TechNet MAGAZIN

2008. JANUÁR – FEBRUÁR

MÉLYVÍZ, CSAK ÚSZÓKNAK!

Windows Server® 2008

A CSOPORT-HÁZIREND
Adu ász a Windows Server 2008 esetén is

A HARKÁLY ÉS A HANGYÁSZ
A Hyper-V virtualizáció és a fürtszolgáltatás

METAMORFÓZIS
Tapasztalatok első kézből: Failover Cluster

TÁROLJUNK – okoSAN!
Az iSCSI alapú SAN-kapcsolatok

SÜSS FEL, NAP!
Nyitott ablakok és ajtók belül?

A GAL ÉS A FREE/BUSY
Csoda, hogy egyáltalán működnek

Ára: 999 Ft

9 771586 518005 08001

Microsoft TechNet

Milyen elvárásai vannak Önnek, ha
adattárolási feladatokhoz,
fájl- és nyomtatási feladatok kiszolgálásához
vagy egy webkiszolgálóhoz keres megfelelő eszközt

?

– Legyen megfelelő teljesítménye!
Az Intel Xeon Dual Core processzor és a PC2-5300 DDR2 memória biztosítja a kívánt számítási teljesítményt.

– Legyen elegendő tárolókapacitása!
A tárolókapacitásról a 3 GB/s Serial ATA-II-es diszkek gondoskodnak, akár 750 GB diszkenkénti kapacitással.

– Legyenek biztonságban a tárolt adatok!
Az adatok biztonságáról az integrált Raid vezérlő gondoskodik, amely Raid-0-ra és Raid-1-re képes. Kiegészítő adapterrel a Raid szintek tovább növelhetők!

– Legyen üzembiztos a működése!
A memóriahibákat az ECC hibajavítás küszöböli ki. A diszkek meghibásodását a rendszer előre jelzi (Predictive Failure Analisys). A diszkek egyes modellekben üzem közben cserélhetők. Továbbá a hűtés és a tápegységek is redundánsak lehetnek!

– Legyen egyszerű az installálása és a menedzsmentje!
Az installálást az IBM ServeGuide szoftver könnyíti meg. A rendszermenedzsment az IBM Director szoftveren keresztül történhet, ezt kiegészíti az integrált menedzsmentvezérlő vagy az opcionális menedzsmentadapter.

– Legyen megfelelő garanciája!
Az eszköz 3 év garanciával rendelkezik, következő munkanapi megjelenéssel. Igény esetén ez a szolgáltatási szint opcionálisan tovább bővíthető!

A megoldás: az IBM System x3200 szerver konfigurációja!

Intel Xeon 3040 Dual Core 1,87 GHz processzor

2x 512 MB PC2-5300 DDR2 memória

2x 250 GB üzem közben cserélhető, SATA-II diszk

Integrált Raid-0, Raid-1 funkcionalitás

CD-RW/DVD-ROM meghajtó

1 GB ethernetadapter

Integrált menedzsmentkontroller

400 W fix tápegység

3 év helyszíni garancia

A konfiguráció bruttó ára:

269 900 Ft

Vásárlási szándéka esetén keresse IBM partnereinket: http://www.ibm.com/hu/partners/systemx/
További információ: http://www.ibm.com/hu vagy http://www.ibm.com/businesscenter/smb/hu/hu/drumbeat
Az akció érvényessége: 2008. február 6. és 2008. március 31. között, vagy a készlet erejéig!
A megoldás: az IBM System x3200 szerver konfigurációja!

Az ajánlat 2008. március 31-ig érvényes. Az árfolyamváltozásból eredő árváltozás jogát az IBM fenntartja. A viszonteladók egyéni árképzése miatt a végső ár változhat. Jelen akció kizárja bármely más promóció vagy különleges feltétel érvényességét. Az IBM fenntartja a jogot az ajánlat előzetes bejelentés nélküli megváltoztatására vagy visszavonására.

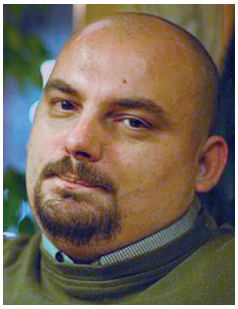
Avnet Technology Solutions Kft.
H - 1117 Budapest, Budafoki út 91-93. IP West Irodaház
Telefon: 06 1 888 2333
Fax: 06 1 888 2334
E-mail: ats.hu@avnet.com
Web: www.avnet.hu

AVNET

IBM Premier Business Partner

NINCS MEGÁLLÁS

A változás tekinthető stabil tényezőnek.



Gál Tamás
szakmai vezető, Windows Server 2008
Microsoft Magyarország

Ha egy matematikus vagy egy történelem szakos tanár a szakmájának 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 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.

Ha szűkebb világunkba látó szemmel tekintünk, akkor azt kell látnunk, hogy mostanság különösen jelentős változások előtt állunk. Kevesebb mint másfél éve jelent meg a Windows Vista, ami a korábbiaktól teljesen eltérő ügyfél-operációsrendszer lett, ezért érthetően idő kell az érvényesüléséhez – no meg egy jó első szervizcsomag: már itt is kopogtat az ajtónkon. Ami viszont nekünk nem kopogás, hanem inkább dörömbölés, az a Windows Server 2008, e számunk kiemelt témája. Szintén 5 év fejlesztés eredménye ez a termék, emellett az első Windows Server R2-változat és a Vista kapcsán szerzett összes tapasztalat és tudás benne van. RODC, NAP, Hyper-V, DFS-R, ADFS, WDS, IIS7, WSRM, NLB, AD CS, TS RA és WA – és még rengeteg újdonság, praktikus és hasznos finomítás, tehát újra rengeteg tanulnivaló. Ehhez a magazinon kívül, a következő időszakban megrendezendő előadások, screencastok és online cikkek formájában mi is hozzájárulunk. Egy (két) szóval tehát: nincs megállás...

Neked lehetőség. Nekünk kihívás.™

Microsoft®

Windows az asztalodon.
Windows a zsebedben.

HTC Touch

Élvezd a Windows előnyeit az irodán kívül is!

www.WindowsMobile.com

Az elérhető programok, funkciók és szolgáltatások a készülék típusától, Windows Mobile operációs rendszer verziótól és szervertípustól függően változhatnak. Bizonyos készülékekhez a Microsoft Office Mobile programot külön meg kell vásárolni. Kapcsolódáshoz és a szinkronizáláshoz szükség lehet külön megvásárolható termékekre és/vagy vezeték nélküli eszközökre (pl. Wi-Fi kártya, hálózati szoftver, szerver és/vagy átirányító szoftver). Internet, Wi-Fi és telefonos hozzáféréshez szolgáltatási terv szükséges. A használható funkciók és a teljesítmény szolgáltatónként eltérhet, hálózati korlátozások befolyásolhatják. További részleteket megtudhatnak a készülék gyártójától, a szolgáltatótól és/vagy a rendszergazdától.

Címlapon

Windows Server 2008

Infrastruktúra

Alkalmazásplatform

TechNet MAGAZIN

SZERKESZTŐSÉG
Főszerkesztő
Sziebig Andrea – *asziebig@itbusiness.hu*
Szakmai lektor
Budai Péter – *i-pbudai@microsoft.com*
Vezető szerkesztő
Varga János – *jvarga@itbusiness.hu*
Nyomdai előkészítés
Graffaello Kft.
Korrektor
Matula Zsolt
Lapterv és címlap
Emotion Bt.

Szerkesztőség és kiadó címe
IT-Business Publishing Kft.
1072 Budapest, Rákóczi út 28.
Tel.: 577-7970, fax: 577-7995

KIADÓ
Kiadja a Microsoft Magyarország megbízásából az IT-Business Publishing Kft.

A kiadásért felel
Sziebig Andrea ügyvezető
asziebig@itbusiness.hu
Tel.: 577-7999, fax: 577-7995

Médiareferensek
Németh Krisztina – knemeth@itbusiness.hu, tel.: 577-7973
Oláh Bernadette – bolah@itbusiness.hu, tel.: 577-7972
Rátóti Sarolta – sratoti@itbusiness.hu, tel.: 577-7971

Fax: 577-7995

Terjesztés
Terjesztett példányszám: 4500

Előfizethető a kiadó ügyfélszolgálatán:
terjesztés@itbusiness.hu
Az éves előfizetés díja 4990 forint.
MCP-k számára ingyenes!

Nyomda:
Pauker Nyomdaipari Kft.
1047 Budapest, Baross utca 11-15.
Felelős vezető: Vértes Gábor ügyvezető igazgató
ISSN 1586-5185

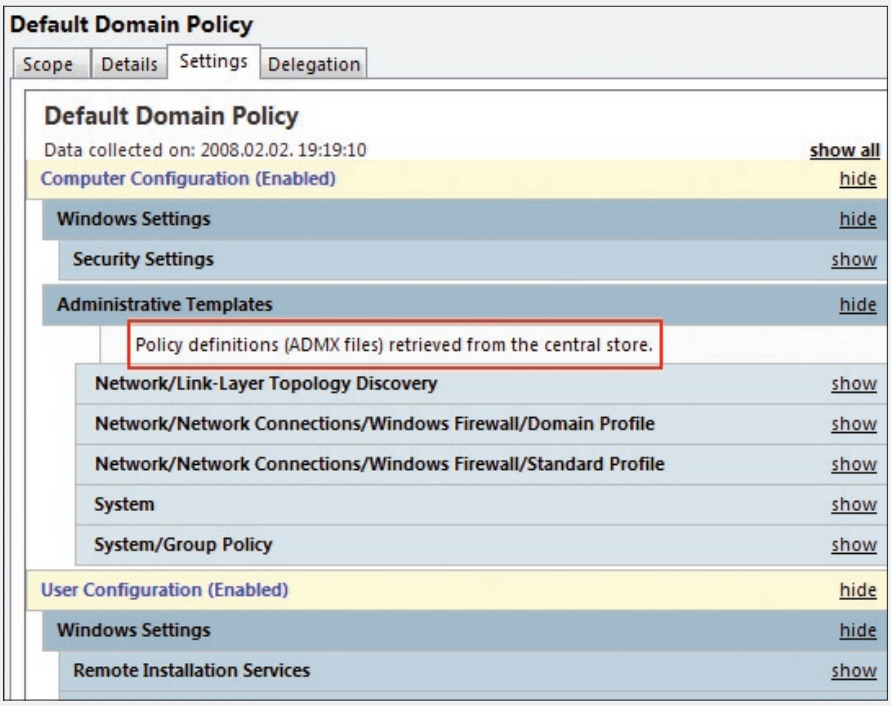
A Csoport-házirend

Adu ász a Windows Server 2008 esetén is.

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 házirendopciókkal, és sok-sok időt és energiát meg tudunk spórolni az energikus Csoportházirend-használattal.

Legfontosabb előnye az egy helyről történő, központi kezelés és a hatókör, azaz akár az összes számítógépre és felhasználóra érvényesíthető beállítások lehetősége. 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 beállításgyűjteményt? Szerencsére igen, ennek több biztosítéka is van, például a címtárszolgáltatáshoz hangolt működés és a közösen használt hierarchia.

Így aztán – akár öt, akár ötezer gép vagy felhasználó esetében – ha van tartományunk, telephelyünk stb., a Csoportházirend adu ászként az asztalunkon hever, csak fel kell fordítani.



1. kép. A szimpla vistás GPMC-ben is látható, hogy van Central Store-unk (a kép egy Windows 2003-as tartományban készült)

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 testre szabott 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 valószínűleg a legtöbbet tudunk spórolni az idővel és az energiával.

A Csoportházirend evolúciója a Windows 2000 Server/Professional párossal kezdődött (ami előtte volt, arról inkább hallgassunk). E két operációs rendszer viszonyában körülbelül 630 beállítás állt a rendelkezésünkre, ami megdöbbentően nagy mennyiségnek bizonyult akkoriban. Azóta viszont minden operációsrendszer-váltáskor, illetve szinte minden szervizcsomag esetén növekedést lehetett tapasztalni, amely egyrészt az egyre „okosabb" opciók kiötléséből, másrészt a szaporodó új komponensek lehetőségeinek lefedéséből következik. Ma (még a Windows Server 2008 előtt), a Vista-tartományban használható házirend opcióinak száma 2400 körüli (XPSP2-vel pedig körülbelül 1800), szóval bátran mondhatjuk, hogy eléggé aprólékosan szabályozható.

WS08-újdonságok

A „fejlődés folyamatos" kijelentés közhelynek számít ugyan, de igaz. Gondolkodjunk logikusan: a Csoportházirend a kliensekben megtalálható komponensek és szolgáltatások lehetőségeinek a szabályozását jelenti. Ha újabb és újabb elemek jelennek meg egy újabb operációs rendszerben, ezeket célszerű – majdhogynem kötelező – lekövetni a házirendopciók között is. Ez pontosan így volt eddig is, sőt egy-egy operációs rendszer szervizcsomagja vagy akár egy-egy új Office-verzió kapcsán is. Ezért van az, hogy a WS08-ban már alapértelmezés szerint is 3000 körüli opcióról beszélünk. Ez mindenféle szempontból irdatlanul, áttekinthetetlenül sok, de szerencsére a bővülő opciókon kívül – hosszú idő után először – jó pár kellemes és kényelmes változást tapasztalhatunk a működéssel, a kezeléssel, illetve a felügyelettel kapcsolatban is. Az újdonságokat első körben felsorolásszе-

rűen szeretném bemutatni, majd rátérünk a részletezésre is:

- Central Store;
- az új GPMC;
- szűrés, kommentek, valamint az „All Settings” nézet;
- starter GPO-k;
- Group Policy Preferences.

A Central Store

Vizsgáljunk meg első körben egy olyan változást, amely nem kizárólagosan a Windows Server 2008-hoz kötődik, azaz Windows 2000/2003 esetén is lehetséges bevezetni, de ha már jelenleg is vannak Vista-klienseink és/vagy ha majd Windows 2008-szervereink is lesznek, mindenképpen célszerű lesz használni. Messziről kell elkezdenünk, mivel a Central Store kialakításának az egyik előzménye 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 az a SYSVOL mappa túlterhelése. Azaz ha egy 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, körülbelül 4 megabájt méretben, teljesen üres állapotban – többször tíz, esetleg még több GPO esetén (akkor is, ha egyetlen beállítást teszünk meg), számolnunk kell az újabb 4 megabájttal. Replikáció, telephelyek, alacsony sávszélesség, mondjam tovább? Pazarlás, az biztos. Nevet is adtak ennek a jelenségnek, ez az úgynevezett 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 XML alapú, tartalmában a nyelvi elnevezésektől teljesen elválasztott .admx fájlunk van a Windows\PolicyDefinitions mappában minden egyes Vistán, illetve Windows Server 2008-on.

Plusz ugyanebben a mappában lehetnek még további mappák is, a nyelvi fájloknak (.adml), amelyekből értelemszerűen szintén 132 darab van. Ezek elnevezése nem tetszőleges, a mappa neve kötelezően csak az adott nyelvre egyértelműen utaló rövidített változat lehet, például En-US, hu-HU stb.

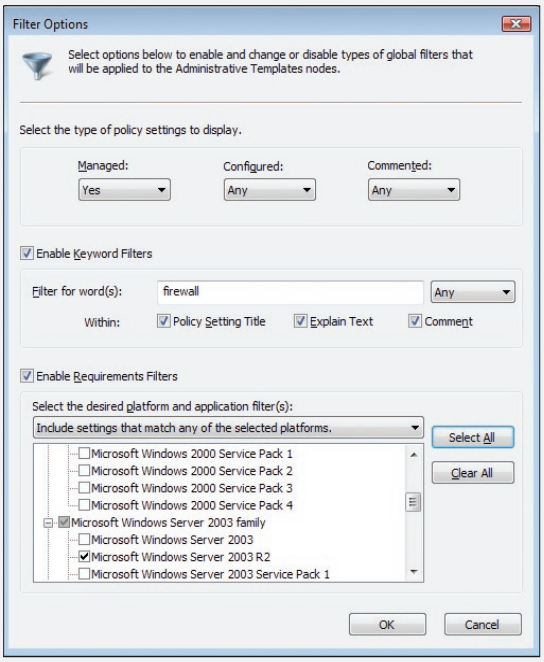
Nos, el is érkeztünk végre a lényeghez, ha vesszük a bátorságot, és ezt az egész szerkezetet (a PolicyDefinitions mappát) bemásoljuk a tartományunk PDC FSMO-val rendelkező DC-jére, a SYSVOL mappába, akkor nincs sablontöbbszörözés, nincs pazarlás, kisebb a replikációs forgalom, mindenki örül. Konkrétan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

```
SYSVOL\sajat.domain\Policies
```

A másolásba vegyük be a tartományunkban lévő összes nyelvű Vista vagy Windows 2008 saját .adml állományait is az említett mappákon keresztül. Ha majd frissíteni kell (például a Vista SP1 jelenleg 134 darab sablonfájllal rendelkezik), akkor pedig csak felülírjuk, és kész. Innentől kezdve az újabb operációs rendszerek automatikusan észrevesszik majd, hogy van központi tároló, és nem is használják majd a helyben letett sablonfájlokat egyáltalán.

