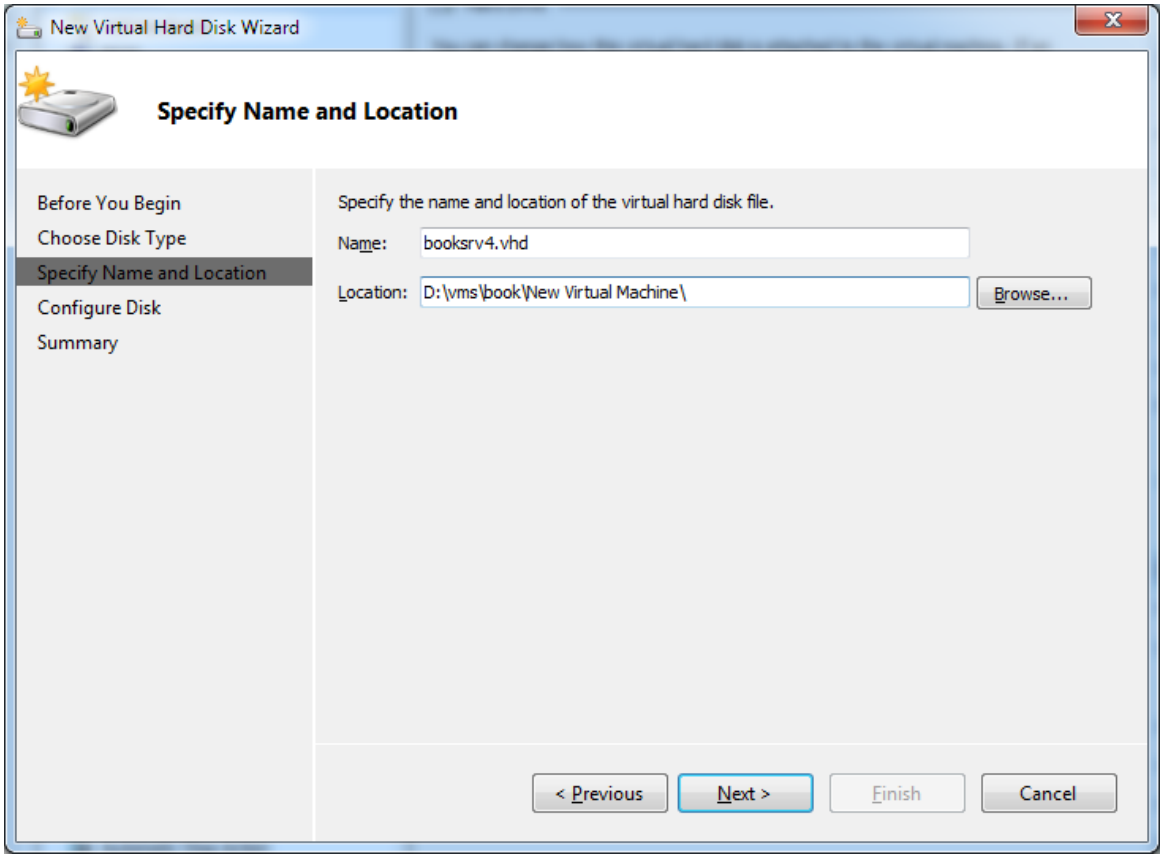
Válasszuk ki tehát a kiválasztott virtuális gép tulajdonságait (helyi menü > Settings), majd keressük meg az „IDE Controller 0” pontot.



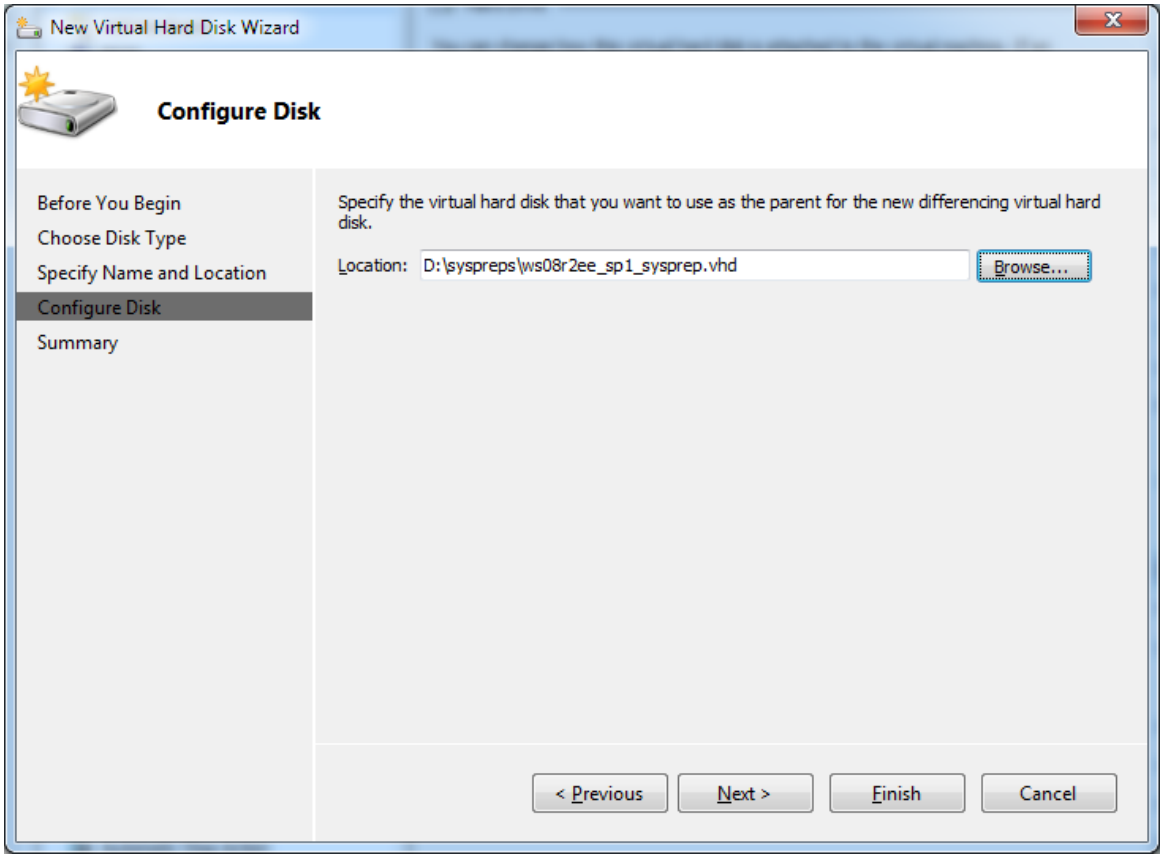
9.13 ÁBRA LEGYEN ÚJ



9.14 ÁBRA A LEMEZTÍPUSOK: A FIX GYORSABB LESZ, DE VALÓSZÍNŰLEG PAZARLÓ, A DINAMIKUS KÉNYELMES ÉS KISEBB HELYFOGLALÁSÚ, DE LASSÚBB, A DIFFERENCIÁLIST MEG LÁSD AZ ELŐZŐ OLDALON



9.15 ÁBRA A KÜLÖNBSÉGI LEMEZ ELNEVEZÉSE ÉS ELHELYEZÉSE



9.16 ÁBRA A KORÁBBAN ELKÉSZÍTETT SYSPREP-ELT SZÜLŐ DISZK HELYE ÉS NEVE, MAJD FINISH

Ezután, azaz a gép elindítása után a sysprep-et követő első indítás mindig egy rövid utótelepítés, amely után viszont kapunk egy már kész operációs rendszert. Amit innentől a virtuális gépben változtatunk, az csak a saját diszkjében történik meg.
Nos, ezzel a harmadik módszernek is a végére értünk, így aztán ideje, hogy megnézzük alaposabban azt, amibe már belecsíptünk: a virtuális gépek tulajdonságait és beállítási lehetőségeit.

9.4 A VIRTUÁLIS GÉP BEÁLLÍTÁSAI[148]

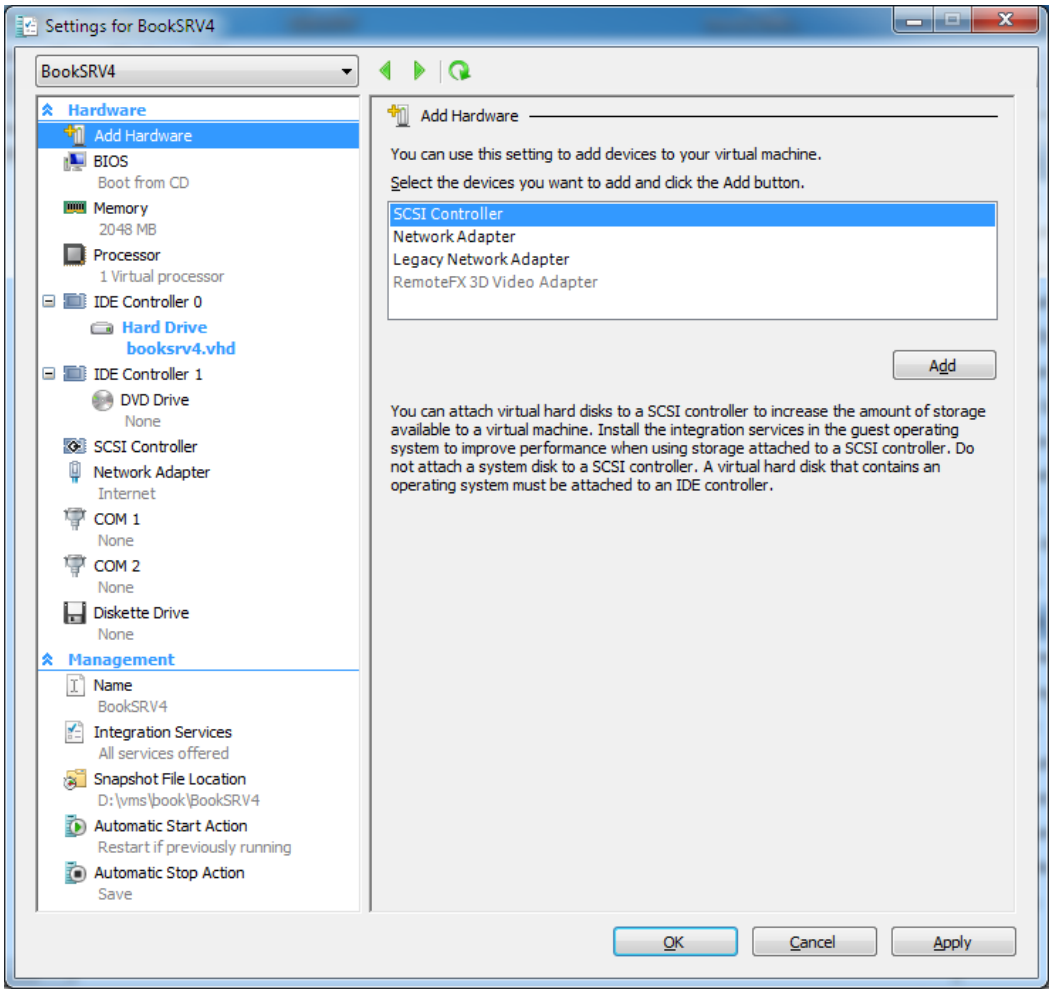
A virtuális gép tulajdonságlapján (helyi menü > Settings) módosíthatjuk a kiválasztott gép hardver és management paramétereit.
A Hardware szakasz részletei:

- Add Hardware: Itt adhatunk új hardvert a gépünkhöz (SCSI controller, Network adapter, Legacy Network adapter, R2 SP1 után RemoteFX 3D Video Adapter is[149])
- BIOS: boot sorrend, Num Lock státusz

[148] Ez az alfejezet jelentős részben támaszkodott Liszák Gábor a technetklub.hu-n megjelent cikkére: https://technetklub.hu/blogs/virtualizacio/archive/2010/08/11/hyper-v-r2-adminisztr-225-ci-243-i-hyper-v-manager.aspx

[149] https://technetklub.hu/blogs/virtualizacio/archive/2010/12/09/remotefx-a-windows-server-2008-r2-sp1-ben.aspx

- Memory: módosíthatjuk a memória méretét, de menet közben nem, R2 SP1-től viszont kihasználhatjuk a dinamikus memória lehetőséget[150].
- Processor: módosíthatjuk a virtuális processzorok számát (kikapcsolt állapotban), szabályozhatjuk az erőforrás-használatot (bekapcsolt állapotban is), processzor kompatibilitási módot állíthatunk.
- IDE Controller: lemezeket, ill. DVD meghajtót (nem lemezt, azaz pl. egy .iso fájlt) csatlakoztathatunk a gépünkhöz, de csak kikapcsolt állapotban.
- SCSI Controller: további diszkeket (maximum 64 db) csatlakoztathatunk a virtuális gépünkhöz. SCSI meghajtóról nem lesz képes bootolni a gépünk, viszont - szemben a virtuális IDE eszközökkel – menet közben is hozzáadhatjuk az ilyen típust!



9.17 ÁBRA AMI SZEM-SZÁJNAK INGERE

- Network Adapter: módosíthatjuk a hálózati kapcsolatokat, új virtuális adaptereket rendelhetünk a szerverünkhöz és kártyánként megadhatjuk, hogy azokat melyik virtuális switch-ünkbe csatlakoztatjuk (a korábban definiált

150 https://technetklub.hu/blogs/virtualizacio/archive/2010/12/09/hyper-v-dinamikus-mem-243-ria-alapok.aspx

virtuális hálózatok közül választhatunk és ha már egyszer felvettük a gép leállított állapotában az interfészt, akkor akár menet közben is változtathatjuk a kártyákon a virtuális hálózatokat).
- DVD Drive: megadhatjuk a médiát, ugyanúgy, ahogy az új virtuális gép varázslóban.
- COM: más kiszolgálókkal történő, virtuális COM porton keresztüli kommunikációt engedélyezhetünk a virtuális gép számára (Named pipe).
- Diskette Drive: virtuális floppy-t (*.vfd) csatlakoztathatunk a gépünkhöz.

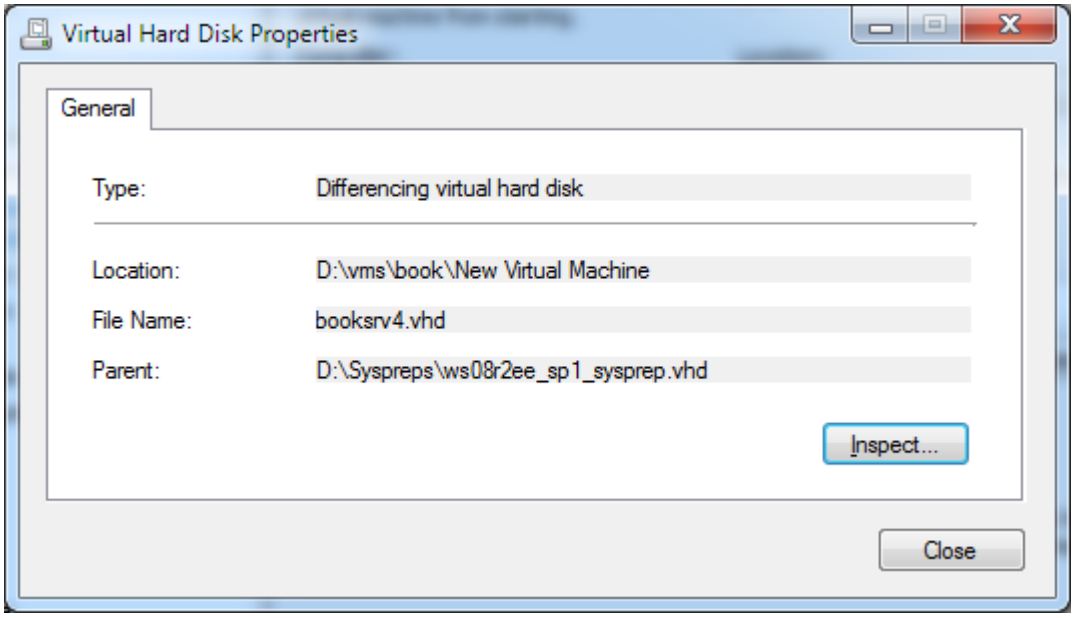
A Management szakasz:
- Name: a gépünk Hyper-V Manager-ben megjelenítendő nevét módosíthatjuk.
- Integration Services: itt találjuk az integrációs szolgáltatások (Integration Services, lásd később) kapcsolóit. Eldönthetjük, hogy ezek közül melyeket szolgáltassa a host gép a virtuális gépünk számára (később kifejtem).
- Snapshot File Location: megváltoztathatjuk a pillanatfelvétel fájlok (lásd később) helyét.
- Automatic Start Action: a fizikai gép indulásához a hozzárendelt automatikus virtuális gép indítási műveletet határozhatjuk meg.
- Automatic Stop Action: a fizikai gép leállásakor megtörténő automatikus virtuális gép leállítási műveletet határozhatjuk meg. [151]

A virtuális diszkek kezelése

A hardveres szakaszban pl. az IDE Controller résznél láthattunk pár, a lemezekkel kapcsolatos műveletet, és ugye a „New” parancs és a differenciális diszkek apropóján már amúgy is jártunk itt. De fontos azt is tudnunk, hogy az „Inspect” lehetőséget választva egy létező .vhd tulajdonságait ellenőrizhetjük.

Az „Edit disk” alatt viszont további, esetenként igen hasznos műveletek is elérhetőek:
- Compact: A fizikai háttértáron elhelyezkedő .vhd fájl mérete nem csökken automatikusan, amikor adatot törlünk a virtuális lemezről,viszont a Compact parancs hatására igen.
- Convert: Dinamikusan növekvő .vhd-ból fix méretű virtuális lemezt készíthetünk. A művelet során az eredeti diszkünk tartalmáról másolat készül egy általunk meghatározott méretű új, fix .vhd-ba.
- Expand: Fix-, illetve dinamikusan növekvő méretű .vhd méretét növelhetjük, egészen 2TB-ig.
- Merge: Csak a differenciális lemezek használata esetén jelenik meg, ugyanis van lehetőségünk arra, hogy összeolvasszuk a szülő és a változásokat tartalmazó .vhd fájlt.

[151] Az utóbbi két opcióval állítható be – némi próbálgatás után –, hogy a megfelelő sorrendben induljanak el a gépek, legalábbis egy hoston belül (a lektor megjegyzése).

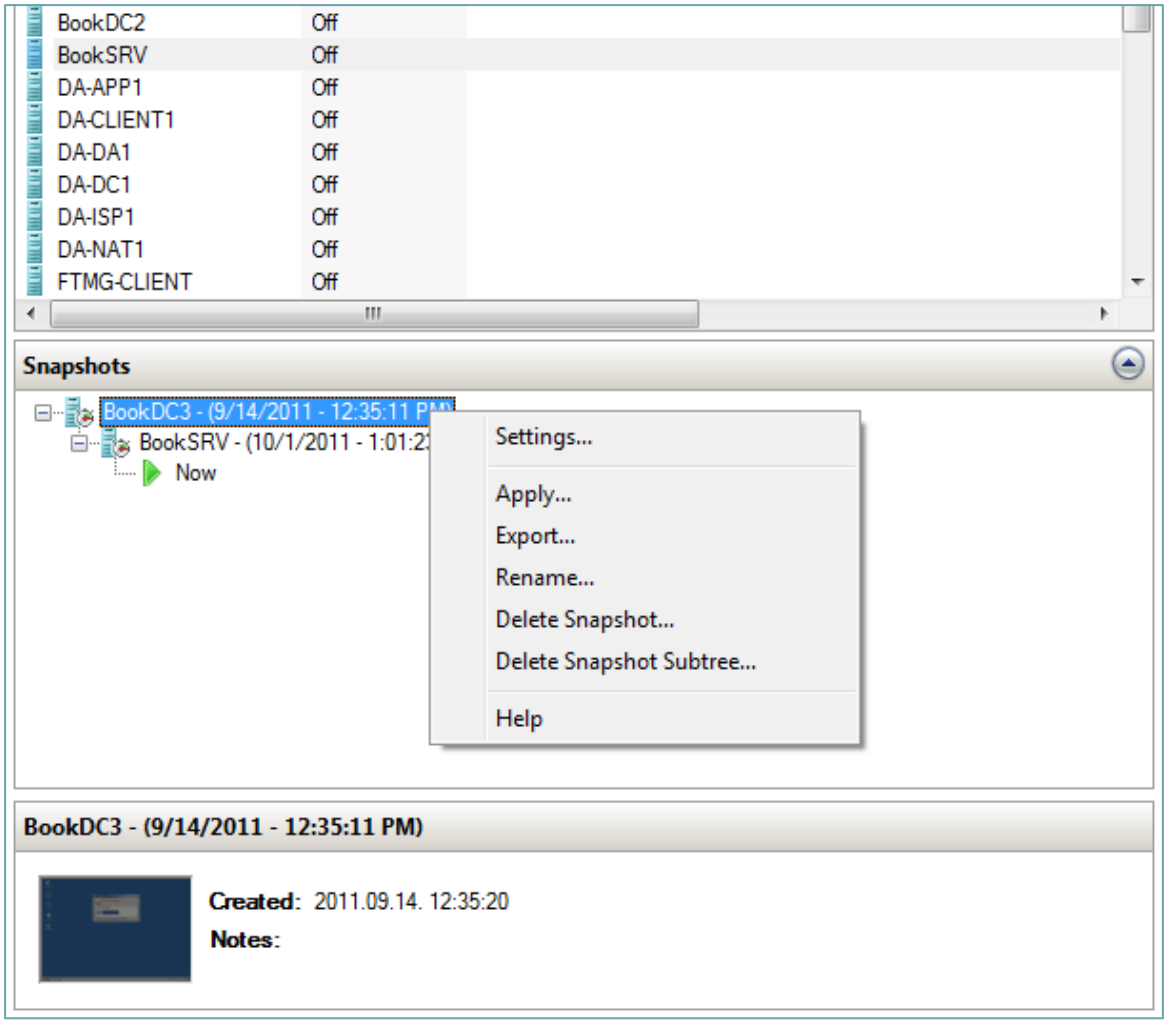


9.18 ÁBRA EGY LEMEZVIZSGÁLAT FÉLÚTON

Snapshot (pillanatfelvétel)

A pillanatfelvétel remek lehetőség, ami kiválóan használható, és ez az egyik dolog a sokból, ami a fizikai gépekhez képest a virtuális gépeknél a magas szintű rugalmasságot adja a kezünkbe. Merthogy a pillanatfelvétel használatával egy adott virtuális gép lemezének, konfigurációjának és az aktuális memóriatartalom tartalmának állapotát rögzíthetjük, és erre az állapotra bármikor visszaállhatunk. Például egy OS-nél egy összetett konfigurálás előtt állok, és lehet, hogy visszatérnék a mostani állapothoz, mert ez csak egy teszt. Készítek egy pillanatfelvételt pár másodperc alatt, szétkonfigurálom a gépet, majd ha úgy óhajtom akkor, visszaállok teljesen az előző állapotra, szintén pár másodperc alatt.

De ez ekkor az igazi, ha olyan változást tervezek végrehajtani, ami egyébként visszafordíthatatlan lenne (nyilván egy olyan művelet esetén, amelynek eredménye például a címtárban tárolódik, kevésbé operálhatunk).



9.19 ÁBRA A PILLANATFELVÉTEL MŰVELETEK

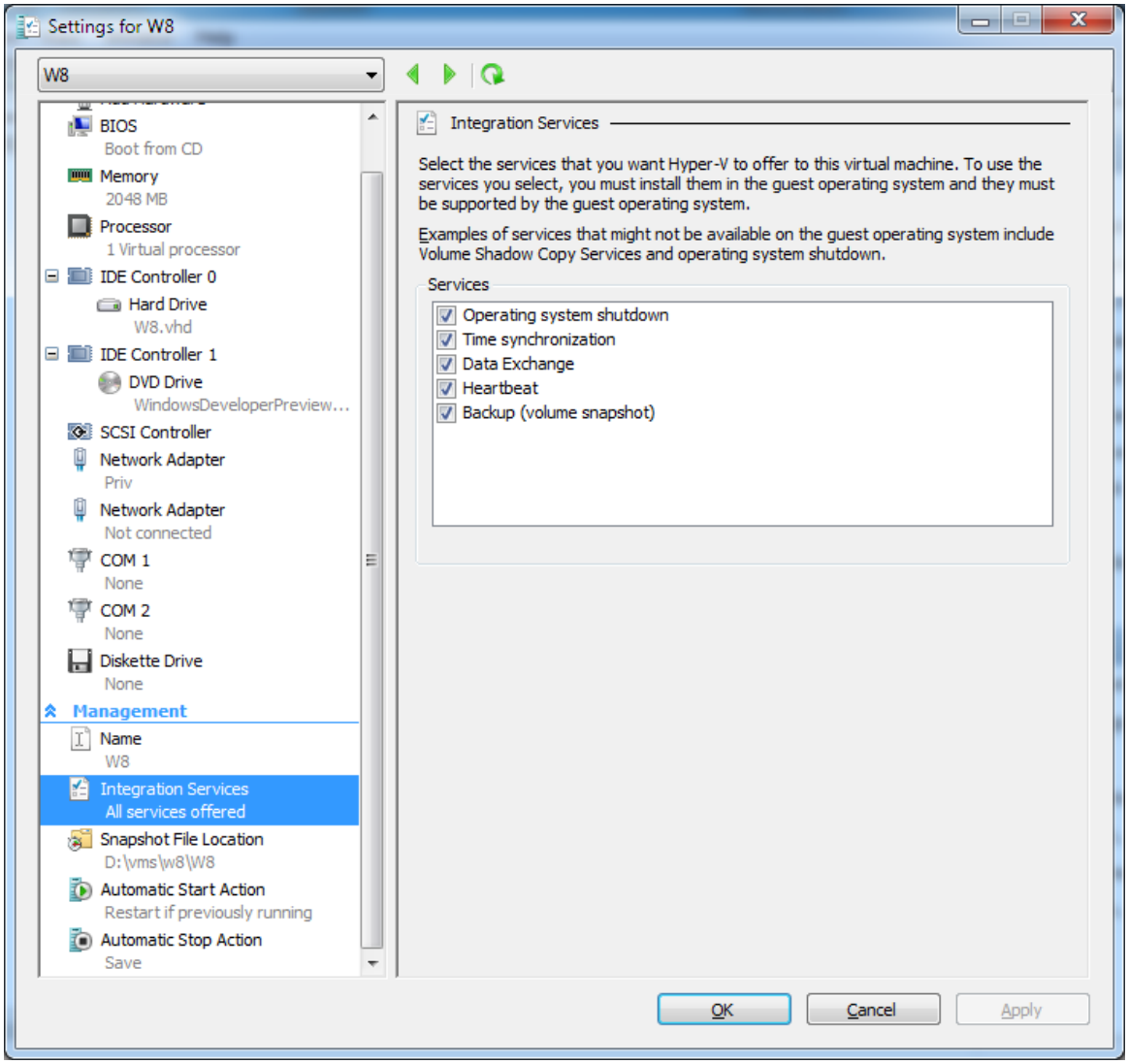
No és persze egy gépről számos pillanatfelvételünk is lehet[152], amelyeket egy faszerkezetbe rendezve találjuk meg az adott gép neve alatt, a különböző időpontokkal elnevezve (persze átnevezhető, és értelmes, az állapotra utaló nevekkel célszerű is ezt megtenni, mert a káosz gyorsan kialakul). A fából lehetőségünk nyílik törölni egyetlen pillanatfelvételt (Delete Snapshot...), de törölhetjük egyszerre az egész fát is, ill. a kijelölt snapshot alatti snapshot-okat (Delete Snapshot Subtree...).