A Central Store kialakításához a kézi másolás is működik és támogatott (KB929841), de ha ez bármilyen okból nem megy, van hozzá egy segédeszköz is (Vista Central Store Creator Utility), amely a következő címen található blogról letölthető: http://www.gpoguy.com/cssu.htm.

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 (http://tinyurl.com/ydb6ub).



2. kép. Szűrés, nagyon alaposan

A GPMC új változata

A lassan másfél éve publikus Vistában is megtalálhattuk a Group Policy Management Console nevezetű MMC-t, azaz már csak a 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, ez tény). Ma már viszont integrált, a WS08-ban elsődlegesen tehát ezt a keretprogramot használjuk, igaz, itt is telepíteni kell a Server Managerrel – a modularitás elveinek megfelelően (leszámítva a forest root DC-t, amelyre a tapasztalataink szerint felkerül automatikusan). Kliensoldalon ellenben kicsit cifrább a helyzet, mert a Vista alapból tartalmazza, a Vista SP1-ből viszont kikerült. Ennek több oka is van, például az, hogy a Vista-féle GPMC-nél a WS08-féle újabb, és többet tud, viszont azért ne csüggedjünk: az új „Adminpackot” a WS08-cal együtt érkező RSAT (Remote Server Administration Tools) tartalmazza, tehát ha a rendszergazda a saját gépére felrakja ezt a csomagot, akkor az összes többi felügyeleti eszköz mellett az új GPMC-t is használhatja.

(Megjegyzés: azért ne feledkezzünk meg arról sem, hogy az RSAT-ot – és így az új GPMC-t – jelen helyzet szerint kizárólag a Vista SP1-re lehet feltenni, tehát a kör bezárult, frissítsünk!)

Keresés, szűrés

Nos tehát, melyek azok az előnyök, amelyek miatt megéri ilyen bonyolult módon előkészíteni és körbejárni a GPMC használatát? Például a keresés vagy inkább szű-

rés. Sok éve és sok mindenre használom a Csoportházirendet, de azért van, hogy egy ismerős opciót percekig keresek feldúltan, de a 2273-as tanfolyamon – a kezdeti Csoportházirend-kábulat után – a hallgatók első és teljesen logikus kérdése is mindig ezzel kapcsolatos. No és ez persze még ennél rosszabb lenne a WS08-ban, a több mint 3000 opció miatt.

Még abban az esetben is, ha a Vista-házirendből megismert módon itt is nagyon részletes a szerkezet, 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.

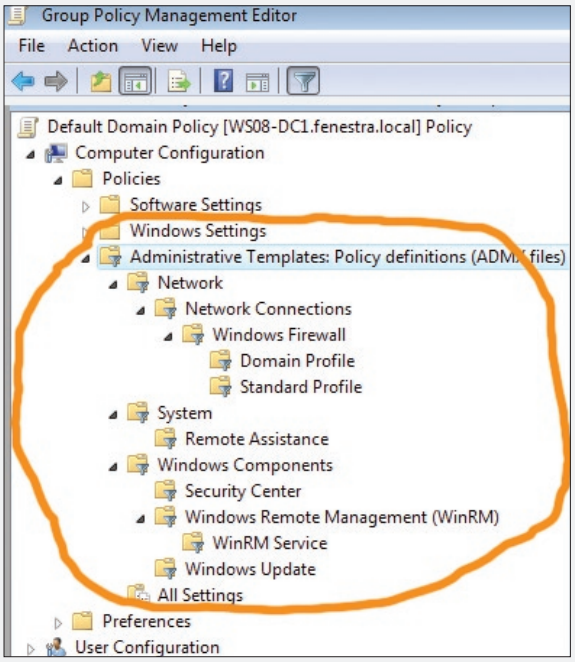
De ez nem elég, jó párszor előfordul, hogy egy-egy komponenssel kapcsolatos beállítások eltérő helyeken is megtalálhatók, és pont a miatt az egyetlen más helyen megtalálható plusz beállítás miatt nem működik a jól kitalált „felhasználókínzó" elképzelésünk.

Szóval, ha minden egyes opciót szeretnénk látni, ami például a „firewall"-lal kapcsolatos, akkor az új GPMC-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 a keresett szavakat magukban foglaló opciókat tartalmazzák.

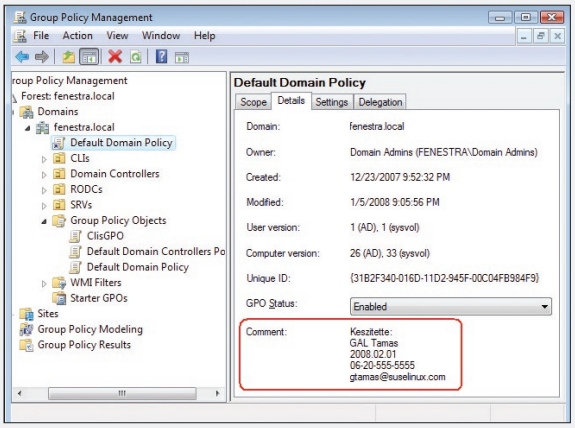
A Filtering panelt jobban megvizsgálva találhatunk jó pár érdekességet. Szűkíthetjük a keresést az „igazi", azaz a menedzselhető opciókra, vagy mondhatjuk azt is, hogy csak azok a beállítások érdekelnek bennünket, amelyekhez már korábban hozzányúltunk, de szűrési opció lehet a felhasználói megjegyzések megléte is (erről majd később).

Ha kulcsszót írunk be, akkor nemcsak az adott beállítás szövegében, hanem a gyári magyarázatokban, illetve a felhasználói megjegyzésekben is kereshetünk (ezek miatt látszik annyiféle találat a *2. 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, 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 dolognak, pedig az.



3. kép. A szűrés eredménye a bal oldali keretben



4. kép. Könnyű eligazodni a GPO-k között is

Ha többen hangoljuk a Csoportházirendet, akkor – lelkiismeretes munkát, rendes kommentezést feltételezve – 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 – amire így talán nem lesz szükség.

Egyébként az Administrative Templates szakaszon kívül még egy 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 (Notepaddel szerkeszthetően) megtalálhatók az adott GPO mappájában, a SYSVOL-on belül. 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 körülbelül 1400 darab, nagyjából egyforma opciót a jobb oldali keretben láthatjuk, alapesetben ábécé-sorrendben, de van lehetőség rendezni az opció állapota, az esetleges kommentek vagy az elérési útvonal szerint is. 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).

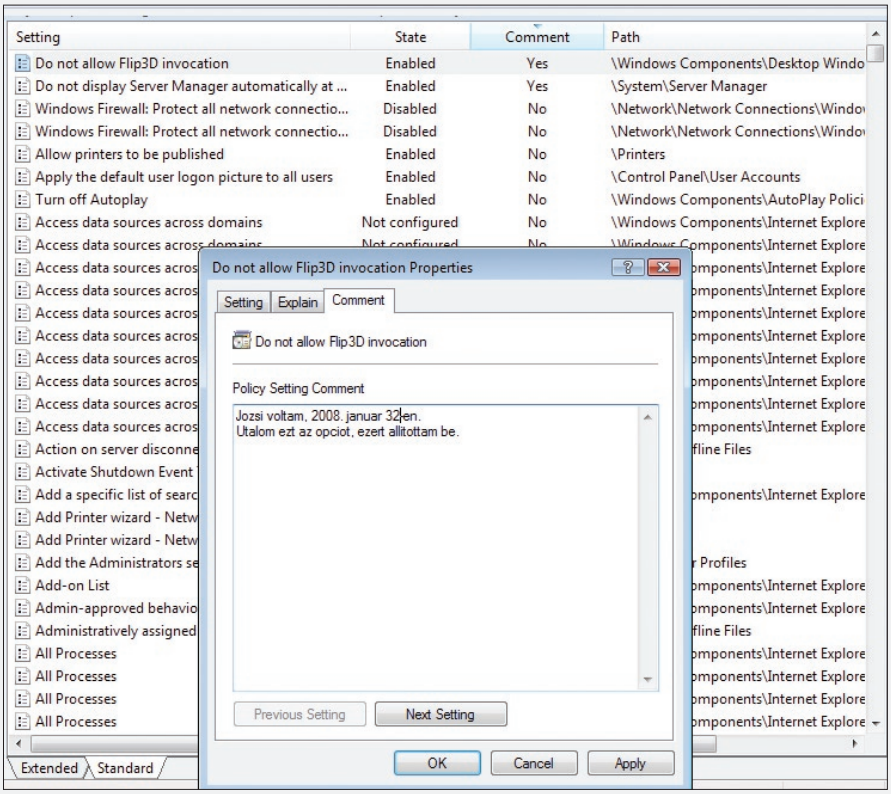
Az Explain text, azaz a gyári „magyarázó" szöveg kibővítése is ehhez a témához tartozik még, sok-sok helyen újraírták, értelmesebbé és használhatóbbá tették, ergo érdemes időnként megnézni. (Megjegyzés: ha valamivel ezekben nem értünk egyet, hibát találunk benne, vagy jobbat tudunk írni, akkor a Group Policy Team szívesen fogadja az alternatívákat a gptext@microsoft.com e-mail-címen.)

GPMC – Startup GPO

Képzeljük el, hogy szükségünk van 5 darab GPO-ra, amelyekben egyenként 100-100 opciót fogunk beállítani. A 100-ból 50 ugyanaz lesz (mert mondjuk ezek a céges alapkövetelmények), a maradék 50-nek viszont teljesen

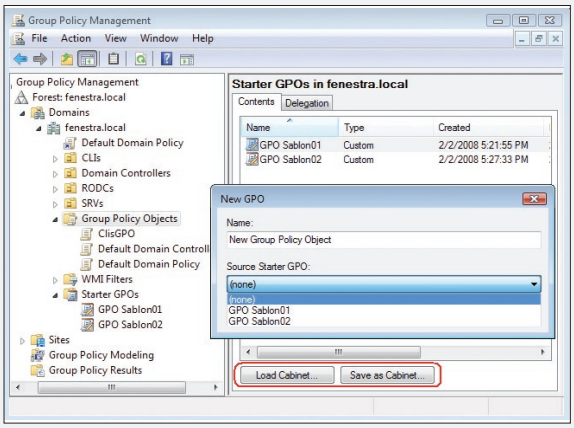
eltérőnek kell lennie. Mit csinálunk? Régóta vannak már sablonjaink (lásd: Security Templates MMC) a Csoportházirendhez, de ezek biztonsági sablonok, az Administrative Templates szakaszra nem vonatkoznak, nekünk pedig kifejezetten a gépek és a felhasználók környezetével és a komponensekkel kapcsolatos konkrét beállításokra lenne szükségünk...

ehhez is). Ezután elkezdhetjük létrehozni az első sablont, amelyben láthatóan nincs is más, mint a két Administrative Templates szakasz. (Azért ne becsüljük le ezt a jelen-



5. kép. All Settings nézet, kommentek szerint rendezve és egy fontos megjegyzés az adott beállításon

Nos, a Windows Server 2008-tól kezdve használhatjuk erre a célra az úgynevezett Starter GPO-kat. Ezek is egyfajta sablonok, amelyeket nekünk kell előzetesen és egyszer elkészíteni (a rendszerrel egy darab sem érkezik, ez is 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 leg körülbelül 2700 opciót tartalmazó részt!) Ha megtesszük a szükséges alapbeállításokat, és bezárjuk az új sablonunkat, akkor egy új GPO készítése előtt akár választhatunk is e sablonok közül kiindulópontként egyet, és máris lesz, mondjuk – a példa szerinti helyzetben – 50 beállításunk.



6. kép. A Starter GPO felhasználása

Szeretném felhívni a figyelmet a piros keretben szereplő két nyomógombra. Szerepük fontos, mivel a hordozhatóságot szolgálják, azaz ha egy Starter GPO-t elmentjük .cab formátumba, akkor egy másik rendszerben is elérhetővé tudjuk tenni a „Load Cabinet" paranccsal. Ezek ismeretében szimpla ügy lesz felszerelni magunkat néhány hasznos Starter GPO-val.

Group Policy Preferences

A Microsoft 2006 őszén megvásárolta a Desktop Standard nevű céget, amelynek volt egy remek alkalmazása – lehet, hogy ismerős többeknek, ez volt a PolicyMaker. Nos, ezt az alkalmazást jelentősen átírták és testre szabták, majd teljesen beépítették a Windows Server 2008-ba (illetve az RSAT-ba is), és immár Group Policy Preferences néven fut. Annyira fontos és annyira más, hogy a GPO-kban egy teljesen külön főágat kapott. Még akkor is így van ez, ha összesen csupán körülbelül 90-100 opciót tartalmaz, tehát a mennyiséget tekintve nem mérhető össze a hagyományos házirendekkel. De más szempontból sem, hatása ugyanis 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 alapházirendeknél).

Amit még meg kell jegyeznünk, hogy ha egy hagyományos házirendopció és egy Preferences opció „összeakad", akkor mindig a hagyományos „nyer", de ez logikus is.

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

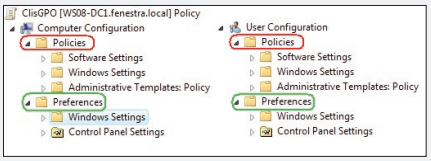
Environment szakasz. Létrehozhatunk, módosíthatunk, kicserélhetünk és törölhetünk környezeti változókat.

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 például 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-

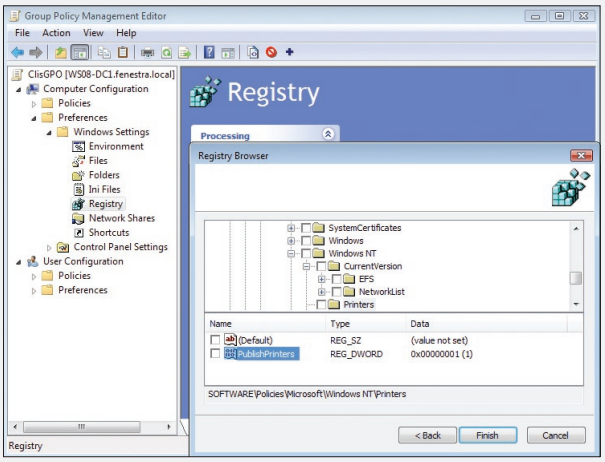


7. kép. Policies és Preferences 2x is egy-egy GPO-n belül

típust érintve – szemben a régi sablonok fapados lehetőségeivel.

Sőt, elindíthatunk egy varázslót is, amelyel csatlakozhatunk a távoli géphez, így „élesben" tudunk változtatni a registry értékein (ehhez persze a távoli gépen futnia kell a Remote Registry szerviznek, a Vistán ez már nem alapértelmezett).

Network Shares. Létrehozhatunk hálózati megosztásokat is, minden egyes, a klasszikus módon is elérhető jellemzőjével együtt, sőt az



8. kép. Működik a klienshez kapcsolódó éles registry-varázsló

Access-based Enumeration (magyarul: csak azt látja a felhasználó, amihez van jogosultsága) opciók is elérhetők.

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 találhatók meg.

Data Source. Létrehozhatunk, módosíthatunk, frissíthetünk és törölhetünk DSN-eket és az 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 Option. Kicsit más, mint fent, a fájltípusok, a fájlösszerendelések 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, elérhetők a tárcsázási, a hitelesítési és egyéb opciók is. Ha már van VPN-kapcsolatunk azon a gépen, amelyiken konfiguráljuk a GPP-t, azt például beimportálhatjuk, elképesztő...

Power Options. Itt gyárthatunk opciókat és sémákat az energiaellátás opciókörében (csak Windows XP esetén).

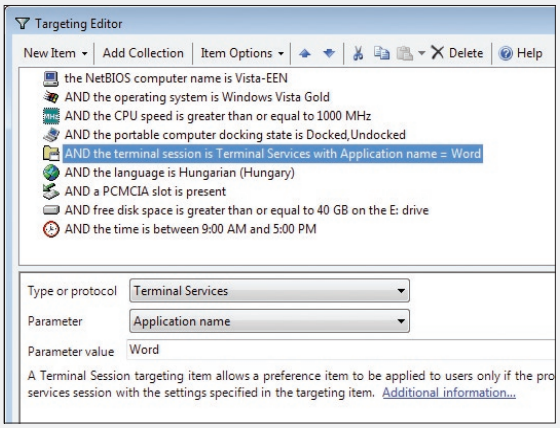
Printers. TCP/IP- és lokális (!) nyomtatókat hozhatunk létre. LPT/USB/COM-portokat, IP-címet és minden más nyomtatótulajdonságot is konfigurálhatunk itt.

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.

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, nézzék meg önszorgalomból, megéri.

Attól viszont nem, hogy bemutassak még



9. kép. Szerfelett granuláris feltételek – csoportba szedve

egy fontos komponenst, az úgynevezett Target Editort, amelyet minden beállításnál megtalálunk (a Common fülről érhető el), és amellyel egyszerűen és látványosan szűkíthetjük a beállított opciónk hatókörét. A *9. képhez* értelmetlen feltételeket szedtem össze, a lényeg nem is ez, hanem a sokszínűség, még legalább háromszor ennyi lehetőség van, ezeket nagyon egyszerűen összepakolhatjuk egy közös feltételrendszerré (szóval nem kell a WMI-vel kínlódnunk). Ami lemaradt a képről, pedig különösen fontos, az a szűrés lehetősége a csoportokra, illetve az egyéni felhasználókra.