Természetesen, ha a Delete Snapshot Subtree... lehetőséget a legfelső felvétel kijelölése mellett választjuk, akkor az összes rögzített állapotot töröljük. Ami még fontos, hogy a pillanatfelvétel exportálható is, viszont nem készíthetünk pillanatfelvételt olyan gépről, melyhez akár csak egy pass-through diszket is csatlakoztattunk.

Az integrációs komponensről

[152] A pillanatfelvétel állományok helyét az egyes virtuális gépek tulajdonságlapján állíthatjuk be. A snapshot állomány kiterjesztése az .avhd.

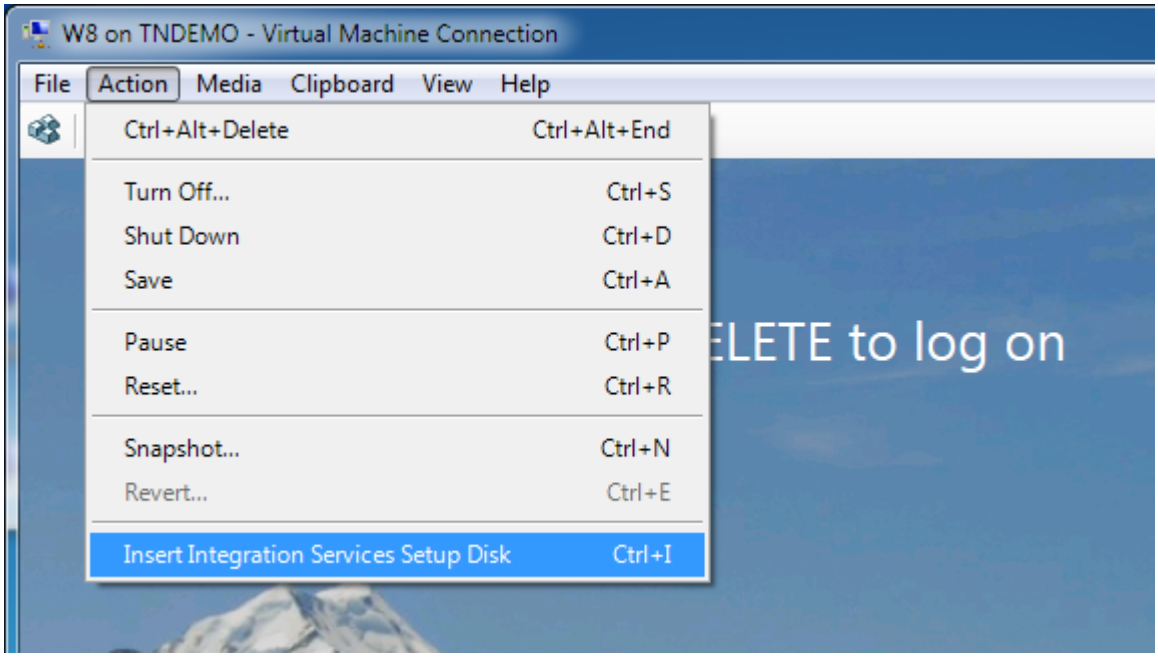
Némi Hyper-V rutin után egyszer csak az ember elgondolkodik arról, hogy ugyan hogy tudom én szabályosan leállítani (shutdown) a virtuális gép eszköztárának menüjéből a virtuális gépet, mikor ezt a parancsot abszolúte „kintről” adom ki? Vagy hogy tudom menteni a komplett virtuális gépet, szintén kívülről? Nos erre és még sok más kérdésre az integrációs komponens a válasz.



9.20 ÁBRA AZ 5 EXTRA LEHETŐSÉG

A fejezet elején említett „Főirányító”, azaz a Worker processz ezeken az integrációs komponenseken keresztül tartja a kapcsolatot például a szintetikus eszközökkel (VMBus) és a többi virtuális géppel (VSP-VSC), valamint feldolgozza a gazdagépről érkező felügyeleti utasításokat (WMI), és leképezi az RDP kapcsolatokat[153], illetve 1-2 további, számunkra is látható extra lehetőséget nyújt (lásd: korábbi példák).

[153] Ezért látható már a boot folyamat is, RDP-n keresztül.



9.21 ÁBRA AZ INTEGRÁCIÓS KOMPONENS TELEPÍTÉSE ÍGY INDUL

Az integrációs komponens általában nem kerül bele automatikusan[154] a virtuális gépbe, hanem nekünk kell - célszerűen a virtuális gép első használatakor - felrakni (9.21 ábra), vagy ha például egy más verziójú Hyper-V-ről importáltunk egy gépet, akkor pedig frissíteni.

9.5 A HYPER-V SERVER R2

Ez a termék mindenféle szempontból különleges. 2007 novemberében a barcelonai TechEd konferencián jelentette be a Microsoft a Hyper-V nevet, a termék különböző verzióit, illetve azt, hogy lesz egy önálló "Microsoft Hyper-V Server" nevű termék is, ami aztán 11 hónappal később meg is jelent. A Windows 2008-as változatban még voltak jogos hiányosságok (lásd a táblázat első oszlopát), az R2-re ezek nagyon szépen kisimultak.

Szóval a Hyper-V Server R2 gyakorlatilag egy Windows Server 2008 R2 Enterprise kiadás, de mivel ingyenes, és mivel nincs benne Windows Server licensz, ezért a névben sincs benne a „Windows" kifejezés. Ráadásul az „Enterprise" név csak a Hyper-V-re utal, ugyanis nincs is benne semmilyen más szerepkör, csak a Hyper-V. De hogy lehet Windows Server licensz nélkül benne a Hyper-V? Hát úgy, hogy GUI nélkül működik, azaz parancssoros, mint a Server Core (lásd: következő fejezet). Így aztán

[154] Van azért kivétel is, az R2-nél és a Windows 7-ben gyárilag van, és azt vettem észre, hogy pl. a Windows 8 Developer Preview-ban benne volt egyből az R2-es Hyper-V-hez való csomag.

egy másik - egyéni - megközelítés szerint ez egy olyan Server Core, amiben csak a Hyper-V van. Remélem, már jól össze is zavartam mindenkit ☺. [155]

De tudom fokozni: szerepkör csak 1 van, de képesség azért akad pár: WoW64, .Net Framework, Failover Cluster (a CSV is), MultipathIO[156]. Mi ezekben a közös? Mind kellhetnek a Hyper-V-hez, egy-egy komolyabb, nagyvállalati forgatókönyvben, magas rendelkezésre állással, rendes storage-dzsal, stb. Kezdjük érteni? Kapunk ingyen[157] egy teljesértékű virtualizációs megoldást, önmagában alacsony teljesítményigénnyel, biztonságos működéssel[158] és nagyvállalati célokra is használhatjuk. Okos.

> Már csak azért is igaz az utóbbi jellemző (nagyvállalati), mivel pl. a CPU támogatás „csak" 8 CPU-ra (foglalat) korlátozódik, és 64 magra. RAM tekintetében 1 TB a támogatás felső határa (mármint a fizikai gép esetén). Azért ez nem tipikusan a „Noname" Kft hardver környezete.

Képességek	Microsoft Hyper-V Server 2008	Microsoft Hyper-V Server 2008 R2	Windows Server 2008 R2 Enterprise, Datacenter
Logikai processzor támogatás	24	64	64
Socket-ek száma	Max. 4	Max. 8	Enterprise = Max. 8 Datacenter = Max. 64
Memória támogatás	Max. 32 GB	Max. 1 TB	Max. 1TB
VM migráció	Nincs	Quick és Live migration	Quick és Live Migration
Fürttagokon futtatható virtuális gépek száma	Nem értelmezhető	32 (server OS esetén) 64 (VDI esetén)	32 (server OS esetén) 64 (VDI esetén)
Szülő OS-el licencelt szerverek száma	0	0	EE = 4 VM DC = korlátlan számú VM
Futtatható virtuális gépek száma	192	384	384
WS08 CAL szükséges a Guest szerver OS-hez	Nem	Nem	Igen
Guest OS támogatás	Windows Server 2008 R2, Windows Server 2008 & SP2, Windows Server 2003 SP2, Windows 2000 Server, SLES 10, SLES 11, Red Hat Enterprise 5.2/5.3, Windows 7, Windows Vista SP1, SP2 & Windows XP SP3/SP2		

9.21 ÁBRA AZ ÖSSZEHASONLÍTÁS SEM HÁTRÁNYOS A HYPER-V 2008 R2 SERVER-RE NÉZVE

[155] A Hyper-V Servernek van egy tulajdonsága, ami nincs meg a „rendes" szerverekben: támogatott módon indítható egy pendrive-ról. Továbbá van egy olyan képessége, amely viszont nincs meg a Server Core-ban: a RemoteFX (lásd később) bekapcsolható rajta, ha SP1 szinten van.

[156] De azért van BitLocker, Backup és 1-2 kisebb képesség is – de mind a Hyper-V miatt.

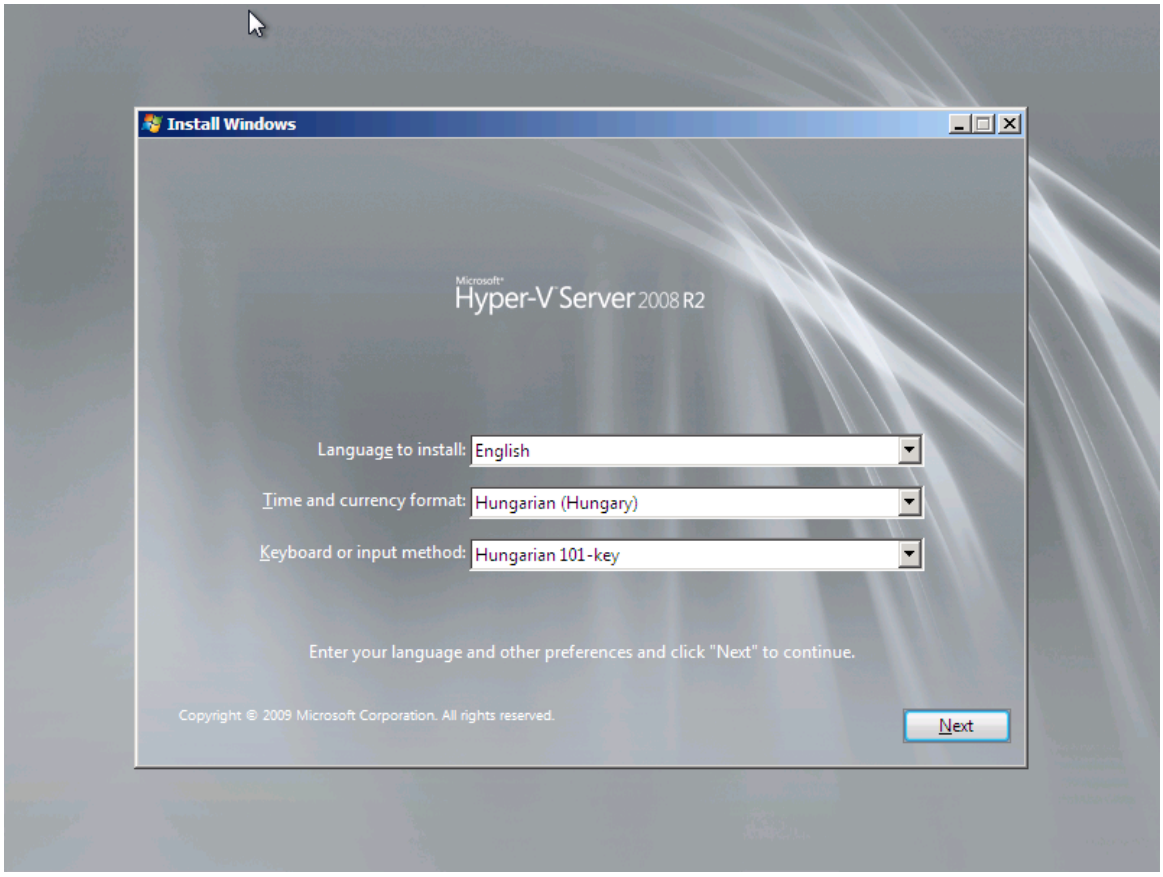
[157] Ugye azt azért értjük (és a következő táblázbatól ki is derül), hogy csak a szülő OS van ingyen, a guest OS-eket természetesen el kell látnunk majd érvényes licenszekkel ☺

[158] Fogjuk majd látni százalékok formájában is a Server Core-nal, hogy a parancssoros változatok patch-elési igénye jóval kisebb.