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 úgynevezett Client-Side Extension (CSE) segítségével működik a GPP. A Vista SP1, illetve az XPSP3 és a CSE viszonya bétaállapotuk miatt jelen pillanatban meg kérdéses, de a hírek szerint a várakozásunk ellenére ezekben sem lesz benne gyárilag (de szerintem a MU/WU/WSUS szórásba egyébként is bekerül majd).

Gál Tamás
(v-tagal@microsoft.com)
Microsoft Magyarország

METAMORFÓZIS

Már jó pár éve szemezek Ovidius Átváltozások című könyvével. Szívesen elolvasnám, de valahogy mindig tolódik a terv. Most éppen a Windows Server 2008 Failover Cluster funkciójának megismerése köti le az időmet. Bár amilyen átváltozáson átesett ez a szoftverkód, akár még a fent említett műben is szerepelhetne…

Mert minek is nevezhetnénk azt a változást, amelynek révén a telepítési, a hálózati, a lemezkezelési, Quorum-kezelési és a GUI alrendszert is teljesen újraírták? Még a szolgáltatás – bocsánat: képesség (feature) – neve is megváltozott. Már nem Microsoft Cluster Server (MSCS) vagy Server Cluster, hanem „Failover Cluster". Kattintgatva az MMC ikonjain, azon gondolkodtam, mi nem változott?

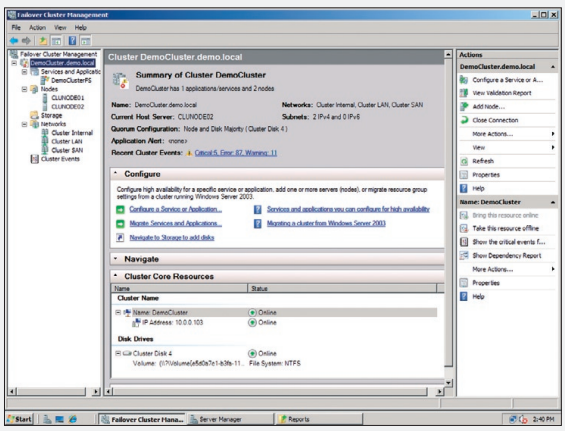
Egy hajdanvolt cikksorozat – Failover Cluster 2002-es szemmel

No, igen. Az, hogy milyen volt a fürtszolgáltatás, egész jól tudjuk. A *TechNet Magazinnak* meglehetősen kedves ez a téma: 2001-ben és 2002-ben mindösszesen tizenhárom cikkben taglaltuk a szoftver képességeit. (A „véletlen" úgy hozta, hogy a jelen írás és a korábbi cikksorozat szerzője azonos.) Van tehát egyfajta előkép, és bár szerettük, azért kritikával is illettük mindazt, amit láttunk. Íme, két idézet az egykori tapasztalatokról:

„A Cluster telepítésének inkább NT4-es formája és érzete van, mint Windows 2000-es. Ez a „gyanú" később igazolódni fog: A Windows 2000-ben nagyon sok mindent átírtak, és nagyon sokat fejlesztettek, beleértve a Cluster szolgáltatást is, mégis maradt jócskán tennivaló a következő kiadásig." (2001. december – II. rész)

„A fürtszolgáltatás, úgy tűnik, mindig egy lépéssel az újdonságok mögött jár. Az eredeti Windows 2000 fürt, akárcsak a korábbi NT4 verzió, lemezszignatúrákat használ, nem ismeri a dinamikus diszkeket, a lemezcsatolás módszerét, ragaszkodik a lemezek betűjeleihez, NTLM hitelesítést alkalmaz, az FRS szolgáltatással hadilábon áll, még a telepítése is olyan 'NT4 szagú'. A sok hiányosságból most az egyik, a hitelesítés, kicsit közelít a 'normális' Windows 2000 szintjéhez." (2002. december – XIII. rész)

Ezeken túl 2002 decemberében – a további idézeteket elhagyva – hiányoltuk a DFS–FRS-Cluster integrációt, az IPv6-támogatást, a GPT-lemezek használatát, a kizárólagos Kerberos hitelesítést, és a cluster.log dokumentálatlanságát. Összegezve: a fürtszolgáltatás bevezetésekor mindeddig egy nagy kompromisszumot kellett kötnünk. A magas rendelkezésre állásért cserébe bizonyos innovatív képességekről lemondtunk, ami főleg a biztonságot növelő képességek esetén fájt, és lépten-nyomon hiányzó puzzle-darabkák akadályozták, hogy teljes értékű rendszerünk legyen. Mindennek fényében különösen izgalmas, mit hoz a 2008-as esztendő Windows-verziója.



1. kép. A Failover Cluster megújult MMC konzolja

Visszatérve az MMC kezdő képernyőjéhez: a sokéves tapasztalat ellenére, az első percekben elvesztem. Ez lenne a Failover Cluster?

Itt már semmi sincs úgy, mint régen… Aztán némi akklimatizáció után rájöttem, nem olyan ijesztő a dolog. Bár külsőleg minden új, az alapok változatlanok.

Az architektúra elve továbbra is a „semmi sem közös" (shared-nothing). Az építőkövek az erőforrások, az erőforrás-csoportok és a függőségek. A mechanizmusok lényege maradt a régi: átköltözés (failover), visszaköltözés (failback), sőt még olyan funkciókat is viszontláthatunk, mint az IsAlive/LooksAlive.

Az alapokon túl azonban az ugrás óriási, érdemes tehát nem hagyatkozni a régi beidegződésekre, a képességek újratanulását nem kerülhetjük el.

Megváltozott környezet – a szerepek kiegészítése

A Failover Cluster megértését kezdjük a környezetének megértésével. A Windows Server 2008 elhozta számunkra a szerepek (roles) és képességek (features) világát. Már nem egyedi szolgáltatásokkal (Windows service) bajlódunk, magasabb fogalmi egységgel, a szerep-

pel kell megküzdenünk. Egy „File Server” szerep, vagy egy „Print Server” szerep telepítésekor a rendszer tudja, milyen egyedi szolgáltatásokat kell telepíteni. A Failover Cluster nem szerep, hanem képesség vagy tulajdonság (feature). Önmagában semmire sem való; egy konkrét szerepet egészít ki magas rendelkezésre állási képességgel. Vagyis, bár önmagában telepíthető, az erőforrások csak akkor hozhatók létre, ha azok szerepkörét előzőleg felraktuk. Példa: a DFS NameSpace egy fürtözhető erőforrás, ám ha nem telepítjük a File Server szerepkör szerepkör-szolgáltatásaként (role service), nem hozhatunk létre ilyen erőforrást sem – végül is érthető. A lényeg: a Failover Cluster tökéletesen érti a környezetét és annak fogalmait, azokkal szorosan integrált.

A fürtadminisztrátorok két szempontból is profitálhatnak a fentiekből. Egyrészt nagyon jól lehet majd tudni, hogy egy fürttagon „mi van fent”, a konfiguráció jobban átlátható. Másrészt, ha a Failover Cluster mindent ért, akkor teljes egészében kompatibilis a „Server Core” telepítési móddal is – és valóban: ott éppúgy működik, mint a teljes telepítéskor. Az első piros pont: a Server Core nyújtotta kisebb erőforrásigényről, kisebb sérülékenységről, kevesebb hotfixről nem kell lemondanunk annak érdekében, hogy magas rendelkezésre állásunk legyen. Ugyanakkor ebből egy egészen más implementációs kényszermegoldás is következik: a Failover Cluster parancssori felülete nem Powershell alapú. És ezúttal nem a Cluster-csapat maradt le. Ha a Server Core-támogatás követelmény, a parancssori felület szintén, a Server Core-on viszont a Powershell (legalábbis a Windows Server 2008 verzióban) nem működik, abból az következik, hogy a fürtszolgáltatás parancssori felülete sem lehet Powershell alapú – hiába a WMI-barát szerkezet.

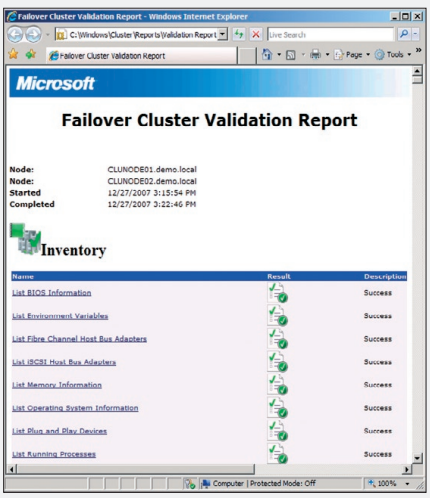
Végül még egy példa a környezettel való összenövésre. Ha létrehoztunk egy magas rendelkezésre állású File Server szerepkört egy fürtön, majd ezután megosztunk egy mappát a Windows Explorer segítségével, a megosztás automatikusan fürtözött megosztás lesz! (Vigyázat! A megosztás már nem erőforrás!) A fürt ugyanis tudja, hogy az adott lemez, amelyen a megosztás létrejött, melyik erőforráscsoporthoz tartozik, tehát magát a megosztást is oda helyezi. Vagyis nem fordulhat elő, hogy egy fürtön megosztott mappa nem fürtözött mappa. És fordítva: nem szükséges a cluster administrator mmc elindítása a fürtözött szolgáltatás létrehozásához. Na, ez integráció!

Telepítés

A fürtöket többnyire ott rontották, rontják el, ahol ez először lehetséges, a telepítésnél. Vagy azért, mert eleve nem támogatott hardver szolgál alapul, vagy mert nem értik pontosan a fürt működését, és rosszul paraméterezik azt. A Windows Server 2003-ba a korábbi kiadásokhoz képest sokkal szofisztikáltabb telepítő, pontosabban inicializáló modul került, de még itt is érvényes a szabály: csak azonos gyártótól származó, Cluster-kompatibilitási listán szereplő alkatrészekből építkezhetünk.

Jelentem, ennek vége. A telepítés során egy nagyon alapos, összetett rendszer esetén akár egy óránál is tovább futó validációs teszt eldönti, hogy az általunk fabrikált gépezeten működik-e majd a fürtünk vagy sem. Ha a teszt eredménye szerint működik, akkor szedett-vedett hardver ide, HCL oda, az egy, a Microsoft által is támogatott fürt lesz.

Sőt! Ha földrajzilag elosztott fürtöt építünk és ezért a storage-teszt figyelmezető üzenettel fejeződik be, még ebben az esetben is a támogatott kategóriába esik a konfigurációnk. A Cluster HCL pedig füstté vált. Nincs többé. Nyomtassuk ki és tegyük el a validációs jelentést, mert azt később meglobogtathatjuk a megfelelő támogatási szerződés meglétekor. Mindez egyébként azért vált lehetségessé, mert mind a lemezkezelés, mind pedig a hálózatkezelés alapos revízión



2. kép. Validációs teszt – működni fog a cluster

esett át, a fejlesztők pedig gondosan eliminálták a hibalehetőségeket, így már belezsúfolható egyetlen tesztbe minden szükséges ellenőrzés.

A telepítés folyamata 3-4 lépésből áll, és egyszerre végrehajtódik az összes, általunk kijelölt node-on. A telepítés most első alkalommal teljes egészében scriptelhető – nagymértékben javítva ezzel az implementálás tervezését, a változáskezelést és a katasztrófahelyzetek megoldását –, és hol máshol lenne erre a legnagyobb szükség, mint éppen a fürtöknél?

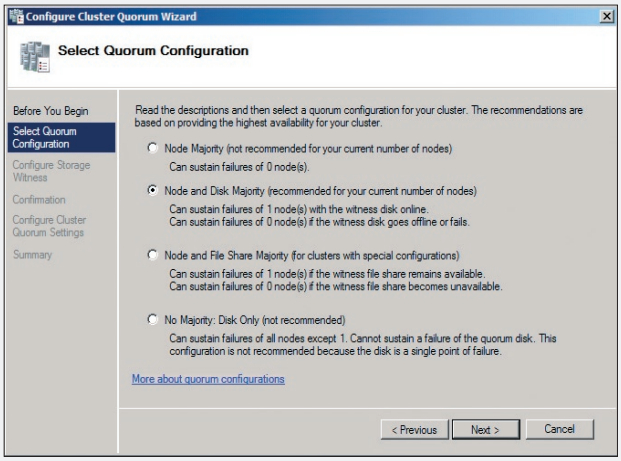
Első benyomások – MMC

A fürtszolgáltatás végre valódi MMC-konzolt kapott – eddig egy MMC-t utánzó exe-állomány (Apage Satana!) nyújtotta a grafikus felületet. A bal oldali fa struktúrája Exchange 2007-es iskolában nevelkedett fejlesztőkről árulkodik: nagyon egyszerű, legfeljebb két lépcsőből álló fastruktúra, mindössze öt fő ággal: szolgáltatások és alkalmazások (az erőforráscsoportok helyett), fürttagok, tároló alrendszer, hálózat, végül pedig a fürttel kapcsolatos események. A középső panel teteje mindig egy áttekintő táblázatot tartalmaz, jobb oldalon pedig a környezetérzékeny menü, amely minden pillanatban eléggé gazdag, úgyhogy a valódi menü használatára alig van szükség. Az egész felület letisztult és feladatközpontú.

A fürt valamely objektumának létrehozását minden esetben varázslóval kell elvégezni. Ez eddig is így volt, legfeljebb a varázslási folyamat áttekintése javult, az ablakok jobban magyarázzák önmagukat. Eleinte kell is, mert számos objektum kapott új nevet. Az erőforráscsoport első hálózati neve például „Client Access Point”. Ezzel együtt a varázslókat nem éreztem idegesítőnek. Megvan a maguk helye és szerepe.

A Quorum átalakulása

A fürtök eddigi nagy kincse a Quorum volt, amely szerencsés esetben saját lemezen ült, és tulajdonképpen eredetileg nem volt más, mint egy tranzakciós rendszerrel kiegészített registry-hive. Hajdanán egyetlen Quorum-típus létezett, aztán a Windows Server 2003 megjelenésekor újabb kettő mutatkozott be (local Quorum, Majority Node Set). Még később, az Exchange 2007 megjelentetésével együtt a Microsoft kiadott egy fürt „hot-



3. kép. A Quorum típusának kiválasztása

fixet" (921181), amely varázsolt egy vadonatúj Quorum-típust. Ez megosztott mappát használ „tanúként" (file-share witness) és a Majority Node Setre emlékeztet.

Nos, a Windows Server 2008-ban a Quorum fogalma a korábbiakhoz képest felborult. Már nem registry-hive vagy lemez, vagy megosztott mappa, vagy többség, hanem mindegyik, illetve egyik sem. A legpontosabban úgy fogalmazhatok: a Quorum annak a tudása, hogy mi a Cluster, milyen a konfigurációja és milyen az aktuális állapota. Ennek a tudásnak a birtokosa – vagy birtokosai – a Quorum. Ilyen értelemben mindig csak egy Quorum van, de az lehet elosztott több node, megosztás, lemez között. Azt, hogy a fürt tagjai birtokolják-e a megfelelő tudást (értsd: a Quorumot), és így a fürt működőképes-e, szavazásos módszerrel döntik el a fürt tagjai. Implementációját tekintve a Quorum négyféleképpen működhet – azt mondhatjuk, hogy négyféle szabály szerint lehet szavazni vagy a szavazatokat kiértékelni.

Úgy érdemes elképzelni ezt, mint egy skálát, ahol a tengelyen a Quorum elosztottsága, hibatűrése változik. A típusok:

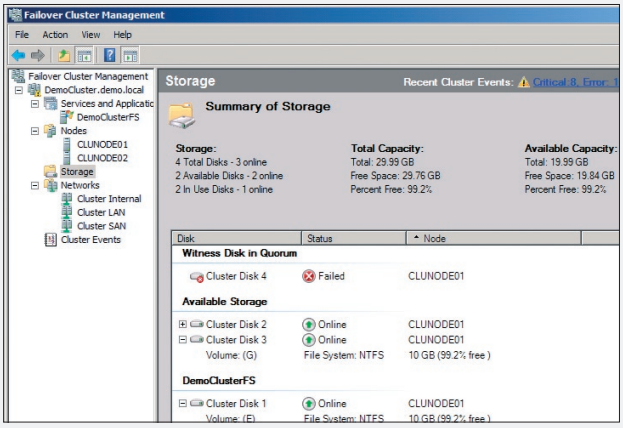
Node Majority. Ez a változat minden tekintetben megegyezik a korábbi majority node set üzemmóddal. Szavazati joguk csak a fürttagoknak van. Ha a szavazásban a többség részt vehet, akkor a fürt működik, ha nem vehet részt, akkor a fürt leáll. A fürttagok száma minimálisan 3, maximálisan 16.

Node and disk majority. Ilyen korábban nem volt. Az előző verzióhoz képest szavazati jogot kap a tanúlemez (witness disk) – a korábbi Quorum disk megfelelője. Továbbra is a többség dönt, de a tanúlemez szavazata kicsit többet ér a fürttagokénál. A fürt túléli a tagjai felének elvesztését, ha a tanúlemez működik, illetve a fürt túléli a tagjai felének –1 tagnak – a kimúlását, ha a tanúlemez az örök vadászmezőkre költözött. Példa: 4 tag + tanúlemez. Ha a tanúlemez működik, kieshet két fürttag. Ha a tanúlemez nem működik, kieshet (4/2) – 1 = 1 tag. Kéttagú fürt esetén ez azt jelenti, hogy a Cluster túléli a tanúlemez kiesését – feltéve, hogy mindkét node hibátlan!

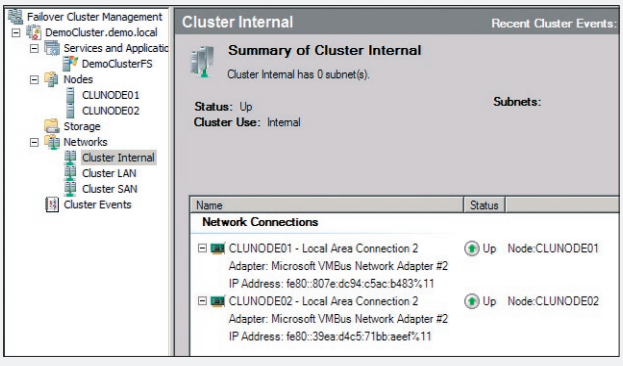
Node and File Share Majority. Pontosan úgy működik, mint az előző esetben, csak a tanúlemez helyett tanúmegosztást (file share witness) használunk. Ezt a Quorum-típust vezette be a Microsoft a 921181-es hotfixszel. Földrajzilag elosztott fürtök esetén érdemes használni. Jegyezzük meg, DFS-link nem lehet tanúmegosztás, annak viszont nincs akadálya, hogy egy másik fürt megosztása legyen tanúmegosztás. A tanúmegosztásnak nem kell azonos telephelyen lennie egyik fürtállomással sem.

No Majority: Disk Only. Ez a diktatúra... A „szavazás" úgy módosul, hogy csak a tanúlemeznek van szavazata. Amíg a tanúlemez plusz egy fürttag él, addig van fürt. A módszerben nincs semmi új, ez az eredeti Quorum-típus – hátránya, hogy maga a Quorum egypontos meghibásodást jelent egy olyan rendszerben, amely az egypontos meghibásodásokat hivatott kiküszöbölni.

A modelleket – ha megfelelő számú fürttag rendelkezésre áll – szabadon átalakíthatjuk egyikből a másikba. Elsőre furcsa, hogy az MMC-felületen a hajdani Cluster group – az első létrehozott erőforráscsoport, amely a Quorumot tartalmazta – nem látható. Végeredményben mégis jobb ez így – nem fordulhat elő, hogy erőforrásokat pakolunk bele. A fent említett 16 maximális fürttag minden üzemmódban elérhető.



4. kép. A cluster lemezeinek gyors állapot-áttekintése



5. kép. A cluster belső hálózata

A hálózat átalakulása

A Quorum átalakulásával összevethető változások történtek a fürt hálózatkezelési technikáiban is. Kezdjük azzal, hogy a fürttagoknak nem kell statikus IP-címmel rendelkezniük. Ízlés kérdése: van, aki a statikus címekre esküszik a szervereknél – én inkább a DHCP-szerver lefoglalt IP-címeit preferálom. Az központosított is meg vezérelhető is. A Failover Cluster mostantól kielégíti az általam jónak vélt módszert. Ha a külső fürtcímeknél ez nem is mindenkinek vonzó, a fürtön belüli (intra-cluster) hálózattal egész biztosan senki sem akar foglalkozni. Ezután nem is kell. Úgy működik az APIPA, hogy azt nem jelzi problémának.

Kell ennél több? Íme: vadvízi evezősök tisztán IPv6-konfigurációt állíthatnak be – mit is idéztünk a cikk elején? És még folytathatjuk: teljes a NetBIOS-függetlenség; fürtök közötti forgalom teljes titkosítása; működik a tisztán Kerberos hitelesítés, NTLMv1, NTLMv2 igény szerint kihajítható.

Régi vesszőparipám is teljesült: a fürtözött megosztások egyenrangú részei lehetnek egy DFS-névtérnek, különösen, ami a replikációt illeti. Így végre felépíthető egy olyan DFS-névtér, amelynek minden megosztása magas rendelkezésre állású, azonos tartalommal. Ezt éppen a Windows 2000 Advanced Serverbe álmodtam bele hét ével ezelőtt!

A hálózatkezelés területén az i-re a pontot a földrajzilag elosztott fürtök létrehozásának lehetősége teszi fel. Elvileg ennek eddig sem volt akadálya – ha a hálózati switcheket és az útválasztókat úgy tudtuk konfigurálni, hogy a fürtök azonos VLAN-ba kerüljenek, és azonos IP alhálózatból kapjanak címet. Ezután már csak „imádkozni kellett", hogy a hálózat válaszideje ne növekedjék egy szint fölé, amit egy fürt már nem tolerált volna. Erre a mutatványra nem lesz többé szükség: a fürttagok gond nélkül külön alhálózatban is működhetnek – hála a (parancssorból) konfigurálható heartbeat időtúllépésnek.

A lemezkezelés átalakulása

A sok újdonság között személyes kedvenceim a lemezkezeléshez kapcsolódnak. Ezt a komponenst is alapos revíziónak vetették alá, néha egészen meglepő eredményeket produkálva. De hogy jobban értsük, tekintsünk vissza egy kicsit a múltra.

A fürtszolgáltatás – ahogy azt már említettem – a „semmi sem közös" elven épült fel, és ez igaz a lemezekre is. A semmi sem közös elv az amúgy közös diszkalrendszernél azt jelenti, hogy semmit sem birtokolnak közösen egyszerre a fürt állomásai. A lemezeket mint erőforrásokat lefoglalják, és egy viszonylag bonyolult algoritmust építettek a szoftverbe, hogy a lemezek átadását, hiba esetén pedig az erőszakos átvételét kezeljék. Amikor erőszakos átvételről írok, egyáltalán nem túlzok. A Windows 2000-fürtök egyetlen lemez átvételét SCSI Bus reset paranccsal oldották meg. Mintha egy fa egy ágának lemetszését úgy végeznénk el, hogy motoros fűrésszel fentről lefelé végigsimogatnánk az egész fát. Ez jól működött 1997-ben a külső házas Parallel SCSI Direct Attached Storage rendszereknél, de a mai konszolidált SAN-világban roppant barbár megoldás. A Windows Server 2003 kulturáltabb módszert alkalmazott, de végső esetben még eleresztett egy bus resetet. A Windows Server 2008 viszont már finom úriember, a bus reset számára ismeretlen fogalom. A lemezek lefoglalására a „Persistent Reservation" módszerét használja – tároló-alrendszer vásárlásakor ezt a képességet tessék tehát árgus szemekkel figyelni, amennyiben a fürtszolgáltatás építését is a fejünkbe vesszük.

Egy kis kitérő. Fürtöt építünk. Mit is jelent ez? A fürtépítés állandó harc az Achilles-sarkok, angolul Single Point of Failure (SPoF) ellen. Van már kiszolgálónk, összekötjük egy új tárolóalrendszerrel. Összekötjük? Hányszor? Ugye, legalább duplán, az SPoF elleni védelem jegyében. Ahh, ettől a pillanattól kezdve viszont már több útvonalon is elérhetjük ugyanazokat a lemezeket, pontosabban LUN-okat.

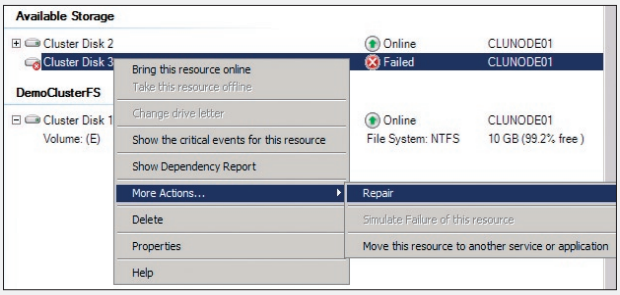
De ha már két storage-kontrollerünk van, nem lenne érdemes megosztani közöttük a terhelést a hibatűrés megtartása mellett? A Windows Server 2008-ban implementáltak egy új tulajdonságot, amely „Multipath I/O" (MPIO) névre hallgat, és a fenti problémakört oldja meg igen magas szinten. Az MPIO nem feltétele a fürtszolgáltatásnak, de tervezési szempontból a két komponens kéz a kézben jár: rendes cluster MPIO-t használ.

Az MPIO ismeri az összes aktuális és modern storage-szabványt, felsorolásszerűen: Fibre Channel (FC), iSCSI és Serial Attached (SAS). Éles szeműek rögtön láthatják, egy valami hiányzik, a Parallel SCSI. És igen, elérkeztünk a tényleges mondanivalónkhoz. A Parallel SCSI támogatása kikerült a fürtszolgáltatásból. Fáj ez nekünk? Elsőre úgy tűnik, igen. A Parallel SCSI egy kiöregedő szabvány, vagyis egyre olcsóbb, és milyen jó lenne, ha ilyen nagyon olcsó vasból építenénk legalább próbálgatásra vagy tesztelésre fürtöt. Nem fog menni. Aztán, virtuális SCSI-kártyákat használhatunk virtual server vendéggépben is, és mindeddig ez volt a fürtépítés módja virtualizált környezetben. A Windows Server 2008-tól már ez sem működik. Mi az, ami maradt? Tesztelésre, virtuális környezetre virtuális iSCSI Target, fizikai megvalósításnál pedig az FC-iSCSI-SAS hármasból bármelyik.

(Lássuk be, azért nem volt ez olyan várat-lan húzás. x64 platform alatt már a Windows Server 2003-nál sem lehetett PSCSI-t használni, ráadásul az ipar is szép lassan kidobja ezt a szabványt, ott az utód, a SAS. Viszlát deszka-cluster, viszlát PSCSI! Béke poraira!)

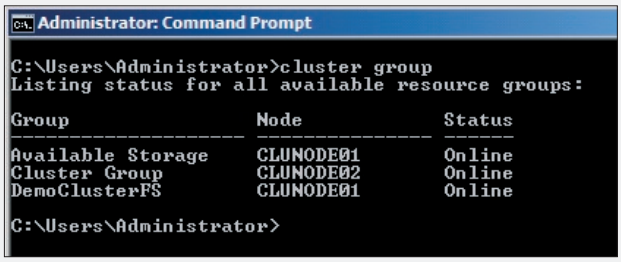
Térjünk vissza a fürt és a lemezek kezelésének témaköréhez. Hat évvel ezelőtt panaszoltuk, hogy a dinamikus lemezekről mit sem tud a fürtünk. Nos, a témába vágóan egy jó és egy rossz hírrel szolgálhatok. A rossz, hogy a Windows Server 2008 sem ismeri a dinamikus lemezeket. A jó hír, hogy ez nem baj... Mire kellenének a dinamikus lemezek? Alapvetően két célt szolgálhatnak: egy adott partíció dinamikus növelése oldható meg velük, illetve szoftveres RAID-tömböket hozhatunk létre a segítségükkel. Ez utóbbi fura igény lenne. Szoftveres RAID-et már évek óta nem láttam használni, olyan olcsó lemeztömböt hardvereszközzel megvalósítani. Ha viszont valaki tényleg templom egere, akkor kizárt dolog, hogy fürtszolgáltatásra van szüksége. A fürtszolgáltatás ugyanis önmagában sem olcsó dolog – ergo, aki létrehoz egy fürtöt, annak már nem fájhat a hardveres RAID-beruházás sem. Marad a partíció növelésének igénye. Erre a céltáblára három golyóval is lőhetünk. Először is, ma már a virtuális lemezek világát éljük, a LUN-ok, amelyeket a fürt tagjai fizikai lemeznek látnak, valójában virtuálisak – olyannyira, hogy a Microsoft Storage szerverben az iSCSI Target ténylegesen egy VHD formátumú állományt ajánl ki. VHD? Akkor az később növelhető is. És ha már megnöveltük a VHD-t, akkor egy diskparttal a partíció is kihúzható. Ehhez nem kell dinamikus diszk.

Jó, maradt a basic lemez. Ez azt jelenti, hogy maradt a diszkek szignatúra alapú azonosítása? És a diszkek cseréje továbbra is rémálom? Egyáltalán nem. A lemezeket a fürt – mint korábban – továbbra is a partíciós táblába írt szignatúrák alapján azonosítja – elsősorban. Emellett – és ez az újdonság – az SCSI szabvány Inquiry parancsát is használja a fürt. A parancsra a választ a storage kontroller adja meg, és egy adott LUN-t lehet azonosítani vele. A LUN a kiszolgálóból nézve egy diszk. Mivel ez két egymástól független módszer, a Windows 2008 szempontjából ugyanaz a „fizikai lemez" azonosítása, a metódusok egymás tartalékai lehetnek. Ha egy lemez nem található a szignatúra alapján, de az SCSI Inquiry működik, a fürt automati-



6. kép. Hibás lemez javítása

kusan javítja a szignatúrát, és fordítva. Persze nem zárható ki az sem, hogy teljes katasztrófa történt, és a teljes lemezalrendszer megsemmisült szignatúrástul, Inquiry-adatostul. A fürt erőforrásai leállnak ugyan, de megfelelő konfiguráció esetén (Node and disk majority) a fürtszolgáltatás még ezt is túlélheti. Ha azután újraépítjük a rendszerünket, a fizikai lemez erőforrásra kattintva, majd a „Repair disk...” parancsot választva már rá is mutathatunk, hogy a fürt lelke, vagyis a definiált erőforrás milyen testbe (értsd: tényleges LUN-be) költözzön. Szép, ugye?



7. kép. Parancssorból is gyönyörűen látszik minden

Három további, lemezekkel kapcsolatos fejlesztést kell megemlítenünk, ebből kettőnek előzménye is van. A GPT támogatást már 2002. végén is ismertük, az akkor még .Net Server leánykori néven futó, később Windows Server 2003 x64-es fürtjeinél citáltuk mint újonnan támogatott partíciós formátum. Jelentem a GPT nagykorú lett, a fürt minden platformja ismeri! Mi a GPT? GUID Partition Table – a Master Boot Record leváltását szolgáló módszertan. Mindenki, aki 2 terabájtnál nagyobb partíciókat szeretne kezelni, GPT-formázás után kiált majd. És hol lenne a legnagyobb jelentősége e szabvány támogatásának, ha nem éppen a legfontosabb, legnagyobb rendszerek esetén?

Talán nüansznyi újítás, de jegyezzük meg: a tanúlemez nem igényel betűjelet. Mivel a nagyméretű Exchange- és SQL-fürtök meg olyan lemezkiosztást szeretnek, ahol a címkeként használt betűk pillanatok alatt elfogynak, adott esetben ez az egyetlen betűjel jól jöhet.

Most pedig szeretném bevezetni az olvasót a lemezekre vonatkozó karbantartási üzemmód (maintenance mode) rejtelmeibe. Bár elsőre azt hittem, hogy ez a Windows Server 2008 újdonsága, rá kellett jönnöm, nem így van.

A Windows Server 2003 SP1 verziójában implementálták. (Részletekkel a 903650-es cikk szolgál.) Mi a karbantartási üzemmód? Azt jelenti, hogy a fürtszolgáltatás mind a négyféle (LooksAlive, IsAlive, SCSI Reserve, Private Sector) lemezellenőrzési funkcióját felfüggeszti, a fizikai lemez erőforrást „online” állapotban tartja, továbbá lehetővé teszi, hogy más processzek kizárólagosan lefoglalhassák a lemezt. Nem kell itt bonyolult dologra gondolni: chkdsk. Ha nincs maintenance mód, akkor csak a fürtszolgáltatás teljes leállításával lehetne hibajavítást végezni. Különben már az első ellenőrzés elhasalna, mire a fürt ijedten átküldené a teljes erőforráscsoportot a másik node-ra – lekaszabolva ezzel a chkdsk-et.

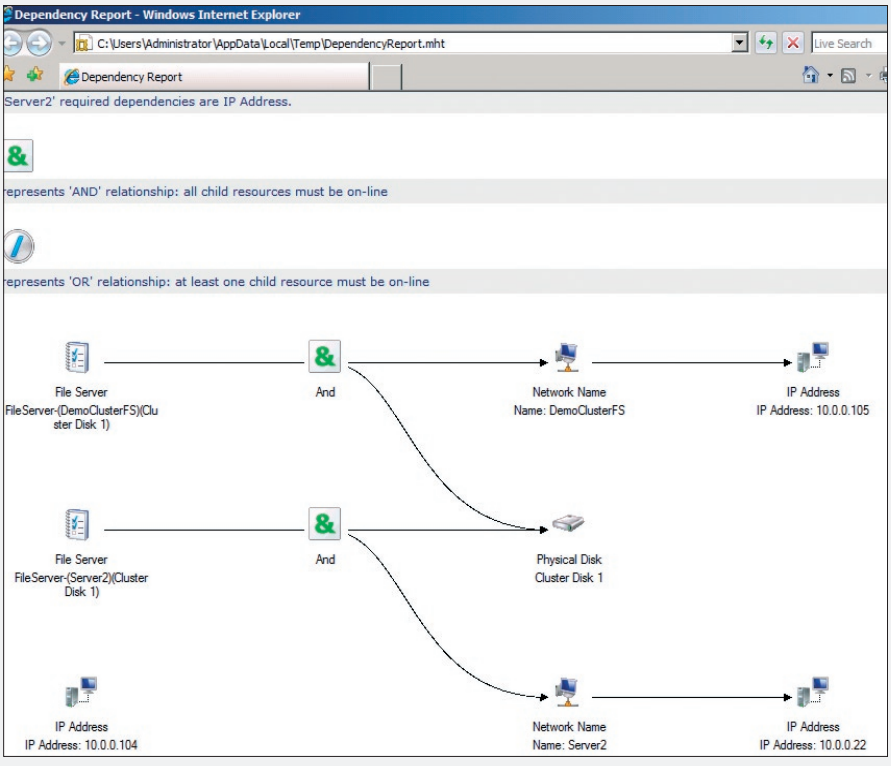
A karbantartási üzemmódnak van még egy járulékos haszna: ez az összekötő kapocs a hardver alapú lemezpillanatkép (snapshot) visszaállításához. A folyamat egyszerű:

- A függő erőforrásokat egy ügynök leállítja.
- Karbantartási üzemmódba teszi a lemezt.
- Exclusive lockot alkalmaz.
- Kicseréli a fizikai lemezt egy korábbi pillanatfelvétellel.
- Feloldja a kizárólagos hozzáférést.
- Befejezi a karbantartási üzemmódot.
- Elindítja a függő erőforrásokat.