A Hyper-V Server 2008 R2 hardveres igényei teljesen megegyeznek a GUI-s változat igényeivel. Semmi további extra, sőt, a parancssoros működésből fakadóan jóval kevesebbel is beéri. Ha megvan a telepítő (1,5 GB), és el is indítjuk, akkor annyira egyszerű a dolgunk, hogy szóra sem érdemes.

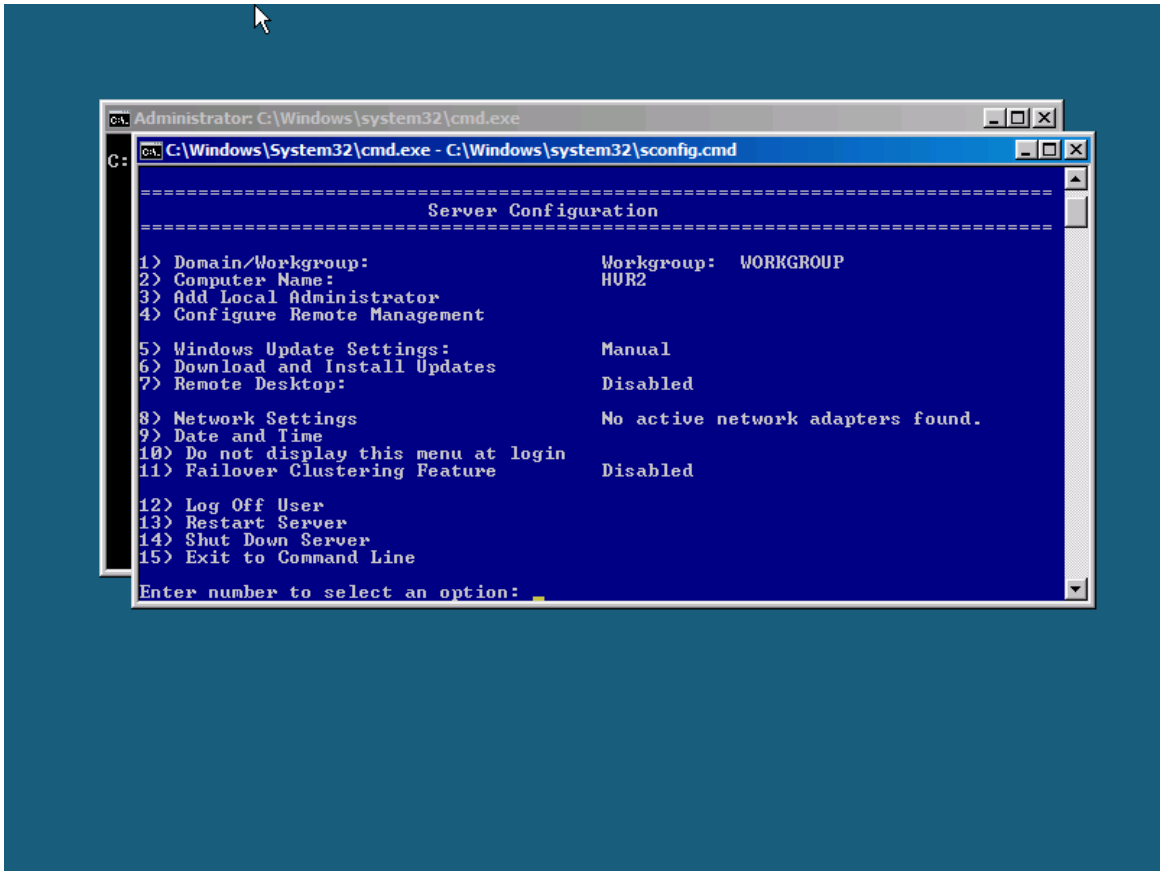
A kezelés az már egy másik tészta, de itt jön az igazi hasonlóság a Server Core-ral, azaz ugyanúgy egy parancssoros menürendszerünk van, mint ott, és csak kicsit eltérő lehetőségekkel (nézzük meg a következő fejezet képeit, csak a „Failover Clustering Feature" a különbség), még az indítása is az *sconfig* paranccsal történik (mármint az R2-ben, mert a Windows Server 2008-ban még a *hvconfig* volt a megfelelő parancs).

A felügyelethez itt sem kell csak és kizárólag a parancssort használni, a távoli WinRM, MMC, RDP hozzáférés megoldott[159], csak engedélyezni kell. És persze tartomány tagja, a Csoportházirend alanya egyaránt lehet, és persze a System Center család felügyeleti hatókörébe is beletartozhat.

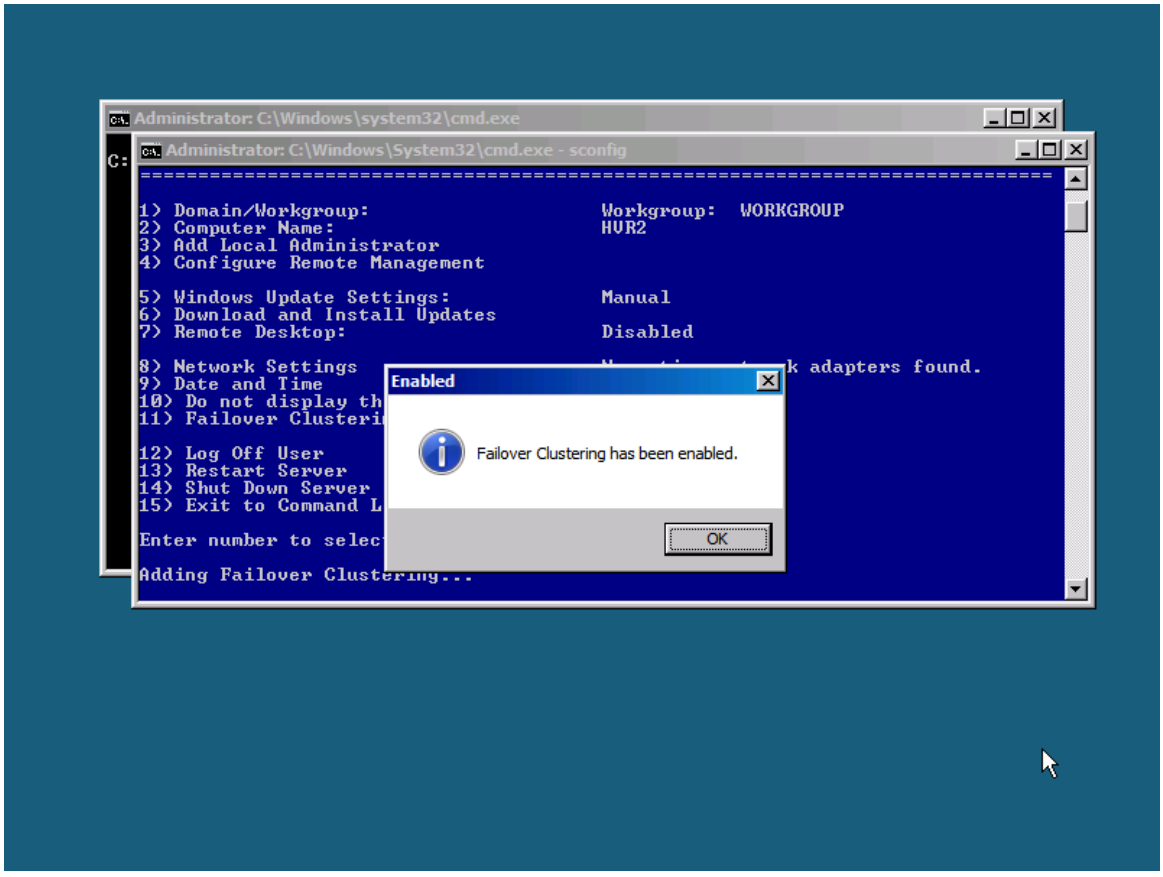


9.22 ÁBRA ÍGY INDUL A TELEPÍTŐ

[159] Igazából a fejezetek sorrendje kicsit zavarba hozó lehet, de az ide tartozó *hogyan*-okat mind megtaláljuk majd a következő fejezetben, a Server Core kapcsán (mivel azt korábban írtam meg).



9.23 ÁBRA A VÁLASZTÉK (AZ SCONFIG PARANCS)



9.24 ÁBRA HA FAILOVER CLUSTER KÉPESSÉGET AKARSZ, NYOMD MEG 2X AZ 1-EST

10 A SERVER CORE

A Windows 2008 család a szokásos Standard, Enterprise és egyéb kiadások mellett egy különleges ún. telepítési változatot is tartalmazott, amelynek a neve Server Core. A különlegessége elsősorban abból áll, hogy 95%-ban parancssorból működik, azaz egyáltalán nincs GUI. Elsőre ez biztosan meghökkentőnek tűnik, de működik és nem is akárhogyan.

10.1 ELŐNYÖK ÉS HÁTRÁNYOK

Nézzük sorban milyen előnyei vannak egy ilyen kiszolgáló verziónak:

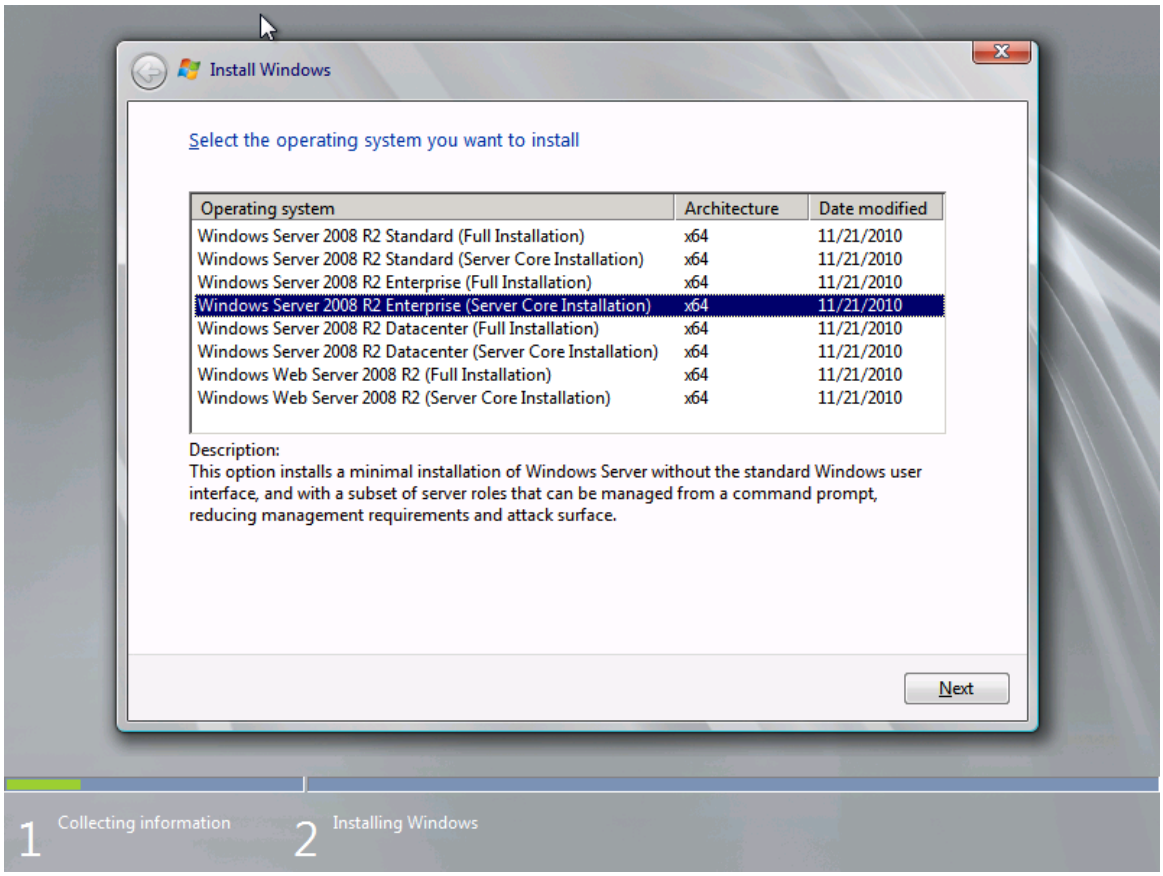
- A erőforrások szempontból lényegesen gyengébb gépen is jól működik. A korábbi tesztjeim során kiderült hogy pl. egy virtuális gépben 80 MB RAM-mal már egy kényelmesen felszerelt tagkiszolgáló is működtethető, 128 MB memóriával pedig egy full extrás tartományvezérlő is tökéletesen jól teljesít. Ha igazi vasról van szó, hasonló a helyzet, bár ilyenkor egy kicsit több erő kell. De nem sokkal, az ajánlás szerint 512 MB RAM [160] elég a teljes funkcionalitáshoz. Ide tartozik a lemezhely igény is, ami az alaptelepítés után a pagefile nélkül valóban nem több, mint 4 GB (és ebben benne van a kb. 2 GB-nyi, kompatibilitási okokból fenntartott Windows\Winsxs mappa tartalma is, ami egyébként a teljes rendszernél a duplája ennek). És persze ne felejtsük el, hogy alapesetben olyan 30 körüli automatikusan induló rendszer rendszerszolgáltatás van! Ez (is) komoly különbség az erőforrás használatot tekintve.
- Számos kiszolgáló feladatkört képes ellátni a Server Core (erről később), de lényegesen kevesebbet, mint pl. egy tipikus teljes[161] szerver. Ezenkívül nem lehet akármit rátelepíteni, azaz léteznek a belső és a 3rd party programok területén is kemény korlátok. A „kevesebb jobb” elv alapján ez nyilván sok forgatókönyvben fontos lesz, hiszen itt szintén nem kevés üzemeltetési időt takaríthatunk meg.
- Becslések szerint kb. 60%-kal kevesebbet kell a biztonsági és egyéb javításokkal törődnünk, ha nincs GUI, és nincs az ehhez szorosan kötődő rengeteg alkalmazás. Ez nyilván azt is jelenti, hogy kevesebbet kell ezzel a kiszolgálóval foglalkozni a beüzemelés után („*...ott lehet hagyni a sarokban*”), és egyáltalán nincs annyi újraindítás sem.
- A telepítés utáni indító konfigurálás (pl. TCP/IP, gépnév megváltoztatása, stb.) tipikusan a parancssorból történik, de ezután minimum háromféle módszerrel vagyunk képesek távolból is felügyelni, üzemeltetni a Server Core-t.