Ez több, mint amire számítani lehetett. A Windows Server 2008-nak csak grafikus felületet kellett biztosítania – megőrizve természetesen a szkriptelési lehetőséget.

Erőforrások és erőforráscsoportok

Évekkel ezelőtt tapasztaltuk már: erőforrások születnek és elhalnak. Kikerült az IIS, jött helyette a Generic Script. Eldőlt – hiába hiányoltuk –, a WDS magas rendelkezésre



8. kép. Pontos függőségek beállításának lehetősége

állását az NLBS, nem pedig a failover cluster biztosítja. Van ugyanakkor húsz alapértelmezett erőforrás, ezek közül a Distributed File System, a File Server, a File Share Witness, az IPv6 Address, az IPv6 Tunnel Address, a Microsoft iSNS és az NFS Share részben vagy egészben új erőforrástípusok.

Sem a súgó, sem az MMC-felület explicit módon nem használja azt a kifejezést, hogy erőforráscsoport-sablon, de tulajdonképpen mégiscsak létezik ez a fogalom. Ha létre szeretnénk hozni egy új „services and application" objektumot – ez a hajdani erőforráscsoport –, akkor a varázsló első lépésénél 13-féle „út" közül választhatunk, s ezek nem mások, mint sablonok. Van köztük DHCP, DTC, Other Server (!) és Virtual Server is – ez utóbbi a Hyper-V-integrációt mutatja.

Az erőforrások közötti viszony legjelentősebb változása a függőségeknél tapasztalható. Korábban a többszörös függőségek kizárólag ÉS kapcsolaton alapultak – vagyis elég volt megállnia egyetlen erőforrásnak a sok közül, hogy a függőségi láncban tőle függők mind megálljanak. A Windows Server 2008-ban viszont az erőforrás-függőség definiálásakor VAGY kapcsolatot is létrehozhatunk. Egy hálózatinév-erőforrás függhet két IP-címtől is. Az egyik leállása VAGY kapcsolatnál nem okozza a hálózatinév-erőforrás leállását. Alhálózat cseréje során ez kifejezetten jól jöhet. Apropó: függőséget – szemben a korábbi verziókkal – működő erőforrásoknál is megadhatunk. Elvégre legalább a fürtszolgáltatás maga ne okozzon leállást...

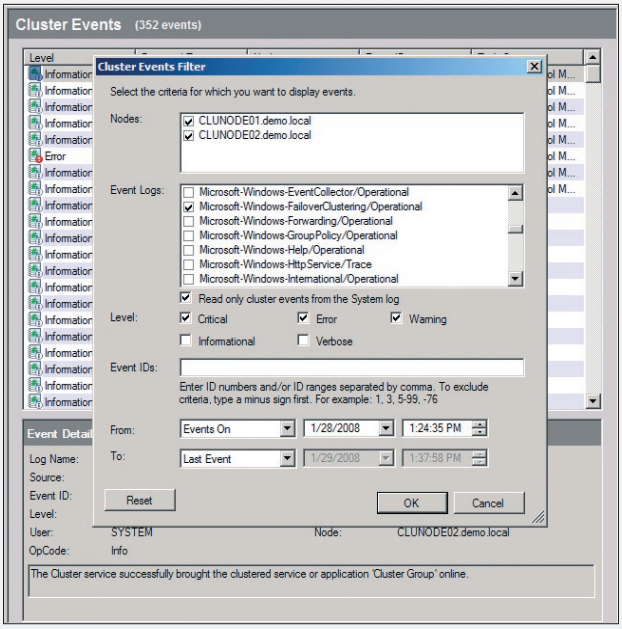
Végezetül egy különös erőforráscsoportra is felhívom az Olvasó figyelmét. A korábbi fürtökön az egyetlen azonnal létrejövő erőforráscsoport a Cluster Group volt a Quorummal. A Failover Cluster ezt kiegészíti még eggyel, amelyet „Available Storage Group"-nak hívnak, és ahogy a neve mutatja, azokat a lemezerőforrásokat tartalmazza, amelyeket még egyetlen „valódi" csoporthoz sem rendeltünk hozzá. Miért fontos ez? Azért, mert így a fürt létrehozásának pillanatától minden lemezerőforrásra egyértelműen foglalt. Az új, rejtett csoport létrehozása a lehetséges rejtett hibák elkerülését jelenti.

Eseménynapló-kezelés

Őszinte leszek: az eseménynapló-kezelés változása okozta a legtöbb frusztrációt a számomra. Nem azért, mintha a fejlesztők nem találták volna el a helyes irányt, hanem... de lássuk előbb, mit hiányoltunk a korábbi verziókból.

„Végezetül feltehetjük a kérdést, hogy vajon elégséges információval és eszközökkel rendelkezünk-e ahhoz, hogy hatékonyan hárítsuk el a fürt hibáit. Úgy gondolom, hogy a Microsoftnak még sok tennivalója van ezen a téren. Két lehetséges úton haladhat a cég a jobb hibafelderítés elősegítésére. Az egyik egy referenciakönyv elkészítése a lehetséges naplóbejegyzésekhez [...] A másik út az, ha szorosabb integrációt valósít meg a fürt és a Windows 2000 eseménynaplózó alrendszere között [...] A naplózási szinteket komponensenként lehetne meghatározni, és ha szükség van rá, akkor bekapcsolva egyre részletesebb eseménysort láthatnánk." (2002. november – Farkasokkal táncoló XII. rész)

A próféta szólt az írásból: a három fenti elképzelésből kettőt viszontláthatunk a Failover Clusternél. Az MMC fastruktúra öt főágából az utolsó az eseménykezelés. Módunk van a konzolból való kilépés nélkül megtekinteni a fürttel kapcsolatos összes eseményt. Melyik eseménynaplóból? „Melyikből szeretnéd?" – jöhetne a válasz helyett a visszakérdezés. Itt is a Windows Server 2008 alapjai köszönnek vissza. Eseménynapló már nemcsak háromnégy-öt van, hanem sokkal több és sokkal részletesebb. A fejlesztők tehát ránk bízzák, hogy milyen eseményeket szeretnénk összeválogatni a mi ablakunkba. Az sem baj, ha kezdetben nincs ötletünk – fogadjuk el az ő eseményszűrő alapbeállításaikat, nem fogjuk megbánni.



9. kép. A bőbeszédű, de szűrhető eseménynapló

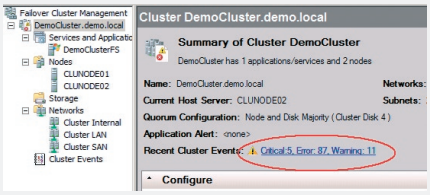
És az integráció itt még korántsem ért véget. Minden csoporthoz, erőforráshoz a lehetséges tevékenységek között kiválaszthatjuk a hozzá tartozó kritikus és figyelmeztető események lekérdezését. Ez egy nem módosítható lekérdezés, de nem is baj: szerepe, hogy az adott objektummal kapcsolatos hibaelhárítást a leghatékonyabban lehessen elkezdeni.

Ha van fontos dolog egy magas rendelkezésre állású szolgáltatás esetén, akkor az az auditálás: ki, mikor és mit végezett el azon a gépen vagy fürtön. Persze ehhez vannak üzemeltető szoftverek, mint például a System Center Operations Manager, de azok is leginkább az operációs rendszer beépített auditálási képességeire hagyatkoznak. Nos, az első lépéseket megtették a fejlesztők, a fürtre vonatkozó események (csoportmozgatás, erőforrás-létrehozás stb.) auditálhatóvá válnak. Ezenfelül minden fontosabb tevékenység, amelyeket varázslók is segítenek, a windows\cluster\reports mappában jelentéseket hagy – vagyis nemcsak az ellenőrizhető, mi történt, hanem az is, hogyan.

És mi lett a cluster.log-gal? Nyugdíjba vonult és átadta helyét a Windows Server 2008 biztosította „Event tracing" szolgáltatásnak. Mindeddig ez a képesség az egyetlen kivétel, amely nem érhető el a fürtszolgáltatás konzoljából. A „Reliability and Performance" konzolban láthatjuk a Data Collection Sets → Event Trace Sessions ágon belül. Láthatjuk, pontosabban megnézhetjük, hogy az élő események kezelése vajon fut-e. Az eseményeket magukat nem – ahhoz egy tracerpt nevű parancssori eszköz áll a rendelkezésünkre. Ha ez nem tetszik, akkor még fordulhatunk a cluster.exe megfelelő kapcsolóihoz, amely az általunk paraméterezett módon és helyre egy olyan logot generál, amilyen korábban a cluster.log volt. Hogy megnézhessük végre.

A rövid próbálgatás némi hiányérzetet hagyott bennem. A hétköznapi események „kéz alatt” vannak, ez jó. Az adott objektumhoz tartozó gyors eseménymegtekintés briliáns ötlet. Az események leírását is megfelelőnek éreztem. A diagnosztikai elemzés azonban nehézkesen indul, és éppúgy nincs tudásbázis cikkekkel, referencialeírásokkal megtámogatva, mint a korábbi verziókban.

Ezenfelül még egy dolog frusztrált. Az MMC-konzol közepén elhelyezkedő belső fejléc automatikusan jelzi a kritikus és figyelmeztető üzenetek számát. Ez még rendben is lenne – de az üzenetet nyugtázni és eltüntetni már nem tudtam, márpedig az nagyon zavaró, hogy



10. kép. A korábbi hibák sokáig láthatóak maradnak

egy problémát megoldottunk, de az eseménynaplóban fellelhető hibát x ideig még a fejlécre is kivezetik, függetlenül az aktuális helyzettől.

Egyéb változások

Sok-sok lelkesítő újdonságról, fejlesztésről esett már szó, de biztos vagyok benne, hogy az üzemeltetők majdani első számú kedvence nincs közöttük. A valószínű győztes egy aprócska dolog: nincs többé szükség cluster service-fiókra! Vagyis, nincs szükség

- ennek a fióknak a létrehozására;
- jogosultságainak kezelésére (annak idején egy fél cikket rászántunk, hogy megmutassuk, a service account tud nem Domain Admin is lenni);
- a jelszóházirend meghágására – ha nem lejáróvá tesszük a fiók jelszavát;
- jelszavának cserélgetésére;
- hibaelhárításra, ha véletlenül töröltük a fiókot, vagy elfelejtettünk időben új jelszót adni neki, vagy csak a jogosultságait vontuk meg stb. stb.
- oh – mennyország!

Amikor a Windows 2000 Server fürtjeit használatba vettük, még a holdban sem volt a SUS/WSUS vagy más automatikus frissítési rendszer. Egyáltalán, a frissítés mint olyan, elég alacsony prioritású feladat volt. Nem úgy ma. A fürtök azonban speciális bánásmódot igényelnek. Mert teszem azt, milyen állapotok keletkeznek, ha egy gépre éppen akkor költöznek át erőforrások, miközben hotfixet rak fel. Sokféle, de csak nem determinált. Épp ezért kellett bevezetni az állomások megállítását (Node Pause) és visszaállítását (Node Resume). Amíg egy állomás „Pause” állapotban van, addig a meglévő erőforrásokat futtatja, de új csoportokat nem fogad be – egy stabil állapot keletkezik: indulhat a frissítés. A „Node Resume” ezt a helyzetet szünteti meg.

Valljuk be őszintén: a fürtök mentése és visszaállítása többnyire az ezoterikus témák közé tartozott a rendszergazdák számára. A fürtön lévő adatokat mentettük persze, de a fürtkonfigurációval nemigen lehetett mit kezdeni. A system state része, és az bizony sokszor nagy gombóc a torokban. No de ne bolygassuk a múltat...

A Windows Server 2008 Failover Clusterének mentése egy kicsit már egyértelműbb, köszönhetően a Quorum letisztultságának. Mivel a Quorum mostantól kezdve egy elosztott valami, a konfiguráció helyreállítása – legalábbis a szóhasználatban – nagyon hasonlít az AD helyreállításhoz. Éppúgy, mint ott „Authorative” és „Non-Authorative” helyreállítást hajthatunk végre. Az elsőnél becsatlakoztatunk egy node-ot a meglévők közé, az utóbbi esetben visszaállítunk egy fürtöt egy korábbi konfigurációs állapot szerint. Részletek az RTM megjelenésével.

Feketeleves

Minden nagyon jó, minden nagyon szép. Tényleg? Ennyire? Bölcs ember tudja: szépség és szörnyeteg együtt járnak. A Windows Server 2008-ban implementált Failover Cluster akkorát ugrott elődeihez képest, hogy a gyökereit is elszakította: történetében először nincs lehetőség a rolling upgrade frissítésére. Mi a rolling upgrade? Elvileg lehetséges volt, hogy egy Windows NT 4.0-val beüzemelt fürtöt átállítsunk Windows 2000-re úgy, hogy előbb az első node-ot frissítettük, majd az erőforrások átmozgatása után a másikat. Azután pedig ezt tovább folytathattuk a Windows Server 2003-mal. Egyszerre csak egy verziókülönbség volt megengedett, a frissítésnek szigorú szabályai voltak, de mégiscsak működött. Eddig.

A Windows Server 2008-cal új korszak kezdődik. Az eltérő storage-kezelési mechanizmus és a hálózat változása bezárta a kapukat. Mit lehet tenni? Azért van egérút, a fürtök migrációját varázslók segíthetik. Egy darabig. Azután kellünk mi, mérnökök.

Összefoglalás

Mielőtt pár szép szóval elbúcsúznánk, még egyszer szeretnék idecitálni egy régi-régi cikkből. Tanulságos.

„Kényelem kontra biztonság kontra kompatibilitás: A biztonsági tényezők alkalmazásakor sokszor felhívják a szakemberek a figyelmet, hogy a biztonság növelése gyakran a kényelem és a használhatóság rovására történhet. Biztonságosabb a jelszóval történő azonosítás, mintha ilyen nem történik, de meg kell jegyezni a titkos jelsort (kényelem csökkenése), és ha tévesen adjuk meg a minket azonosító adatokat, a rendszer kizárhat minket (a használhatóság korlátozódik).

Az üzemeltetési tapasztalatok azonban azt mutatják, hogy egy harmadik dimenzió is befolyásolja a biztonsági funkciók bevezetését, ez pedig a kompatibilitás. A rendszer egyes elemeit más-más csoportok fejlesztik, akik eltérő sebességgel képesek a központi biztonsági igényekhez alkalmazkodni. A fürtszolgáltatás például nem képes a Kerberos hitelesítésre, így akik ezt a szolgáltatást igénybe veszik, nem tudnak tisztán Kerberos rendszert bevezetni.”

Úgy érzem, hosszú oldalakon keresztül soroltuk azokat a példákat, amelyek alapján világossá vált: a Failover Cluster – legalábbis a 2008-as verzió nem tartozik a fenti kompromisszumok közé. A fürt és az azon futó alkalmazások mindazt tudják, ami az operációs rendszer része – kompromisszumok nélkül.

A virtualizáció megjelenésével a fürt – amely maga is egyfajta virtualizációs technológia – oda került, ahová való: nem alkalmazásokat biztosít (értsd: nem izolál), hanem azok magas rendelkezésre állását teszi lehetővé.

És a jövő? Szemetek a virtualizációra vessétek! A Failover Cluster már most is integrált a Hyper-V-vel, scriptek helyett csupán erőforrásokat kell felvennünk. A jövőben azonban ennél többre lesz szükség: éles migráció, erőforrás-kihasználtság alapú csoport (értsd: virtuális gép) mozgatása és vagy még egy tucatnyi egyéb ötletem van, mire lenne szükség a jövőben. Úgy érzem, a Failover Cluster csapata felpörgött a jövendőbeli kihívásokra.

Lepenye Tamás
(tamasl@microsoft.com)
MCSE, Microsoft Magyarország

Windows Server 2008 – Az előkészületek

Az operációs rendszer frissítése, sémafrissítés és a működési szintek.

A címben említett három téma tekinthető akár egy egységnek is, mivel elvégezve ezeket, a Windows Server 2008 bevezetésének szoftveres előkészületeit nagyjából meg is tettük. Persze pontról pontra követni, kész receptnek venni az alábbiakat nem okos dolog. Szinte 100 százalék, hogy a legtöbb esetben, a való világban sokkal összetettebb, bonyolultabb feladat lesz az áttérés, és természetesen nagyobb mértékben testre szabott is egyben. Sok-sok éve gyakorló rendszergazdaként tudom, hogy minden információ, ami a támogató dokumentumokban elolvasható, és így minden, ami ebben a cikkben is szerepel, az maximum elméleti alap lehet a sok-sok egyedi rendszer üzemeltetője számára.

Az operációs rendszer frissítése

A Windows Server 2008 nyolc változatát az alábbi táblázatban foglaltuk össze.

SKU	Hyper-V-t tartalmaz?
WS08 Standard (x86/x64)	–
WS08 Enterprise (x86/x64)	–
WS08 Datacenter (csak x64)	–
WS08 Standard (csak x64)	+
WS08 Enterprise (csak x64)	+
WS08 Datacenter (csak x64)	+
WS08 Web Server (x86/x64)	–
WS08 Itanium Edition (csak 64)	–

Kiegészítések:

1. A WS08 egyik remek újdonsága a Server Core, de ez nem egy különálló termék vagy változat, hanem egy speciális telepítési mód, amely a Standard, az Enterprise vagy a Datacenter változat 32 és 64 bites környezetében egyaránt használható.

2. A Hyper-V komponens csak x64-es operációs rendszerre kerülhet fel.

3. A WS08 Web Edition csak helyi SQL-támogatással működhet.

A támogatott frissítési útvonalak szintén egy táblázatban láthatók.

Amit futtatunk	Amire áttérhetünk
WS03 R2 Standard Edition WS03 Standard Edition SP1 WS03 Standard Edition SP2 WS08 Standard RC0	WS08 Standard WS08 Enterprise
WS03 R2 Enterprise Edition WS03 Enterprise Edition SP1 WS03 Enterprise Edition SP2 WS08 Enterprise RC0	WS08 Enterprise
WS03 R2 Datacenter Edition WS03 Datacenter Edition SP1 WS03 Datacenter Edition SP2 WS08 Datacenter RC0	WS08 Datacenter

1. Ami rögtön látszik, pontosabban nem látszik a táblázatban, az a WS03 Web Server változat hiánya, de ez nem véletlen, hiszen erről nincs frissítési útvonal, annak ellenére sem, hogy WS08-as változat is van belőle.

2. Minden felsorolt útvonal feltételezi azt, hogy nem x86-ról x64-re történik az áttérés, mivel az ilyen frissítés továbbra sem támogatott.

3. A Server Core változatra semmilyen operációs rendszerről sem lehet áttérni, még egy WS08-változatról sem. Sőt, egy működő Server Core-t sem lehet frissíteni egyik hagyományos változattal sem.

4. Általánosan a Microsoft nem blokkolja a frissítést a bétaváltozatokról (azaz, akár a Beta3-tól végigmehetünk az RTM-ig), de ezek a frissítések nem támogatottak, kivéve a belső és a TAP-ügyfeleket.

Változások a Windows Server 2008 telepítésében

A Vistához hasonlóan a WS08 telepítése is egyszerűbbé vált, persze ez úgy értendő, hogy ha nincs szükség rá, akkor alig kell beavatkoznunk.

Valamennyire azért muszáj, mert például a háttértárakkal variálnunk kell, és ezzel kapcsolatban akadnak extra lehetőségeink.

A telepítés gyakorlatilag három fő részre osztható:

1. A szintiszta operációsrendszer-telepítés,

a DVD-s rendszerindítástól a termékkulcs, a nyelvi és a billentyűzetkiosztás-beállításig.

2. Initial Configuration Tasks, a valóban alapbeállítások, amelyeket tipikusan egyszer használunk (időzóna, AU-kliens, gépnév, hálózat, TCP/IP, RDP, tűzfal stb.)

3. Server Manager, amely egy rendkívül széleskörűen használható eszköz, és amely a következő, korábban használatos varázslók és MMC-konzolok kombinációja egyben:

- Manage Your Server Wizard;
- Configure Your Server Wizard;
- Add/Remove Windows Components;
- Computer Management.

A Windows Server 2003 SP1-ben megjelent SCW-t (Security Configuration Wizard) nem említettem, mivel ennek futtatására már nincs szükség – a WS08 szerepkörei és szolgáltatásai ugyanis alapállapotban is megfelelő biztonságossággal konfigurált állapotban dolgoznak.

A sémafrissítés

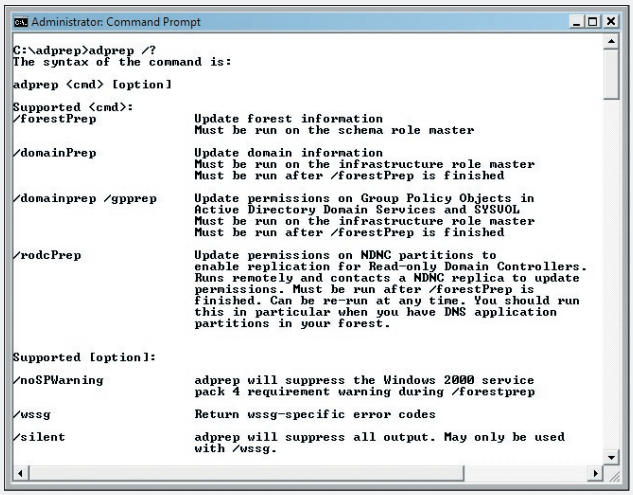
Egy új Windows-szerverváltozattal tipikusan együtt jár a címtárszolgáltatás változása, a különböző kisebb-nagyobb újdonságok megjelenése is. Ezek általában kényelmes és kellemes változások, de ez előkészítés, a tartomány és/vagy az erdő felkészítése a legtöbb esetben azért némi terhet is jelenthet (még ha általában édeset is). Ha másért nem, akkor azért, mert alapos áttekintést és mérlegelést követel meg az üzemeltetőktől, mivel a sémafrissítés egyik különlegessége abban rejlik, hogy visszafordíthatatlan, visszavonhatatlan folyamat, azaz végtelenül körültekintően kell eljárnunk a változtatásokkal, főképp nagyobb és/vagy bonyolultabb környezetben. A Windows Server 2008 apropóján tehát az operációsrendszer-frissítési tudnivalók után a sémafrissítésről is feltétlenül meg kell emlékeznünk.

Köztudomású, hogy mielőtt egy új 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 WS08- 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). 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, Windows 2000-es natív működési szinten kell lennie a Windows 2000-tartományunknak, vagy Windows 2003-as natív szinten a Windows 2003-tartományunknak (a működési szintekről később még bőven lesz szó).

2. Ha az adott gép lesz az első WS08 DC az erdőben, akkor előzetesen az erdőt is preparálni kell az Adprep/forestprep paranccsal.



Az új Adprep paraméterei és opciói

Ekkor a séma frissítését a Schema Master egyedi szerepkörrel ellátott DC-n kell elvégeznünk, ami annyira egyedi, hogy összesen egyetlenegy ilyen gépünk lehet csak az egész erdőben – ez az úgynevezett forest root DC.

3. Ha ez a gép lesz az első WS08 DC a tartományban (de az erdő már elő van készítve), és a tartomány Windows 2003-as működési szinten van, akkor az Adprep /domainprep parancsot kell használnunk az Infrastructure Master FSMO szerepkört birtokló DC-n a tartomány előkészítéséhez. Ha a tartomány esetleg még Windows 2000-es működési szinten van, akkor viszont az Adprep /domainprep /gpprep parancs lesz a nyerő, mivel ekkor a Group Policy-objektumok és a SYSVOL-jogosultságok problémáját is rendeznünk kell.

4. Ha gond nélkül lemegy minden parancs, és így az erdő és a tartomány preparálása, akkor nem lesz rá szükségünk, de egyébként jó, ha tudjuk, hogy az Adprep debug naplófájlok helye megváltozott, immár a következő helyen találjuk őket: %systemroot%\debug\adprep.

E rész végére került extra információ is, amellyel még nem találkozhattunk, akárhány éve ütjük-verjük a sémát.

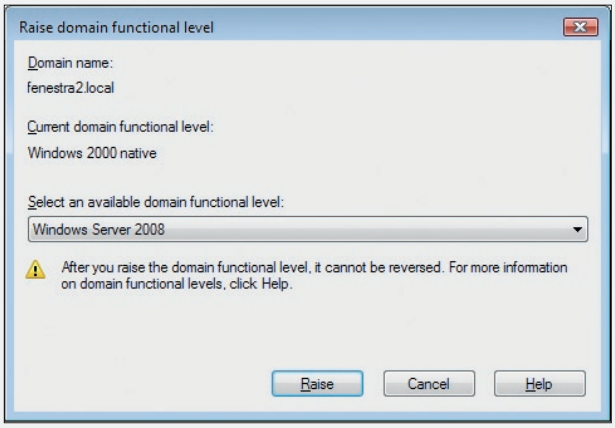
Az a speciális helyzet állt elő ugyanis, hogy a WS08 egyik nagy dobásaként számon tartott teljesen új típusú tartományvezérlő, a RODC (Read-Only DC) működik az erdő Windows Server 2003-es szintjén is (igaz, egy kisebb szépséghibával, lásd e cikk legvégén). Ha tehát a Windows 2003-as tartományunkban szeretnénk 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.

Ha úgy tervezzük, hogy a RODC-nk egyben GC (globáliskatalógus-kiszolgáló) is lesz, akkor az erdő minden egyes tartományában kivétel nélkül futtatnunk kell az Adprep/domainprep parancsot, akár van ezekben WS08 DC, akár nincs. Ennek a kritériumnak az oka az, hogy így a RODC képes lesz replikálni a globális katalógus adatait minden tartományból, és így – és csak így – teljes értékű GC-nek számít majd.

Az első WS08 DC egy meglévő Windows 2000/2003/2008-as tartományban semmiképpen nem lehet RODC, ezt a szerepet csak egy második WS08 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.

A működési szintek

Harmadik lépésben a szintén speciális működési szintekről lesz szó, mégpedig azért, mert az ezzel kapcsolatos teendők is minimum lehetséges, de sok esetben kötelező elemei lesznek a WS08 bevezetésének. A most következő áttekintéssel tehát ezen a terhen szeretnénk kicsit könnyíteni, sorba állítva a lehetséges forgatókönyveket. Persze, azt is szeretném rögvest megjegyezni, hogy ugyan a WS08 RTM bejelentésének már stabil, kitűzött dátuma van (2008. február 27.), jelen pillanatban még nem 100 százalékosan tiszta minden körülmény, egy-két apróbb dologról esetleg még kiderülhet, hogy időközben megváltozott. Kötelességem szólni arról is, hogy a sémafrissítéshez hasonlóan a működési szintek változtatása is visszavonhatatlan folyamat, tehát csak óvatosan!



A WS08 alapértelmezett tartományi működési szintje a Windows 2000 natív

Az alapfogalmak

Csak tömören és a Windows Server 2003-ra kihegyezve jöjjön egy kis összefoglaló, egy még erőteljesen nyomdaillatú, de remélhetőleg a jövőben sokak által alaposan megforgatott könyvből, amelynek címe: Rendszerfelügyelet rendszergazdáknak: http://tinyurl.com/2jgwdp.

„A tartományok és erdők Windows Server 2003 Active Directoryban bevezetett működési szintjeinek segítségével engedélyezhetők bizonyos tartományi és erdőszintű Active Directory szolgáltatások. A hálózati környezettől függően másféle beállítások állnak rendelkezésre a tartományok és az erdők különböző működési szintjein. A működési szint egyrészt meghatározza a tartományban, illetve erdőben elérhető szolgáltatások körét, másrészt a működési szint emelésével régebbi tartományvezérlők már nem adhatók a tartományhoz. A tartományok működési szintjei a teljes tartományban, és csakis az adott tartományban elérhető szolgáltatásokat befolyásolják. A tartományokhoz négy működési szint áll rendelkezésre: Windows 2000 – vegyes (mixed), Windows 2000 – natív, Windows Server 2003 – átmeneti (interim) és Windows Server 2003.

A működési szint előléptetését követően a korábbi operációs rendszereket futtató tartományvezérlőket nem lehet a tartományba beléptetni. Ha például a tartomány működési szintjét előléptetjük a Windows Server 2003 szintre, Windows 2000 Servert futtató kiszolgálókat tartományvezérlőként már nem lehet hozzáadni a tartományhoz. Természetesen továbbra is beléptethető a tartományba egy Windows 2000 Server, bármiféle feladatot is elláthat, csak tartományvezérlő nem lehet többé.

Az erdők működési szintjének beállításával az erdő összes tartományán engedélyezhetők szolgáltatások. Az erdőkhöz három működési szint áll rendelkezésre: Windows 2000, Windows Server 2003 – átmeneti (interim) és Windows Server 2003. Az erdő működési szintjének előléptetését követően, a korábbi operációs rendszereket futtató számítógépeket tartományvezérlőként nem lehet az erdőbe beléptetni. Ha például az erdő működési szintjét előléptetjük a Windows Server 2003 szintre, Windows 2000 Server rendszert futtató tartományvezérlőket már nem lehet hozzáadni az erdőhöz.

A működési szint emelése több előnnyel is jár, például így tehetjük lehetővé bizonyos erdő- vagy tartományszintű új szolgáltatások, megoldások használatát (univerzális csoportok stb.), és az Windows Server 2003 R2 változat bizonyos szolgáltatásai is csak magasabb működési szinteken használhatók."

Nos, annyi biztosan kiderülhet bárki számára ebből az idézetből, hogy a WS08 kapcsán is szét kell választanunk a témát két részre, a tartományok és az erdő szintjére. Először koncentráljunk a tartományok működési szintjével kapcsolatos okosságokra!

WS08: tartományműködési szintek

A legfontosabb: a WS08 a mixed üzemmód kivételével a többi felállásban képes lesz tartományvezérlőként dolgozni. Tehát a WS08 DC egy NT4 PDC-vel már semmiképp nem, viszont a Windows 2000/2003-as tartományvezérlőkkel biztosan egyet fog érteni.

Windows 2000-es natív módú tartományok

Tartományvezérlő lehet: W2K, W2K3, WS08.

Berakhatunk tehát egy ilyen tartományba is WS08 DC-ket, de a tökéletes együttműködéshez szükség lesz még némi plusz technikai információra, amely azonban még nem közkincs, de nyilván hamarosan az lesz. A tisztán WS08-újdonságok (lásd a végén) viszont a tartománynak ebben az állapotában nem használhatók, hiszen az új technológiák alapfeltétele a natív WS08-as tartományi üzemmód. A W2K-s natív módú tartományok viszont a következő pluszokat adhatják az előző (a mixed) módhoz képest:

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

Windows Server 2003-as módú tartományok

Tartományvezérlő lehet: W2K3, WS08.

Ebben az üzemmódban a Windows 2000 DC-k már nem, a Windows Server 2003-ak viszont csont nélkül használhatók együtt a WS08-as tartományvezérlőkkel. A jó pár WS08-újdonság viszont szintén nem működik majd ilyen körülmények között. A W2K3 natív módú tartományok például a következő pluszlehetőségeket biztosítják az előző (a W2K-s natív) módhoz képest:

- A Netdom.exe-vel átnevezhetjük a tartományvezérlőt.
- A „Users" és a „Computers" tárolók (azaz nem OU-k) átirányítása.
- Képes frissíteni a gépek, illetve a felhasználók viszonylatában a LastLogonTime attribútumot és replikálni a LastLogon-

TimeStamp-et a tartományon belül (még ha kissé nehézkesen, azaz nem túlságosan nagy pontossággal is).
- 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-as módú tartományok

Tartományvezérlő lehet: WS08.

Ha már itt tartunk majd, akkor az azt fogja jelenteni, hogy csak WS08 DC-ink vannak (vagy elszúrtuk, de nagyon). Ez a szint azért fontos, mert gyakorlatilag az összes nagyobb és fontosabb címtárszolgáltatási újdonság ekkor érhető el csak teljes mellszélességgel. A WS08-as módú tartományok tehát például (a lista nem teljes!) a következő extrákat adják az előző (a W2K3-as) 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 (a hírek szerint elvileg az ismerős Acctinfo.dll integrálásáról van szó, bár nekem még eddig sehogy sem sikerült előcsalogatni ezeket az infókat az ADUC-ban).
- Fine-grained password policies, azaz alternatív jelszóházirend (eddig egy tartományban maximum egy jelszóházirend kialakítására volt lehetőségünk, de ez változott), akár OU-ként különböző jelszóházirend-opciókkal. További, részletes infót erről a *TechNet Magazin* korábbi számában találunk: http://tinyurl.com/2eo7sx.

A tartományok után az erdők működési szintjének WS08-as szintre emelésével folytatjuk. Mindenekelőtt visszanyúlunk az alapokhoz az előző alkalommal is emlegetett könyvből vett idézettel:

„Az erdők működési szintjének beállításával az erdő összes tartományán engedélyezhetők szolgáltatások. Az erdőkhöz három működési szint áll rendelkezésre: Windows 2000, Windows Server 2003 – átmeneti (interim) és Windows Server 2003. Az erdő működési szintjének előléptetését követően, a korábbi operációs rendszereket futtató számítógépeket tartományvezérlőként nem lehet az erdőbe beléptetni. Ha például az erdő működési szintjét előléptetjük a Windows Server 2003 szintre, Windows 2000 Server rendszert futtató tartományvezérlőket már nem lehet hozzáadni az erdőhöz.”