[160] A telepítéshez viszont mindenképpen 512 MB RAM kell, a telepítő motorja ennyit megkíván.

[161] Nem szeretem ezt a kifejezést, szerintem a Server Core is sok szempontból teljes, de a hivatalos angol „full”-t követem azért.

Használhatjuk az MMC-t, az RDP-t és a WS-Management képességet, azaz a WinRM/WinRS párost, ami gyakorlatilag távoli parancssorként működik. Tehát nem kell halálra rémülni a szerver konzolon a fekete háttér előtt villogó fehér kurzortól, létezik módszer a mindennapok feladatainak elvégzésére pl. a rendszergazda gépéről.

- Négy R2 kiadásban (ST, EE, DC, Web) is megtalálható, és egyformán használható x86/x64 környezetben is (ez nyilván csak a Windows Server 2008-ra igaz, mivel az R2, mint tudjuk, csak az x64 platformon érhető el).



10.1 ÁBRA ITT DŐL EL MINDEN

A teljesség és a tisztánlátás kedvéért tekintsük át a hátrányokat is, mert azért az sejthető, hogy a felsorolt előnyök számos kompromisszummal is járnak!

- Tényleg nincs GUI. Nincs Explorer, MMC, CLR, shell, IE, Media Player, Windows Mail, Paint és Calculator, RDP kliens, stb. El kell gondolkodnunk azon, hogy hogyan lehet DNS zónát telepíteni parancssorból? Hogyan lehet szintén innen felhasználót felvenni az AD-ba? Hogy csinálunk egy kivételszabályt a tűzfalban, hogyan hitelesítünk egy DHCP szervert az AD segítségével, ha nincs GUI? Még sok ilyen kérdést fel fogunk tenni magunknak a használat során, de a válasz végül mindig az, hogy lehet, csak kicsit (ritkán nagyon) bonyolultabb.

- Ami előny, az egyben hátrány is, azaz kevesebb komponens és alkalmazás működik a Server Core kiszolgálókon. 10 fő szerepkör[162] van, amelyet teljes körűen ellát(hat): DHCP, DNS, File Services (DFS/R és a többi is persze), Active Directory, Active Directory Lightweight Directory Services, Active Directory Certificate Services, Print and Document Services, Remote Desktop Services (de csak az RDVH a VDI-hoz), Web Server (IIS) és a Hyper-V. Ezek mellett azért van egy kellemes listánk a képességekről is:
    - BranchCache
    - Bitlocker Drive Encryption
    - Failover Clustering
    - Multipath IO
    - Network Load Balancing
    - NFS Server, Subsystem for UNIX-based Applications
    - Removable Storage Management
    - Quality Windows Audio Video Experience (Qwave)
    - SNMP
    - Telnet Client
    - Windows Server Backup
    - WINS
    - WoW64 Support

Némi hátrány mutatkozik a telepítés, pontosabban a frissítés és migráció környékén is, azaz három fontos részletet kell kiemelni:

1. Nem lehetséges egy korábbi Windows szerver verzióról frissíteni.
2. Nem járható út a teljes verziókról történő frissítés sem.
3. A Server Core-t szintén nem lehet egy teljes kiadásra frissíteni.

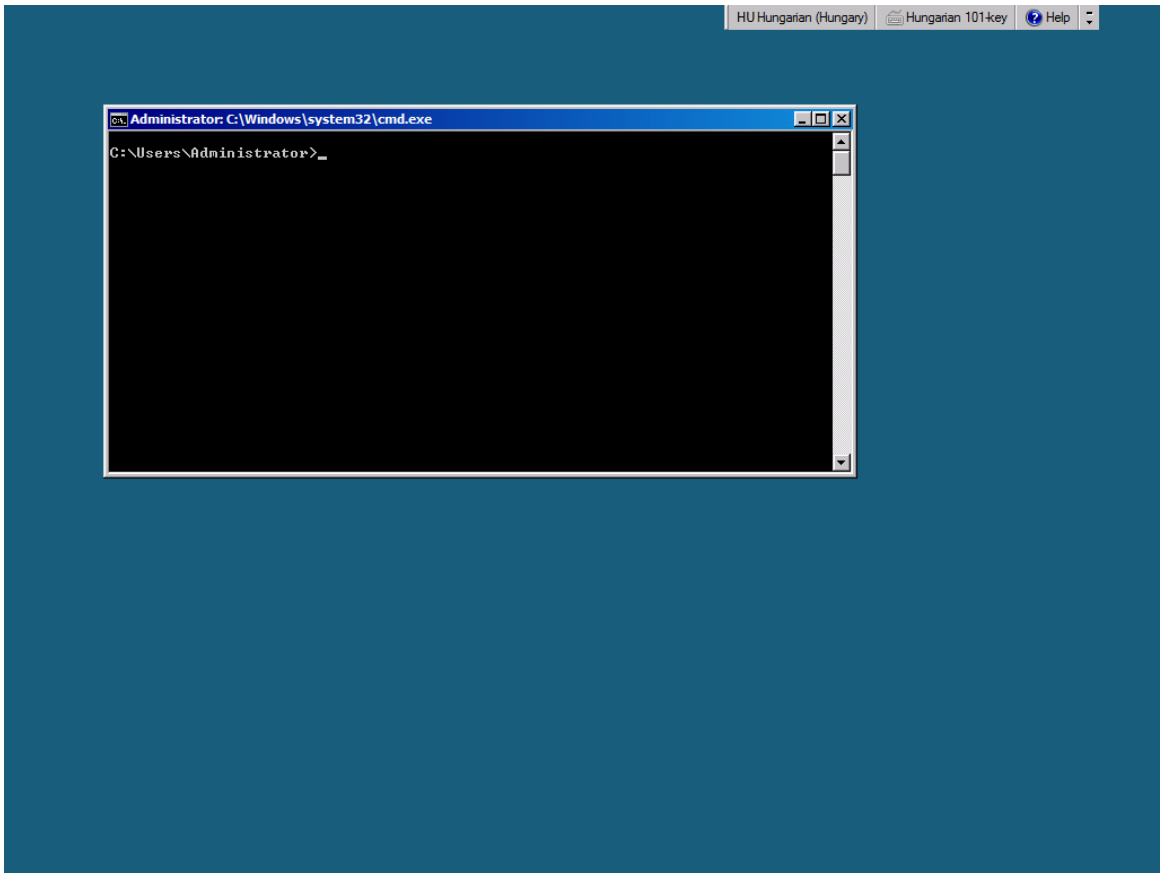
Ezekből értelemszerűen az következik, hogy a Server Core telepítés csak tiszta (clean) telepítés lehet. Hogy szépítsem a képet, jelzem, hogy egy komoly előny viszont látszik a telepítésnél, ugyanis villámgyors, kb. 8-10 perc, és kész is vagyunk.

Még egy fontos dolog: a csendes telepítés megvalósítható, a Server Core képes egy Unattend.xml alapján települni, azaz testre szabhatjuk (képernyő felbontás, RDP engedélyezése, stb.) és automatizálhatjuk a telepítést ugyanúgy, mint a teljes verziónál (pl. Windows System Image Manager-rel).

10.2 Az első lépések

[162] Itt nem lesz külön R2-es fejezet, hanem itt és később is csak az R2-ről beszélek, illetve... de majd meglátjuk ☺.

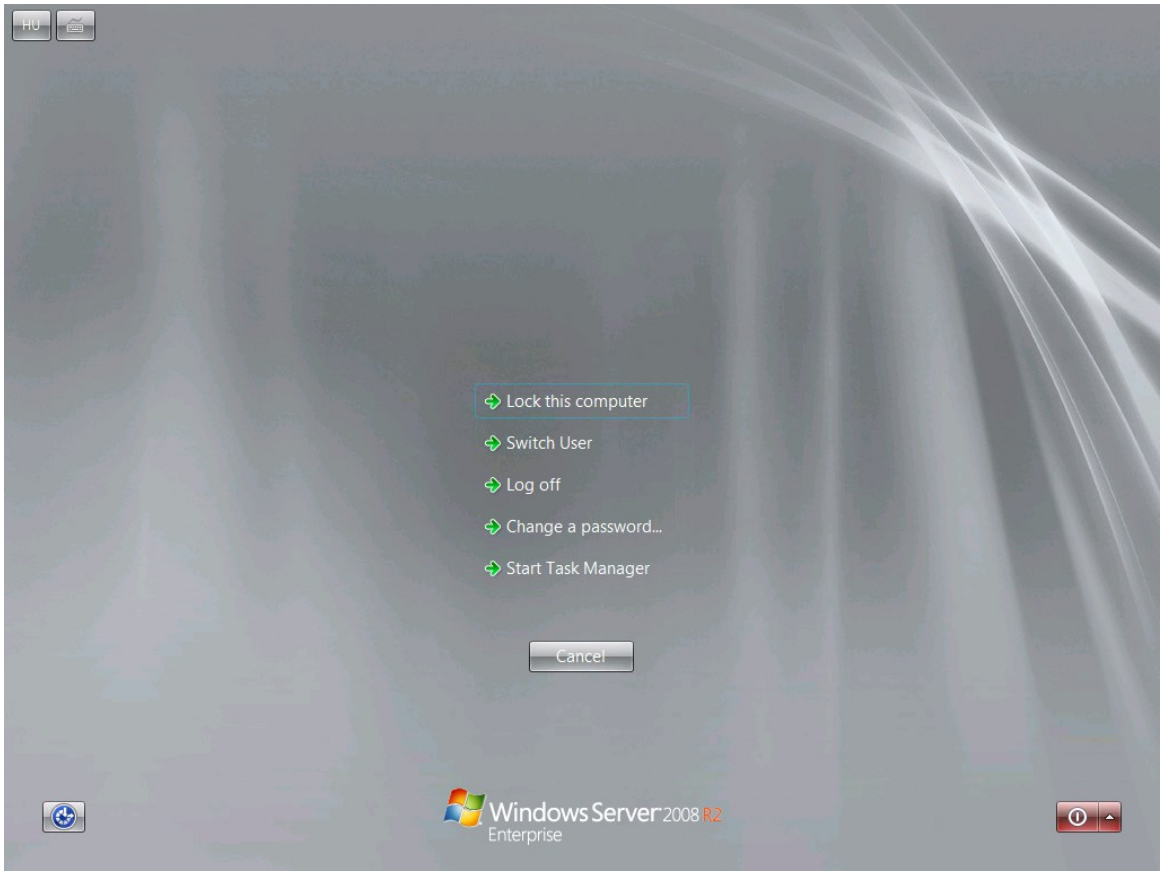
A telepítésben semmi extra nincs, azt viszont még egyszer és előzetesen kell rögzíteni, hogy vagy-vagy, tehát licenszelési szempontból vagy egy teljes verziót telepítünk, vagy a Server Core-t.



10.2 ÁBRA A SERVER CORE-BÓL ENNYI LÁTSZIK A BELÉPÉS UTÁN

Ha készen vagyunk, az újfajta egész képernyős belépési képernyőt láthatjuk. Tudnunk kell, hogy itt is egyetlen működő felhasználói fiók van csak (ez az Administrator, persze van még egy, a Guest, de szokás szerint letiltva), és szokásosan ennek sincs még jelszava. Ha megadjuk ezt, és így belépünk, akkor az előző képen látható látvány tárul a szemünk elé. Ha viszont fogjuk, és becsukjuk az X-szel a parancssor ablakot, akkor csak az egyszínű háttér marad ☺.