Összegzésként elmondható tehát, hogy sokkal óvatosabban kell bánnunk az erdő működési szintjének változtatásával.

A WS08-as erdő működési szintjei

A négyből (3 + a WS08) három erdő működési szintje mellett használhatunk WS08-as tartományvezérlő(ke)t. Nézzük át az idők kezdetétől, hogy mi minden pluszt lehetett korábban elérni egy-egy erdő működési szintjének emelésével.

Windows 2000-es natív módú erdő. Tartományvezérlő lehet: W2K, W2K3, WS08.

Az akkor még újnak számító és előd nélküli címtárszolgáltatás összes alapértelmezett tulajdonságát használhattuk.

Windows 2003-as natív módú erdő. Tartományvezérlő lehet: W2K3, WS08.

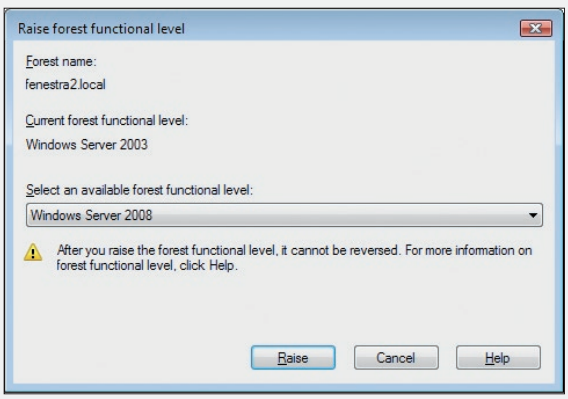
Néhány újdonság (természetesen nem az összes):
- Cross Forest Trust, azaz erdők közötti bizalmi kapcsolat kialakítása, magyarul két erdő összekötése, például két cég összeolvadásának apropóján. Kétirányú, tranzitív az erdők összes tartománya között, de nem az egyik erdőhöz ugyanígy kapcsolódó harmadik erdő felé.
- Tartományátnevezés.
- Link valued replication, azaz az „finomított” replikáció, amely sávszélesség-takarékos, és lehetővé teszi, hogy ne az adott elemet tartalmazó egész tömb replikálódjon, hanem csak az az elem, amely ténylegesen megváltozott.
- Sémaelemek inaktiválása, azaz olyan osztályok és attribútumok kivonása a forgalomból, 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 koszt is, tudniillik az inaktiválás visszavonása, a deaktiválás is működik.
- A RODC használata.

Windows Server 2008-as módú erdő. Tartományvezérlő lehet: WS08.

Kicsit megdöbbentő, de a tartományi szint számtalan újdonságával nagyjából el is lőttük a puskaport, azaz erdőszinten nincs semmilyen extra újdonság. Egyetlen dolgot azért meg kell említeni, ami miatt valószínűleg érdemes is lesz megemelni az erdő működési szintjét, ha lehetséges. A dolog a RODC-val kapcsolatos, de messziről futunk neki. Néhány alkalmazásnál megszokott dolognak számít, hogy a címtárban tárol szenzitív adatokat (jelszavakat, jogosultságokat, titkosított kulcsokat stb.).

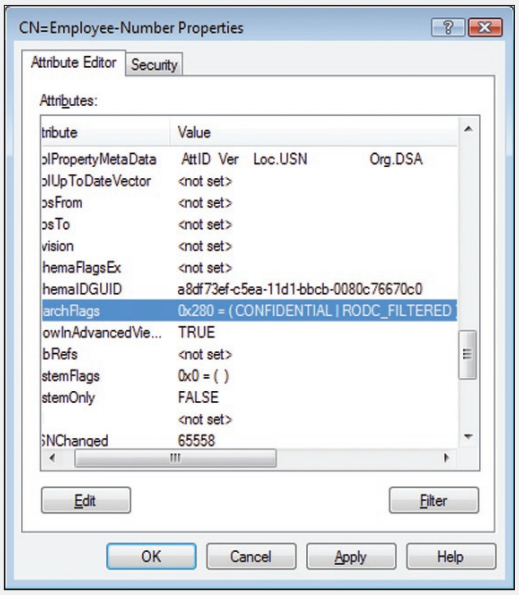
Ezzel nincs is gond, sőt praktikusnak is tekinthetjük a módszert, a tartományvezérlőkre amúgy is fokozottan oda kell figyelünk, és hát valóban ritkán tűnik el egy-egy DC a szerverszobából/-teremből. Viszont ha bekerül majd a képbe egy-egy RODC – ismerve a tulajdonságait: csak olvasható, jelszavakat nem tárol, Server Core-ra is felmegy stb. – a telephely egy sötét sarkába lerakva, akkor azért kicsit mégis aggódhatunk. Egy címtárpéldány ugyanis azért lesz azon a gépen is, szóval ha történetesen ellopják, azért kibányászható lesz belőle ez-az.

Nos, erre találta ki a Microsoft okosan az úgynevezett RODC Filtered Attribute Set (RODC FAS, korábban RO-PAS néven is futott) használatának lehetőségét, ami azt jelenti, hogy a WS08 Schema Master DC-n például az ldfide-vel vagy az ADSIEdit-tel megnövelhetjük az adott attribútum tulajdonságai között a searchFlags értéket (például



Megtörténik mindjárt…

0-ról 640-re = CONFIDENTIAL/RODC_FILTERED, lásd a képet, bár ott még hexában van). Így aztán ha a tartományvezérlő beleakad ebbe az értékbe, akkor ezt az attribútumot nem fogja replikálni az RODC kérésére. Mármint a WS08 GC DC-k, merthogy egy WS03 GC DC továbbra is megengedő lesz (kipróbáltam ezt is, hiába piszkáljuk meg az említett flaget a WS03 Schema Masteren, nem érti), 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.



Az általam variált Employee-Number attribútumon szépen látszik a változás

Sőt, a WS08-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;
- 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.

Ha már itt tartunk, azért említsük meg, hogy a FAS mellett/helyett van még egy lehetőségünk, ez pedig a védendő attribútum searchFlags értékének feljavítása a „CONFIDENTIAL" szintre (ennek 128 a decimális értéke, ami az előző esetben ugye automatikusan benne van a 640-ben, látszik is az előző képen). Ezt a WS03 SP1 óta lehetséges művelni, van is hozzá egy fárasztóan bonyolult KB cikk (Q922836). 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 jónéven.

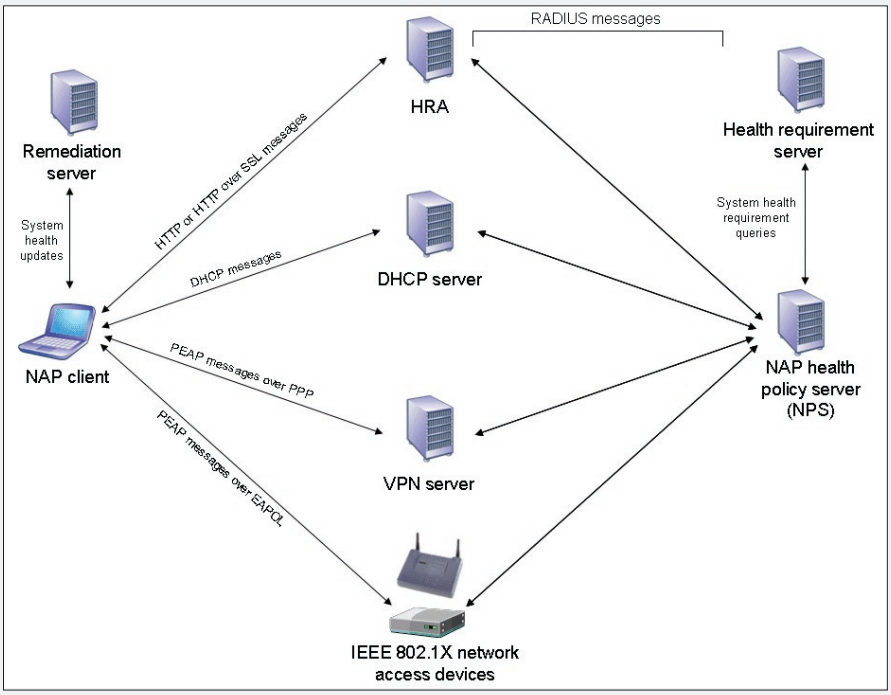
Gál Tamás
(v-tagal@microsoft.com)
Microsoft Magyarország

Süss fel, NAP!

A Microsoft kiváló biztonsági szakemberétől, Steve Riley-től származik az a hasonlat, hogy mostanáig a vállalati hálózatok egy lakóparkra hasonlítottak: kerítés, sorompó és biztonsági őr kívül, nyitott ablakok és ajtók belül, és grillparti a gyepen.

A boldog békeidők elmúltak: a napjainkban elérhető fenyegetések közvetlenül a házacskákra támadnak, nem elég többé a távoli kerítés: amíg a kerti grillt sütögetjük, valakik szétlopják a tulajdonunkat bent a házban. Vasrácsot kell szerelni minden ajtóra és ablakra. Erre a feladatra való a Network Access Protection.

A Vistában és a Windows Server 2008-ban megjelenő technológia nem előzmények nélküli. Már a Windows Server 2003/XP felállásban is használhattunk hasonló szolgáltatást a VPN-kapcsolódás ellenőrzésére. Úgy hívják: VPN-karantén. Igaz, kevesen használják, mert egyrészt



1. ábra. A NAP belül mindig RADIUS-t használ

bonyolult, másrészt a sok „HTTP over...” protokoll miatt a VPN-használat visszaszorulóban van, ennek ellenére érdemes áttekinteni a technológia elvi alapjait, mert a karantén és a NAP ugyanaz, csak picit más. (Persze valójában egyáltalán nem ugyanaz, a kettő vígan eléldegél egymás mellett, egymással párhuzamosan. Kiegészítik egymást. Viszont VPN-keretben jobban áttekinthető a történet. Ígérem, rövid leszek.)

Mi is a VPN? Egy meghosszabbított UTP-kábel, amely a céges hálózattól vezet az otthoni szutykos gépemig. Ne dugjuk homokba a fejünket: az otthoni pécék, amelyeken a gyerek játszik, és vírusokat tenyészt, a VPN-kapcsolat révén közvetlen TCP-kapcsolatba kerülnek a vállalati hálózattal, hogy ott sikeresen szétszéledhessenek a különböző gusztustalan férgek. Ez ellen természetesen van védekezés: mi lenne, ha minden otthoni számítógép fitt lenne a kibocsátott frissítések területén, esetleg lenne rajta egy naprakész víruskergető, bezárt tűzfal stb. Szép kis kívánságlista, de hogyan biztosítható, hogy ez a Józsi bácsiék pécéjén valóban így legyen? Sehogy. A megoldás kulcsa, hogy a határállomáson (a VPN-kiszolgálón) alapos ellenőrzést hajtunk végre, és ami nem felel meg nekünk, azt nem engedjük be.

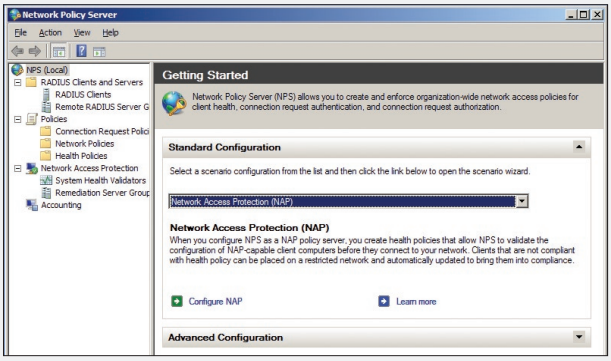
Nos, a NAP ugyanez, csak azzal a különbséggel, hogy a lakóparkon belüli személyeket vizsgáljuk: kijöhetnek-e a gyepre a közös grillpartira, vagy leteperte őket valami betegség, úgyhogy inkább maradjanak szobafogságban. Az érdekes az, és ennyiben minden életből vett hasonlat sántít, hogy mind a karantén, mind pedig a NAP esetében a vizsgálatot maga a célszemély hajtja végre önmagán, és dönt arról, hogy közösségbe mehet-e. A központi doktor bácsi csak a vizsgálat szabályaiért és azok betartásáért felelős, magáért a vizsgálatért nem.

Tehát ez egy kliens–szerver architektúrában működő szolgáltatás.

Kényszerek (enforcement)

A NAP számos trükköt tartalmaz az egészségtelen számítógépek távol tartására. Mindegyikben közös viszont a tyúk–tojás paradoxon, mert mindaddig nem tudjuk, hogy egy szá-

mítógéppel kommunikálhatunk-e, amíg meg nem beszéltük vele, hogy egészséges-e. Ehhez meg nyilván hálózati kapcsolat kell. A megoldás a szűkített hálózati szolgáltatásban rejlik. Attól függően, hogy pontosan melyik korlátozási módszert használjuk a betegek ellen, más és más módon adhatunk nekik a vizsgálat idejére valamilyen korlátozott kapcsolatot. A NAP külső gyártók által is bővíthető, jelenleg a következő megszorítási módszerek érhetők el: IPSec, 802.1x, VPN és DHCP.



2. ábra. Kezdjük el konfigurálni a NAP-ot!

IPSec Enforcement. Az IPSec-et már régen nemcsak titkosításra használjuk, hanem ez az eszköze a nagyképűen Domain Isolationnek nevezett eljárásnak, ami lehetővé teszi, hogy a hálózaton jelen lévő számítógépeknek csak egy bizonyos köre tudjon kommunikálni egymással. Ez a korlátozás tehát viszonylag egyszerű, mert más IPSec-szabályokat alkotunk az egészséges, és mást a beteg ügyfeleknek. Az egészségesek mindent vagy sokkal több szolgáltatást elérhetnek, mint a betegek.

802.1x Enforcement. A 802.1x szabvány mind vezetékes, mind vezetéknélküli hálózaton lehetővé teszi, hogy csak azonosított (újmagyarul: autentikált) eszközök léphessenek fel a hálózatra. Ez mind jelszóval, mind tanúsítvánnyal működik, az azonosítást pedig egy központi címtárra bízhatjuk. (Így lehet elérni, hogy például egy adott switchre csak olyan gép csatlakozhasson, amelyik tagja egy adott Active Directory-tartománynak.) Ez a megszorítás a NAP alatt a következőt tudja: a hálózati csatlakozási ponton valami minimális hozzáférést engedünk mindenkinek (a betegeknek is), hogy például legalább bejelentkezni tudjanak, a NAP viszont nem engedi bejelentkezni a betegeket. A végeredmény, hogy a betegek már a switch vagy a WiFi Access Point szintjén kiszűrődnek.

VPN Enforcement. Itt kellene megmagyaráznom a NAP és a VPN-karantén közti különbséget, mert úgy tűnik, mind a kettő ugyanazt csinálja. Igen, de másképp. A korábbi (ősi) módszer, a VPN-karantén alapvetően a rendszergazda kezébe adja, hogy mit akar ellenőrizni, és mit tart az egészség biztos jelének. Ehhez egy furfangos batch-fájlt kell készíteni, amihez nem minden földi halandónak van türelme – nekem sincs. A NAP-féle VPN-megszorítás viszont már az XP SP2-ben megjelent biztonsági központ állapotjelentésére épít, azaz az egészségügyi vizsgálat teljesen magától megtörténik, nem kell értékes órákat áldoznunk arra, hogy bugos batch-fájlokkal kísérletezzünk. Ha valakinek mégis szüksége van a teljes szabadságra, a NAP-pal párhuzamosan használhatja az ősi karantént is, és olyan scriptet rittyent, amilyet csak akar.

DHCP Enforcement. Itt már fogós kérdés a védelem, mert egy számítógépnek vagy adunk IP-címet, vagy nem. Mit lehet ezen korlátozni? Az opciókat! Például a betegek nem kapnak alapértelmezett átjárót. Emellett aki beteg, annak a Subnet Maskja 255.255.255.255, így csakis önmagával képes kommunikálni (egygépes subnet). Nem ártana azonban, hogy ha a hamarosan bővebben is kifejtett patikaszervereket el tudná érni, ezért kap egy marék DHCP 249-es (Classless Static Route) opciót, ezáltal az ő rút táblácskájába bekerül az a néhány bejegyzés, amelynek segítségével el tudja érni azokat az erőforrásokat, amelyek a gyógyulásához szükségesek (beutalókat kap). Hozzá kell tennünk, hogy a DHCP-kényszerzubbonyt egy Administrator bármikor leveti magáról. Hallottunk már statikus IP-címekről?