De ne pánikoljunk be, használjuk a CTRL+ALT+DEL-t, és ekkor azért némi vigasz gyanánt kaphatunk némi grafikus felületet, ahol a jelszóváltoztatáson kívül ki is léphetünk vagy lezárhatjuk a gépet, illetve elindíthatjuk a Task Manager-t is. Ha pedig van Task Manager, akkor futtathatunk egy újabb parancssort.



10.3 ÁBRA A MINI START MENÜ (MAJDNEM UGYANAZ, MINT A TELJESNÉL)

Egyébként csak a teljesség kedvéért: a jelszóváltoztatáshoz a *net user administrator ** parancs is megfelelő. De vajon mi a következő lépés? Eltaláltuk: a TCP/IP bekonfigurálása. Persze ha van DHCP, és megfelel nekünk, akkor nincs probléma, de kiszolgálóknál ez nem így szokás, úgyhogy jöhet a manuális beállítás, de először tájékozódjunk:

netsh interface ipv4 show interfaces

Ez azért is különösen fontos most, mert az eredményből több adatot is hasznosítani fogunk a későbbiekben, pl. az adott hálózati kapcsolat pontos nevét és a sorszámát. Ezután jöhet a tényleges konfigurálás:

netsh interface ipv4 set address name=2 source=static address=x.x.x.x mask=x.x.x.x gateway=x.x.x.x

A „name” utáni sorszám a hálózati kapcsolat sorszáma az előbbi listából az Idx oszlop alól. Persze, vissza is állíthatjuk bármikor a DHCP-t:

netsh interface ipv4 set address name=2 source=dhcp

A DNS kiszolgáló beállítása kulcsfontosságú feladat:

netsh interface ipv4 add dnsserver name=2 address=x.x.x.x index=1

Mivel több DNS szerver is felvehető, az index adja meg a használandó DNS szerverek sorrendjét. A telepítés közben a szokásos véletlenszerűen kiválasztott, hiperérthetetlen nevet kapja a gép, ebbe a folyamatba közben nem avatkozhatunk bele, utólag viszont igen, mégpedig az ismerős netdom paranccsal:

netdom renamecomputer GepMostaniNeve /newname:GepUjNeve

Felmerülhet a kérdés: hogyan derítjük ki a gép jelenlegi nevét? Nos, a legeslegelső alkalommal utána kellett néznem nekem is[163], de aztán kiderült, hogy a „hostname" parancs működik itt is, sőt a „set c" és a „systeminfo" is.

Aktiválni szeretnénk a szervert? Íme:

Cscript c:\windows\system32\slmgr.vbs -ato

Ha kiadjuk, kb. 1-2 percig nem történik az égvilágon semmi látható, majd ezután diszkréten közli egy apró panelen, hogy sikerült. Egyébként az aktiválás állapotának kiderítéséhez a következő parancsra lesz szükség:

Cscript c:\windows\system32\slmgr.vbs -xpr

Mint szinte minden lépésnél, itt is van lehetőség távoli végrehajtásra, egy másik gépről:

Cscript c:\windows\system32\slmgr.vbs gépneve\administrator jelszó -ato

Ha nem a Server Core lesz a tartományunk alapköve, hanem egy létezőbe szeretnénk beléptetni, akkor még az elején célszerű gondoskodni erről, mivel a felügyelet (pl. WinRM) is feltétele ennek, vagy ha nem, akkor is sokkal egyszerűbb a megoldás (pl. MMC). Ehhez gépeljük be a következőt parancsot:

*netdom join gépnév /domain:domain_név /userd:user_neve /passwordd:**

Ennyi. Egy újraindítás, azaz röpke pár másodperc után a gép a tartomány tagja. A user_neve természetesen egy olyan felhasználói fiók, amelynek van megfelelő

[163] Sok mindennek utána kellett néznem, még 2007-ben a Server Core tesztelés alatt, de ennek azóta is látom a hasznát, mivel rengeteg parancsot megismertem és megtanultam használni.

jogosultsága a gépet a tartományba beléptetni, a passwordd* pedig nem elírás, a csillag hatására kéri be a jelszót.

Természetesen a Domain Admins csoport automatikusan tagja lesz a helyi Administrators csoportnak a tartományba léptetés után, de ha mégis szükségünk lesz egy tartományi felhasználó helyi admin csoportba helyezésére, használjuk ezt a parancsot:

Net localgroup administrators /add domain_neve\user_neve

10.3 Ellenőrzés és felügyelet

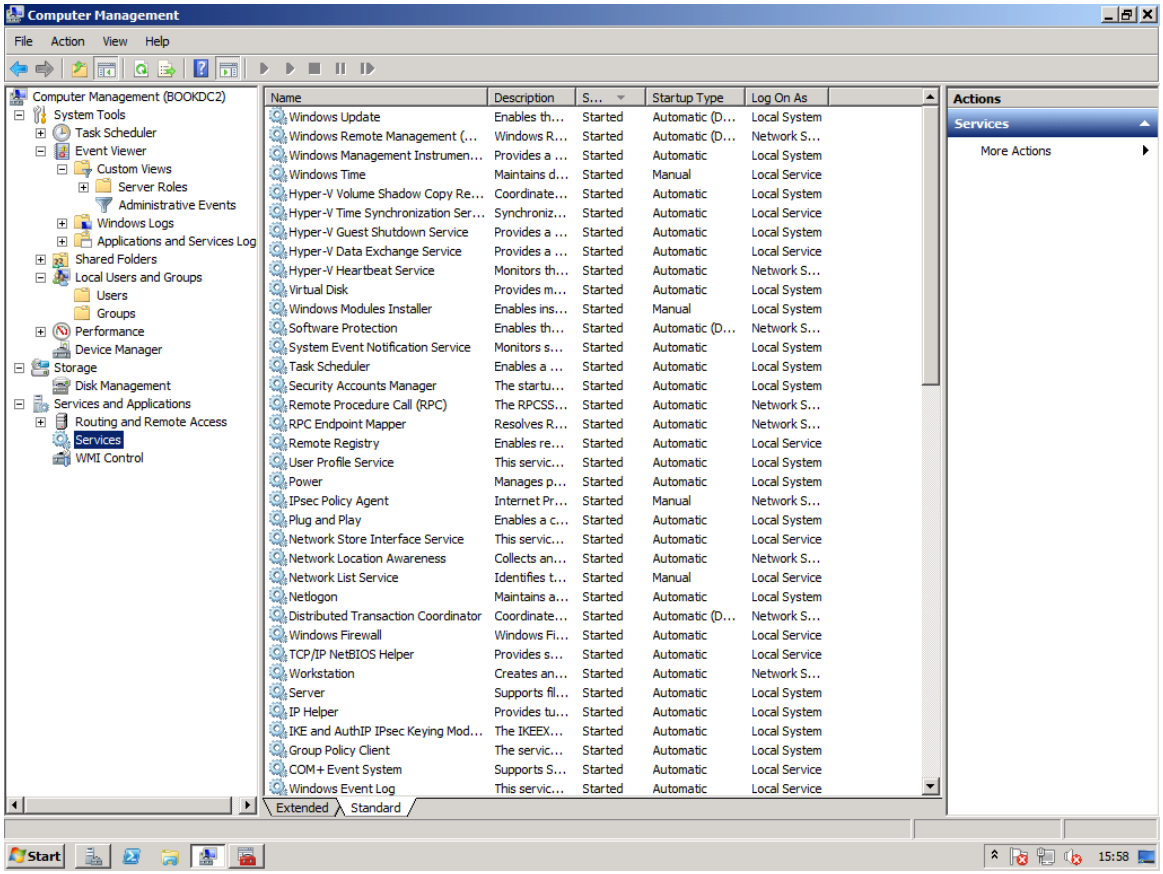
Mint ahogyan már említettem, a felügyelet ellátható távolból három különböző módszerrel is, és igazából célszerű is ez, hiszen helyi eszköz viszonylag kevés van. A három módszer közül az egyik az RDP kapcsolat, amelyet először engedélyezni kell a kiszolgálón:

cscript C:\Windows\System32\Scregedit.wsf /ar 0

De van itt egy kis trükk is, mert ez az engedélyezés az RDP 6.0-ás kliensekre vonatkozik csak (Vistától kezdve alapból ez van, az XPSP2-re letölthető, XPSP3-ban benne van), ha régebbi RDP kliensről óhajtjuk kezelni, akkor:

cscript C:\Windows\System32\Scregedit.wsf/cs 0

Ezután csont nélkül működik, ami azért is jó, mert pl. a vágólapon keresztül is letámadhatjuk a Server Core-t a megfelelő kötegelt vagy egyszeri parancsokkal. Egy másik módszer az MMC-n keresztüli elérés, amely azonos tartományban, megfelelő jogosultsággal semmi extra tudást nem igényel.



10.4 ÁBRA EZ A SERVER CORE COMPUTER MANAGEMENT MMC-JE EGY MÁSIK GÉPRŐL – NINCS KÜLÖNBSÉG

A képről az is kiderül, hogy az újfajta még a Vistában bevezetett Event Viewer, Task Scheduler vagy Performance Monitor képességeket korlátozás nélkül használhatjuk a Server Core esetén is.
Ha viszont nem azonos tartományban vagyunk a kiszolgálóval, akkor elsőként szükség lesz erre a parancsra ahhoz, hogy ne egy Access Denied sorozatba fussunk bele:

*Net use * \\szerver_neve\c$ /u:user_neve*

A harmadik módszerhez a Windows Remote Management / Windows Remote Shell használatához viszont célszerű azonos tartományban lenni a Server Core kiszolgálóval, hiszen ekkor könnyedén használhatjuk pl. a Kerberos-t a hitelesítésre, ami egyúttal az alapértelmezés is. A következő paranccsal indíthatjuk a szerver oldalon a szolgáltatás beállítását:

WinRM quickconfig

Ezzel a paranccsal elindítjuk és automatikus indítására tesszük a WinRM szolgáltatást, beállítjuk a HTTP listener-t a WS-Management protokoll üzeneteinek fogadására és küldésére, valamint létrehozunk egy tűzfal kivétel szabályt (TCP 3190)

a WinRM szolgáltatás részére. És ennyi! Ellenőrzés gyanánt győződjünk meg az alapértelmezett hitelesítés típusáról:

winrm get winrm/config/service

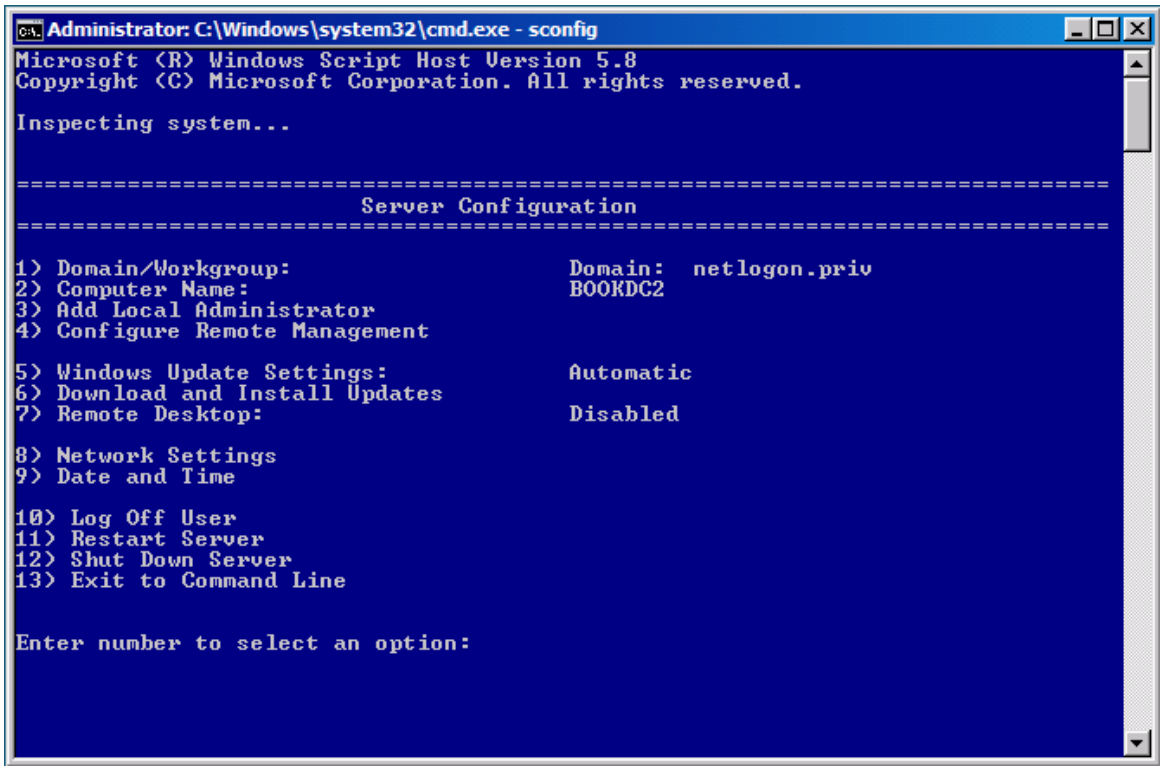
Példaként nézzünk meg néhány további parancsot! A Server Core rendszerpartíciója tartalmának listázásához a következő utasítást adjuk ki egy másik gépről:

winrs -r:http://szerver_neve dir c:

A kiszolgáló újraindításához pedig gépeljük be ezt:

winrs -r:http:// szerver_neve shutdown -r /t 0

És ha a kedves Olvasó lelkiismeretesen követte eddig az instrukcióimat, akkor most elmondanám, hogy ez mind, amit eddig csináltunk, nem is szükséges ☺.

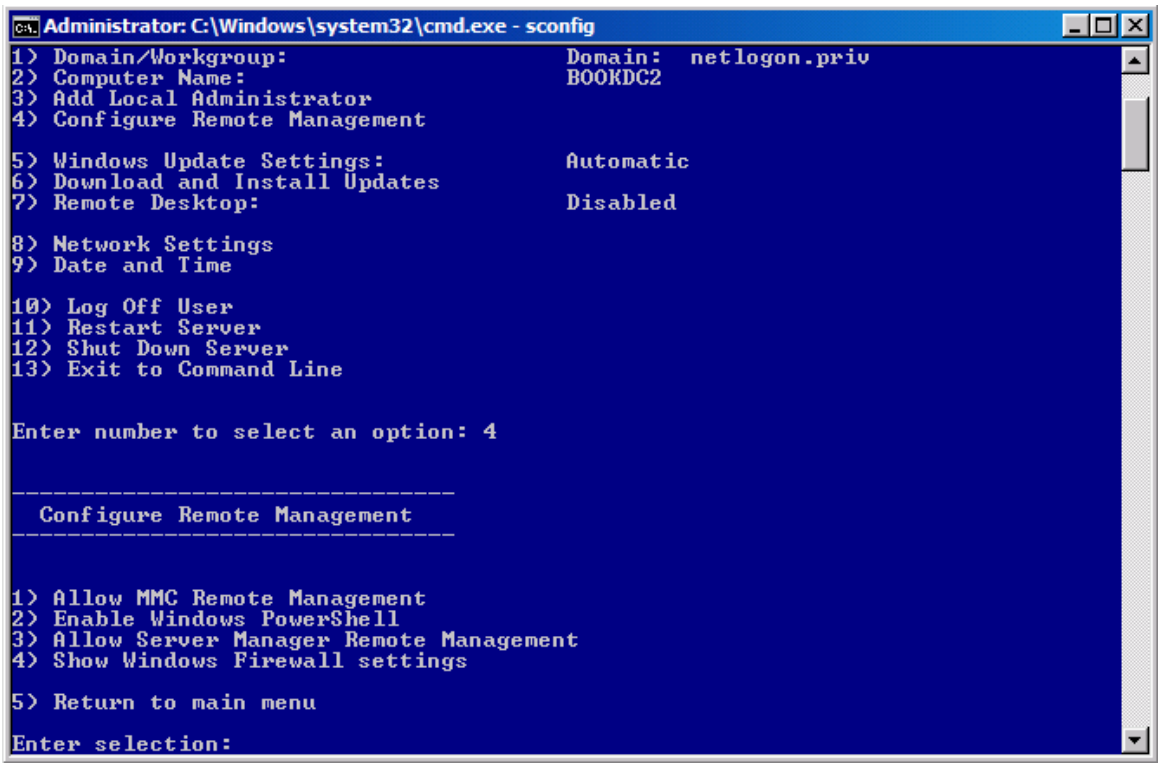


10.5 ÁBRA MENÜ A PARANCSSORBAN, TISZTÁRA MINT A DOS-OS IDŐKBEN ☺

Pontosabban ha csak Windows Server 2008 áll rendelkezésre, akkor igen, ha R2, akkor nem. Illetve igen, persze hogy be kell konfigurálni a TCP/IP-t és a többit, de

nem így, hanem sokkal egyszerűbben. Úgyhogy ismerjük meg az R2-es *sconfig* parancsot![164]

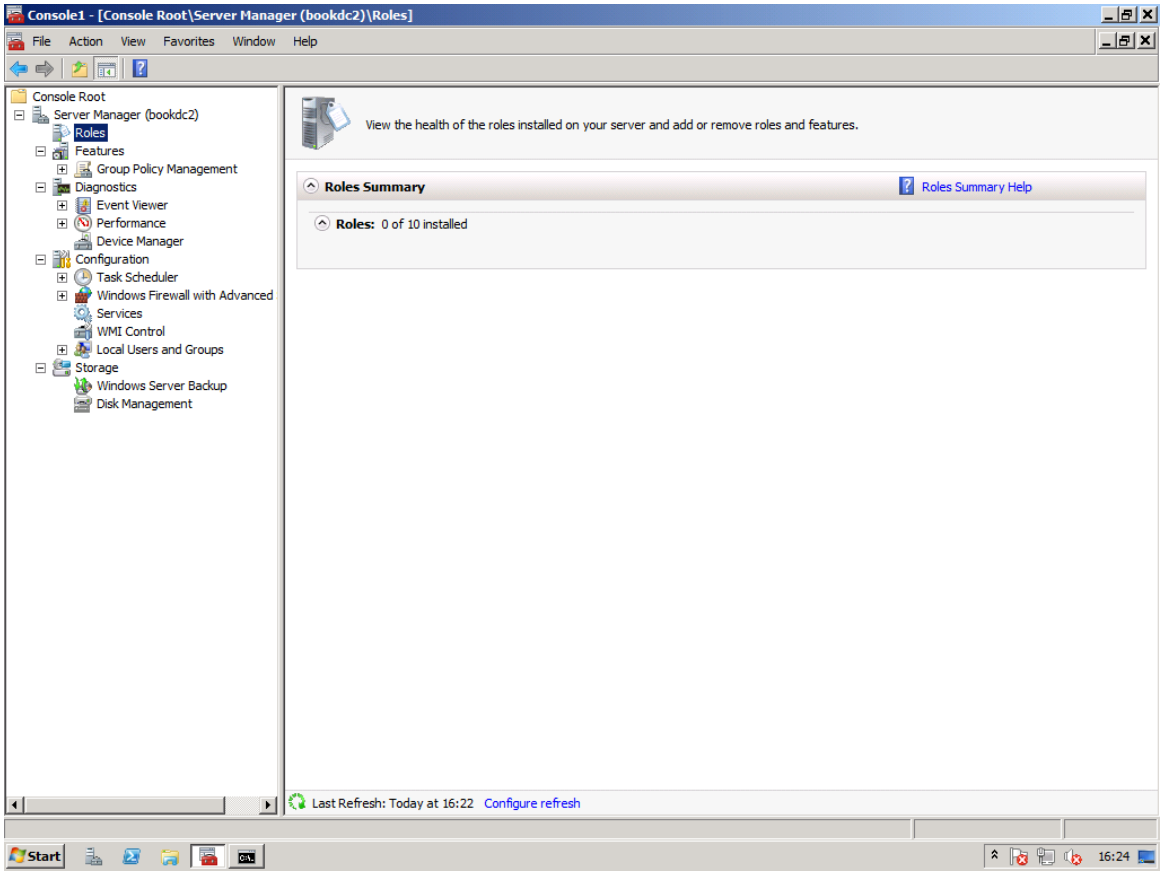
Szóval itt a menüben mindent beállíthatunk amit eddig csináltunk, illetve még sokkal többet is, csak éppen teljesen egyszerűen. Nem fogunk mindenhová benézni, mert minden pont teljesen logikus, de javasolnám, hogy mivel a felügyelet témakörben vagyunk (és mivel mint az előző képen látható, minden mást már amúgy is beállítottam), nézzünk be legalább a 4. pontba!



10.6 ÁBRA MENÜ A PARANCSSORBAN, TISZTÁRA MINT A DOS-OS IDŐKBEN ☺

Ha végigmegyünk az almenün (lesz közben újraindítás is), akkor minden eddigi felügyelet megoldást megengedhetünk, sőt mivel van Powershell is, ezért a Server Manager Remoting-ot is beizzíthatjuk, lásd következő kép.

[164] És van ennél még barátibb, majdnem teljesen GUI-s megoldás is, úgy hívják, hogy *Core Configurator*, de ez már annyira egyszerű, hogy semmilyen kihívás nincs benne ☺: http://coreconfig.codeplex.com/



10.7 ÁBRA CSAK 10 ROLE ÉS 17 FEATURE – DEHÁT EZ A SERVER CORE

Ha a Server Manager megvan[165], akkor már szinte minden megvan, de azért nem minden. Némi kézimunka még kell egyes eszközökhöz, még a tartományban is. Ennek oka a beépített tűzfal (amit kikapcsolni nem érdemes, mert pl. a WinRM ekkor nem működik), amelyen engedélyeznünk kell további szabályokat az MMC konzolok működéséhez. A legfontosabbak:

Disk Management (a Virtual Disk Service-nek futnia kell a Core-on, ez a Service ágból ellenőrizhető)

Netsh advfirewall firewall set rule group="Remote Volume Management" new enable=yes

Device Manager

Ez egy különleges eset, ugyanis nem a tűzfal, hanem a helyi házirend miatt nem érhető el távolról, bármi mást is mond a hibaüzenet.

Computer Configuration\Administrative Templates\System\Device Installation\Allow remote access to the PnP interface

[165] Ne feledjük, a tartományba már beléptettem a Server Core gépet!

A házirendet szabályozhatjuk tartományi szinten is, illetve egy lokális házirendobjektum szerkesztővel csatlakozhatunk távolról a Core géphez, és elegendő a lokális házirend módosítása. A művelet elvégzése után viszont újraindítás szükséges.

Sajnos még a Server Manager Remoting-gal sem tudunk sem szerepköröket, sem képességeket telepíteni vagy eltávolítani távolból. Ez a Server Core verzió esetében jelent nagyobb problémát, de erre mindjárt rátérünk.

Visszatérve a felügyelet témakör elejére, meg kell említeni még egy-két helyben is használható eszközt is. Ide tartozik két Control Panel elem, amelyek megmaradtak a Server Core-ban is.

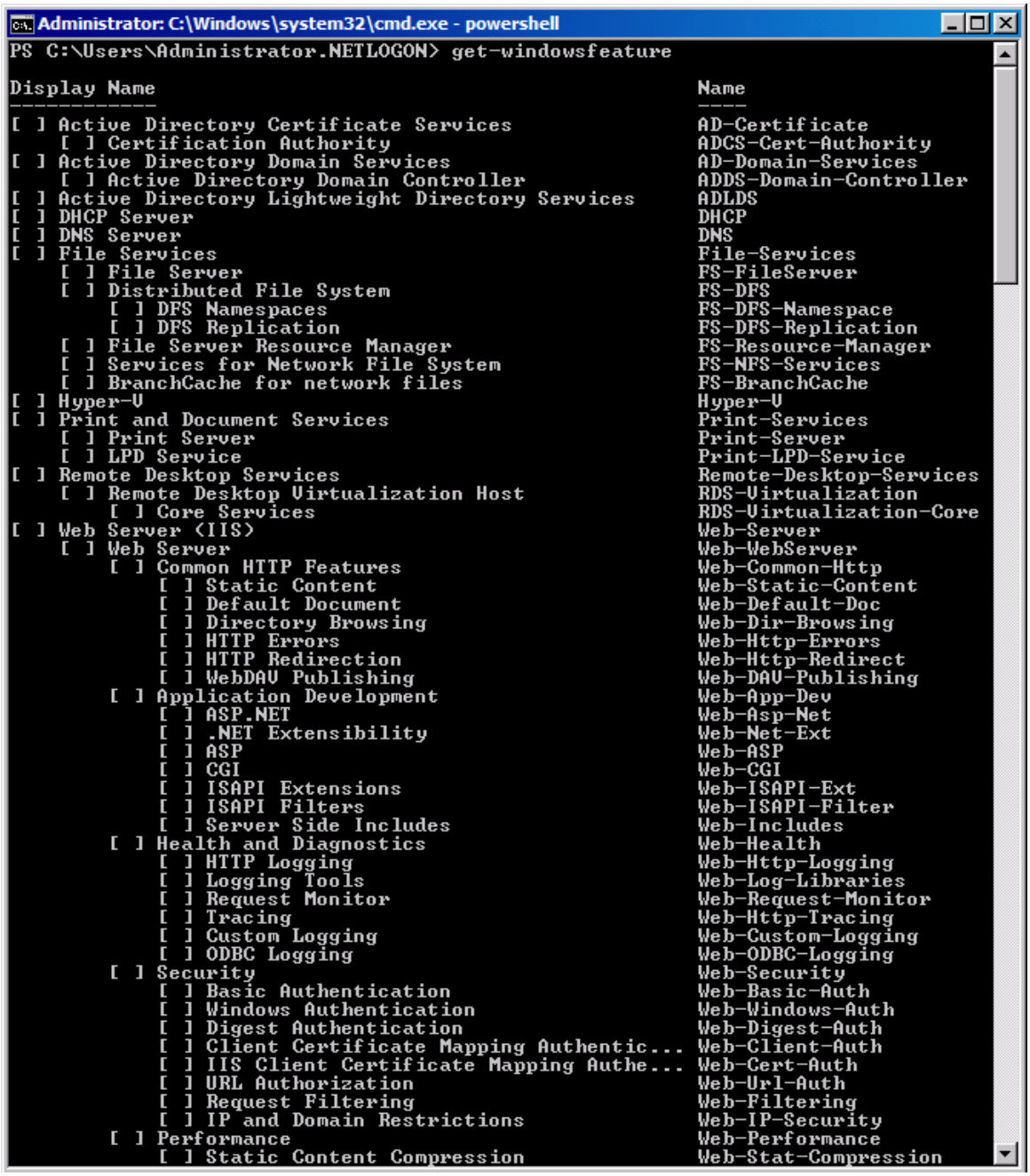
1. Az idő/dátum beállítása: timedate.cpl.
2. A Területi beállítások: intl.cpl
3. iSCSI beállítás: iscsicpl

10.4 Szerepkörök, komponensek telepítése

Fontos kérdés, hogy hogyan tudunk alkalmazásokat és komponenseket telepíteni, illetve hogy melyek állnak rendelkezésünkre akár rögvest a telepítés után, azaz melyeket kell gyakorlatilag csak élesíteni.

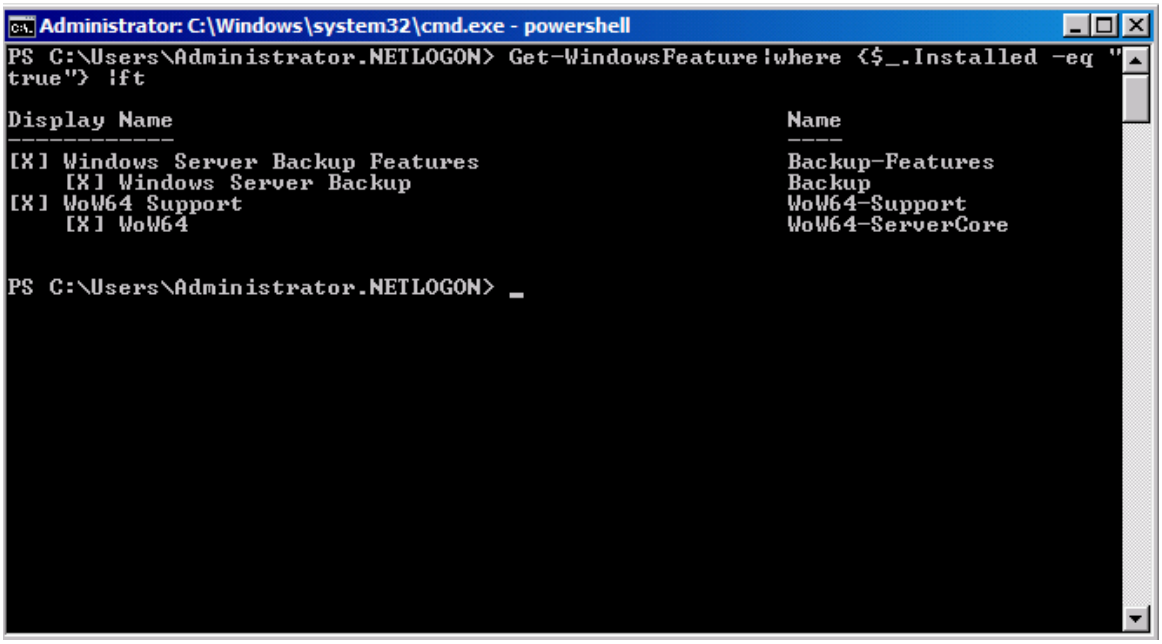
A fontosságuk szerint két részre szedett listát a cikk elején már láthattuk, most viszont az is kiderül, hogy a parancs gyakorlatilag ugyanaz mindkét csoportnál, azaz használjuk a Powershell-t és az ismerős parancsokat!

powershell
import-module servermanager
Get-WindowsFeature



10.8 ÁBRA AZ IIS 7.5 RENGETEG MODULJA MIATT NEM FÉRT KI EGY KÉPERNYŐRE MINDEN

A parancsok után a megfelelő szerepkör vagy komponens neve jön, a különbség maximum annyi, hogy a komolyabb szerepkörök nevei hosszabbak, pl. DNS-Server-Core-Role vagy File-Server-Core-Role és így tovább. A következő képen szépen látszik, hogy ez egy friss Server Core, egyedül a mentés komponenst telepítettem fel kézzel, illetve a WoW64 gyárilag felment, miközben konfigoltam a sconfig-gal.



10.9 ÁBRA GET-WINDOWSFEATURE | WHERE {$_.INSTALLED -EQ "TRUE"} | FT

És akkor még egy dolog, amit tisztáznunk kell: nincs különbség a Server Core és a teljes rendszer bináris állományai között, nincsenek Server Core specifikus .dll-ek és egyebek. Minden ugyanolyan, illetve teljesen ugyanaz – csak egy halom dolog nincs beépítve.

10.5 SERVER CORE + AD

Van viszont egy komoly elem, amely kívül esik a Powershell hatókörén, és egyéni törődést igényel. Az Active Directory telepítéséről van szó, amely nem túl egyszerű művelet, több előkészületre is szükség van hozzá. Először is, tényleg kell a fix IP, ezenkívül a többi előkészületre (pl. sémabővítés) is sort kell kerítenünk.

Ha ránézünk a 10.7 ábrára, akkor mondhatjuk, hogy nahát, de a PS tudja! De nem, ez ugyanaz, mint a Server Manager-nél, azaz a binárisokat felrakja, de csak ennyi a dolga. És miután nem elérhető a grafikus felületű dcpromo, muszáj az unattend módszert választani (amiről már volt szó). Szóval össze kell kalapálnunk egy szövegfájlt, amely az ismert módon vezérelni fogja a telepítést, parancssori indítással. Egy példa egy szűkre szabott, de telepítésre tökéletesen alkalmas szövegfájlra[166]:

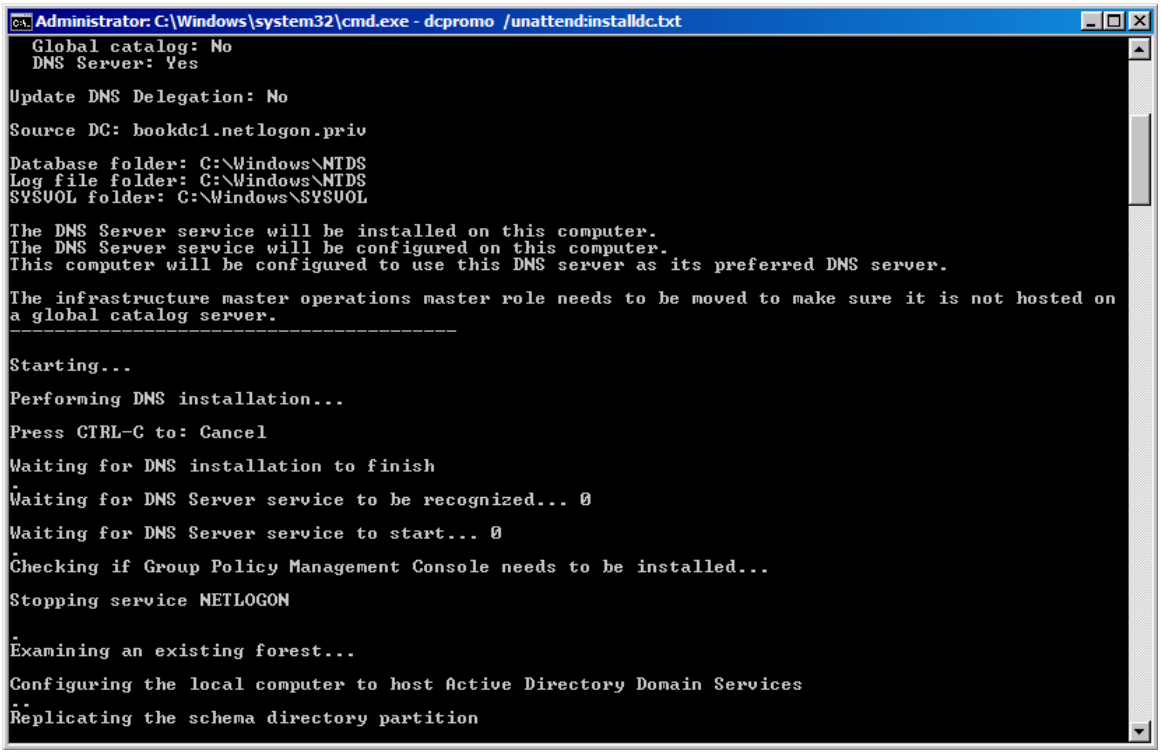
[DCInstall]
AutoConfigDNS = Yes
CriticalReplicationOnly = Yes
DomainNetBiosName = xxx

[166] A szövegfájlba felvehető paraméterekről a vonatkozó Windows Server 2008-as dokumentumból tájékozódhatunk (http://support.microsoft.com/kb/947034).

ReplicaDomainDNSName = xxx.yyy
ReplicaOrNewDomain = Replica
ReplicationSourceDC = zzz.xxx.yyy
SafeModeAdminPassword =
UserDomain = xxx.yyy
UserName = Administrator
Password = [167]

Ezután már csak egyetlen további teendőnk akad, az indító parancs kiadása:
Dcpromo /unattend:fájlneve.txt

Ha kész, akkor a szokásos újraindítás után egy tökéletesen működő [168] tartományvezérlőnk fut a Server Core-on (amit szintén egy másik GUI-s gépről fogunk majd felügyelni, az eddig megismert eszközökkel).



10.10 ÁBRA DC TELEPÍTÉS PARANCSSORBÓL

10.6 EGYÉB ALKALMAZÁSOK ÉS A MEGHAJTÓ PROGRAMOK

[167] Egy megjegyzés egy érdekes jelenségről: ha bármilyen okból elrontjuk elsőre a telepítést, akkor a szövegfájlba újra be kell vinni a jelszavakat, mert egy használat után – akár sikeres volt, akár nem – törlődnek, biztonsági okokból.
[168] Az itthoni rendszerben (ami igen erős, sok szerveres környezet) a Windows Server 2008 bétatesztelésem alatt 2 teljes hétig futott egy Server Core FSMO DC-ként, és tökéletesen működött, pedig itthon tényleg ötkilences rendelkezésre állást kell nyújtanom. ☺

Nem sok egyéb alkalmazásunk van az eddig említetteken kívül, de ezek közül ami fontos, azt a következő táblázat összefoglalja.

GUI Application	Executable with Path
Command prompt	%WINDIR%\System32\Cmd.exe
Microsoft Support Diagnostic Tool	%WINDIR%\System32\Msdt.exe
Notepad	%WINDIR%\System32\Notepad.exe
Registry Editor	%WINDIR%\System32\Regedt32.exe
System Information	%WINDIR%\System32\Msinfo32.exe
Task Manager	%WINDIR%\System32\Taskmgr.exe
Windows Installer	%WINDIR%\System32\Msiexec.exe

10.11 ÁBRA AZ ESZKÖZTÁR

Végül legyen szó egy szintén kritikus területről, azaz a driverek telepítéséről, bár a tapasztalatom szerint a hardverek felismerésével és illesztésével abszolút nincs gond. De ha mégis, akkor a következő módszer szerint járjunk el:

1. Másoljuk be a meghajtó programot egy mappába!
2. Pnputil -i -a mappa_neve\<driver>.inf
3. Újraindítás (nem mindig szükséges).

A jelenlegi meghajtó programok listázásához a következő régi ismerős parancsra lesz szükség (a szóköz a „driver” előtt szándékos):

sc query type= driver

Nos, ezzel végére is értünk a Server Core fejezetnek, lenne értelme még jó pár részt megemlíteni, mert általában igen érdekes dolgokról van szó, de inkább próbáljuk ki, és próbáljuk kihasználni az előnyeit is, személyes véleményem szerint megéri a kicsit több kínlódás.

11 ZÁRSZÓ

Mindig kimarad pár dolog, olyan nincs, hogy mindent le tud írni az ember fia. Pedig csak 200 oldalra terveztem ezt a könyvet, és mi lett belőle? De azért így is van hiányérzetem.

Nagyon jó lett volna írni még az IIS-ről, a WDS-ről, a telephelyekkel kapcsolatban további megoldásokról, vagy akár a hibakeresés és a problémamegoldás új eszközeiről, de a magas rendelkezésre állási komponensek terén is lett volna még mit mondani (pl. Hyper-V + Failover Cluster), és még bizonyára további más területeken is.

Egyetlen vigaszt tudok csak nyújtani, mégpedig a technetklub.hu oldalt, ahol a régebbi és az új anyagaink, az előadások, konferenciák, szakmai napok, stb. „végtermékei" témakörök szerint megtalálhatóak, és nagyon sok esetben akár screencastok formájában is megtekinthetőek (az előző bekezdés felsorolt hiányosságai közül például biztosan mindről van anyagunk). Éljünk ezzel a lehetőséggel, mert érdemes!

Köszönöm a türelmet.

Cegléd, 2011. október

Gál Tamás
v-tagal@microsoft.com
IT üzemeltetési szakértő
Microsoft Magyarország
http://www.technetklub.hu

tamas.gal@iqjb.hu
informatikai vezető, vezető oktató
IQSOFT-John Bryce Oktatóközpont
http://www.iqjb.hu