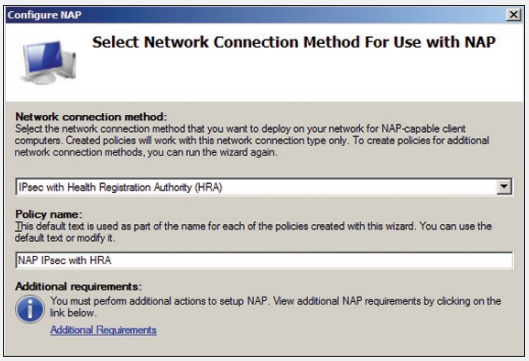
Szereplők

Elérkeztünk a stáblistához. Lássuk, kik vesznek részt ebben a játékban? Az operációs rendszerek oldaláról három szereplőnk van: kiszolgálóként a Windows Server 2008, amelyet márciusban jelent be a Microsoft, ügyfélként pedig a Vista, valamint a Windows XP SP3 áll rendelkezésre. Az összes többi operációs rendszer csak az árnyékban mozoghat, rájuk sohasem süt le a NAP, és ha csak valami kötelező érvényű házirendnek nem kell engedelmeskednünk, nem engedjük be őket a NAP-pal védett hálózatba.

A NAP maga is sokszereplős. Emeljünk ki két fontos kiszolgálószerepet!

A NAP-rendszer központjában a NAP Health Policy Server áll, amit a dokumentációkban NPS rövidítéssel illetnek. Ez foglalkozik a kliensekről befutó egészségügyi zárójelentések kiértékelésével; olyan Windows Server 2008 kiszolgáló, amelyen az NPS-szolgáltatás fut. Maga az NPS egyébként a korábbi IAS-t (Internet Authentication Server) váltja fel, tehát RADIUS-kiszolgáló és VPN-házirendi központ is egyben. Néha úgy is hívják, hogy egy AAA, azaz Authentication, Authorization és Accounting szerver.

Ha IPSec-kel szeretnénk NAP-ozni (például mert buta a switchünk), szükségünk lesz egy Health Registration Authorityra (HRA), amely közvetlen kapcsolatban áll az ügyfélszámítógépekkel, és átveszi azok kórházi zárójelentéseit, és továbbítja az előbb említett NPS-nek. Ezen a kiszolgálón Windows Server 2008 és IIS fut. Ide kapcsolódnak be a NAP-ügyfelek HTTP- vagy HTTPS-protokoll segítségével, megmutatják a zárójelentésüket, és ha a HRA egészségesnek találja őket, visszaad egy Health Certificate-et, ami lehetővé teszi majd a megfelelő IPSec-házirend használatát. Tehát valahol a horizonton látszódnia kell egy Certificate Servernek is...



3. ábra. Mivel biztosítsuk az izolációt?

Ha nem IPSec-et használunk, akkor az egyes szolgáltatásoknak megfelelő NAP Enforcement Pointok látják el a védelmet a

korlátozott vagy teljes hozzáférés megadásával. Ilyen lehet például a DHCP- vagy a VPN-kiszolgáló, a 802.1x-nek megfelelő switch vagy a WiFi Access Point. Ezek mindegyike közös abban, hogy RADIUS-szal kommunikálnak az NPS felé. A switch és az Access Point gyárilag képes erre – vagy ha nem, kukába velük. A DHCP és az RRAS csak akkor, ha feltelepítjük rá a RADIUS-klienst. Most jön a csavar: ezeken a gépeken tehát futnia kell az előbb említett NPS-szolgáltatásnak, de csak azért, mert abban van megvalósítva a RADIUS-protokoll! De ettől ezek nem válnak NPS-szerverré!

Remediation Servers: ezek azok a kiszolgálók, amelyeket mindenki, tehát a betegek is elérhetnek. Patikák. Ezekre érdemes feltenni azokat a frissítéseket, ami a gyógyulásukat hozhatja, hogy ha véletlenül lebetegedtek, legyen hova fordulniuk orvosságért.

Health Requirement Servers: ezekkel egy darabig nem fogunk találkozni, külső gyártók által létrehozott egyéb egészségügyi központok, amelyek további ellenőrzési lehetőségeket adnak a NAP-rendszernek. Ilyen lehet például egy központi víruskergető-adatbázis, amelyik „sugározza” a megfelelőségi szempontokat.

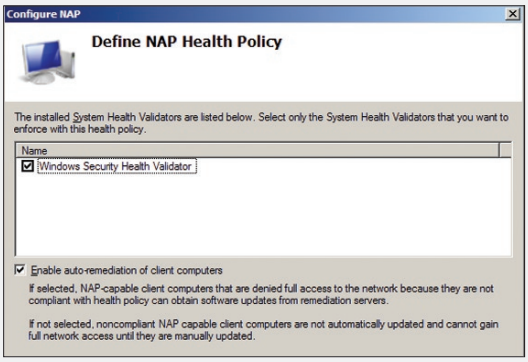
Ezeken felül vannak a védendő objektumok, a hálózatok és hálózati eszközök. Az *1. ábra* remekül összefoglalja a különböző NAP-esetek kommunikációs útvonalait.

Érdemes megfigyelni, hogy bár az ügyfelek sokféle úton-módon, többféle protokollal (és autentikációs módszerrel) próbálkozhatnak bejutni a hálózatba, a NAP-kommunikáció az NPS felé mindig RADIUS! Egyébként nem kell ennyi vasat vásárolni: mindegyik NAP-szerepkör felpakolható ugyanarra a gépre.

A NAP kezelése

Kezdjünk el dolgozni a NAP-pal, indítsuk el a Network Policy Servert a rendszergazdai eszközök közül! A *2. ábra* a NAP kezelőfelületét mutatja Windows Server 2008 kiszolgálón. Megfigyelhető, hogy magában foglalja a teljes RADIUS-protokollt is. Láthatjuk a Remediaton Server Group-ot, a patikákat is. Ha valaki az RRAS-házirendeket keresi, azokat is megtalálja a Policies\Network Policies mappában. A főablakban egy varázsló fogad bennünket, amely előzékenyen a NAP-varázslatot kínálja fel (a másik két varázsló a RADIUS-protokollt állítja be).

Menjünk végig az úton! Az első lépésben nevet kell adnunk a NAP-házirendnek, és ki kell választanunk a felhasználandó korlátozási módszert. Én most az IPSec-es ágon megyek végig, mert ez az egyetlen, amelyik helyi hálózaton működik, nem igényel speciális hardvert, és meghekkelhetetlen. (A 802.1x-hez megfelelő switch kell, a DHCP pedig elég könnyen megkerülhető. A VPN pedig VPN.)



4. ábra. Mi ellenőrizze a kliensek egészségét?

Amint kiválasztjuk a varázsló első lépésében az IPSec-korlátozást, megjelenik egy figyelmeztető ikon, hogy tudassa velünk: a varázslat után még rengeteg teendőnk lesz: Certificate Services, Group Policy stb. *(3. ábra)*.

Ezt követően be kell állítanunk a még fel sem telepített HRA-kiszolgálókat mint RADIUS-ügyfeleket. Emlékezzünk: ezek a jószágok állítják ki az egészségességet bizonyító tanúsítványt. Én egy gépen szeretném futtatni az NPS–HRA párost, ezért egy Next-tel továbbmegyek. A következő lépésben lehet kiválasztani az érintett ügyfélszámítógépeket, ahol szintén továbsiklok egy Nexttel (és a képernyőképet sem vágom be ide), így minden számítógépre érvényes lesz, még a tartományon kívüliekre is. Az a jó!

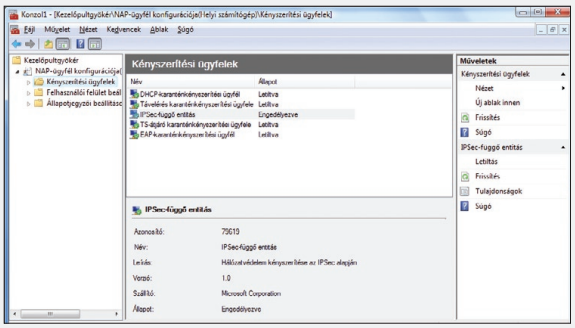
Ezután következik a Health Validatorok kiválasztása. Egy alap Windows-rendszerben a Windows Security Health Validator érhető el csupán: az ügyfélgépeken futó Security Center által nyújtott adatok fogják adni az egészségügyi információkat: van-e Defender telepítve, hogy állunk a hotfixekkel, elavult-e a víruskereső.

Ezt már megmutatom *(4. ábra)*, mert itt lehet beállítani azt is, hogy legyen-e gyógyszerárusítás a patikákban. Az összefoglaló képernyőn lehetőségünk van a teljes varázslat dokumentálására (HTML formátumban), hogy később is tudjuk, mit tettünk. A varázslat eredménye két Network Policy: egy az egészségeseknek (teljes hozzáférés), egy pedig a betegeknek (patika only). Ezzel a dolog könnyebbik részével meg is volnánk. Most jön a neheze: a HRA elkészítése, IIS-estül, Certificate Serverestül, valamint az ügyfélszámítógépeken a megfelelő NAP-ügynök bekapcsolása Group Policyval.

A munkaállomások beállítása

A munkaállomásokon található NAP-ügynököket akár egyesével is be lehet kapcsolgatni a Vistában már megtalálható NAP-ügyfélkonfigurátor MMC-konzollal. Amikor betöltjük ezt a konzolt, rákérdez, hogy nincs-e a birtokunkban konfigurációs fájl, amivel egycsapásra elintézhető az egész beállítás. Kezdetben nincs, de ha már egy gépen megcsináltuk, mint például ezen a magyar nyelvű Vistán itt *(5. ábra)*, akkor a konzolból ki tudjuk exportálni a beállításokat, és a következő gépen már gyorsan végzünk az importtal.

Egyébként ezeket az ügynököket nemigen kell és lehet finomhangolni. Kikapcs-bekapcs, és nagyjából ennyi. Ezenkívül be lehet állítani egy címből, egy feliratból és egy képből álló figyelmeztető üzenetet a felhasználónak, hogy tudja, ha a NAP miatt (a gépének egészségi állapota miatt) nem ér el valamit a hálózaton. Ugyanezt megtehetjük Group Policyból is.



5. ábra. Több kényszerítési ügynökünk is működhet párhuzamosan

Fóti Marcell
MCSE, MCT, MVP, MZ/X
(marcellf@netacademia.net)

A HARKÁLY ÉS A HANGYÁSZ

Ha az a feladat, hogy a hangyát ki kell enni a fa kérge alól, arra jó a harkály. Ha a bogarat az odvas fából kell kirágni, rögtön hangyászért kiáltunk. Nem lehetne összepárosítani a kettőt? Talán, de addig is házasítsunk össze két másik fajt, amelyek talán nem is olyan idegenek egymástól! Legyen, mondjuk, a Failover Cluster és a virtualizáció.

December közepe óta letölthető a Windows Server 2008 RC1 x64-Hyper-V kiegészítéssel. A számtalan újdonság közül kettő ragadja meg első látásra a rendszerintegrátor figyelmét: a Hyper-V virtualizáció és az arculatában és belvilágában is jelentős változtatásokon átesett fürtszolgáltatás. Mind a kettő izgalmas, és a gyakorlatban egyre inkább előtérbe kerülő megoldást kínál, már magában is: a clustering megvalósításakor manapság már nem (feltételenül) kell a jellemzően szűkös költségvetésbe méregdrága Fibre Channel-infrastruktúrát is beleerőltetnünk – az iSCSI a gyors hálózatokkal vállvetve hódít teret a failover clusternek is –, a virtualizáció pedig – függetlenül attól, hogy melyik típussal van dolgunk – tagadhatatlanul csábító előnyökkel jár. Gyors helyreállítások, migrációk és gazdaságos hardverkihasználtság, hogy csak a legvastagabban szedett címszavakat említsük.

Mi sül ki kettejük házasságából?

Gondoljunk csak bele, a clusterbe szervezett szolgáltatások „ősidők” óta mint virtuális szerverek vannak jelen a hálózaton. Objektumokkal dolgoznak, amelyeken belül az elérhetőséget és az érdemi tartalmat képviselő resource-ok együttesen képeznek egy halmazt, a groupot. Ha pedig ez a group egyszer rá lett bízva a clusterre, az bizony annak létéért, életben tartásáért és cluster-aware

1. kép. A virtualizáció a Cluster applikációs varázslójában

applikáció esetén egészséges működéséért is a körme szakadtáig ragaszkodni fog. A clusternek számtalan ötlete van arra, hogy a legváratlanabb esetekben is elvégezze feladatát. A Windowsba integrált alapszolgáltatások és a „nagy, komoly kiszolgáló” szerepkörű alkalmazások jó részét ugyanúgy támogathatja, mint az általunk a rendszerbe illesztett scriptet vagy egy olyan szolgáltatást, ami még életében nem is hallott fürtözésről.

Miért is maradna ki ebből a körből a Hyper-V? Hát, nagyon úgy néz ki, hogy esze ágában sincs kimaradni *(1. kép)!*

Hol igényli a virtualizáció a fürtszolgáltatással való kapcsolatot? Természetesen a rendelkezésre állásban. A virtualizáció magában nem kínál magasabb rendelkezésre állást, mint amennyit Murphy szán neki, hiszen akár a hardvert, akár a gazda-operációsrendszert bármikor elütheti a villamos, a vendég-operációsrendszer vagy a benne futó alkalmazás is csak egyszer lépjen le figyelmetlenül a járdáról... és kész a baj. Ha sóhajtozunk egy integrált megoldásra áhítozva, hát tessék! Több modell is rendelkezésre áll, csak győzzünk választani!

Guest Cluster – egy gépen

Legyen ez inkább csak játékszer – remek lehetőség egy fejlesztőnek, aki inkább az alkalmazásának fürtben való viselkedését vizsgálja, vagy tesztplatform a cluster témában szárnyait bontogató olyan rendszergazdának, akit nem dobnak meg egy teljes kiépítettségű blade-rendszerrel, hogy tesztelgessen csak, okosodjék bátran. Viszont akár komolyan is vehetjük, ha kizárólag a clusterbe szervezett alkalmazás rendelkezésre állását vizsgáljuk: a szolgáltatás védve van...

Hogy is néz ki egy ilyen „Egygépes Guest-Cluster”?

Először is szükségünk lesz egy jó sok memóriával rendelkező gépre. A gazdarendszer és a virtualizációs környezet telepítése után létre kell hozni minimum 3 virtualizált vendég-operációsrendszert. Kettőből lesz a cluster két node-ja, egyet megtartunk tartományvezérlőnek. (Lehet akár a 2 node bármelyike is DC, vagy akár mindkettő, de egészségesebb, ha külön DC-t tervezünk be.) A megosztott diszkalrendszer lehet többféle: iSCSI, amit a tartományvezérlőre telepített target-komponenssel valósíthatunk meg,

vagy a komolyabb virtualizációs környezetek által emulált „shared parallel scsi” (vigyázat, a Windows Server 2008 Failover Cluster ezt már nem támogatja!).

Gyors telepítés, teszt, tapsvihar. Ha iSCSI-val futottunk neki, és a gazdagépen maradt még szabad kapacitás, akár 3 vagy többtagú fürtöt is létre lehet hozni.

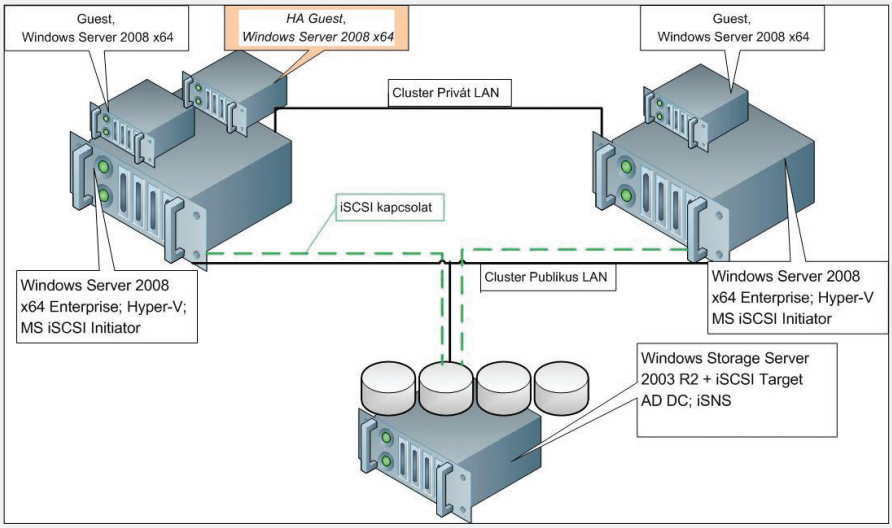
Guest Cluster – több gépen

Ez a megoldás már éles környezetben is megvalósítható, sőt! Megvalósítandó minden olyan esetben, ahol rendelkezésre áll két vagy több olyan szervergép, amelyekből, illetve ver bázisú iSCSI-megoldása, mint például egy HP MSA 1510i, akkor még a target megvalósításához sem kell gép, de szegény ember vízzel főz...

A Host Cluster

Igen, lassacskán a cikk témájánál vagyunk, hiszen pont ilyet építhetünk a még csak tesztelésre való Hyper-V és a Failover Cluster segítségével a Windows Server 2008-ban! Mi is ez a Host Cluster?

Gondolkodjunk kicsit máshogy, mint az előző modellek esetében: ne a fürtöt illesszük a virtualizációba, hanem...hmm... csináljuk



2. kép. Ebben a környezetben vizsgálódunk

a rajtuk futó gazda-operációsrendszerekből nem akarunk clustert építeni, de az egyes node-okon futó vendégekből igen – tehát a cluster node-jai az egyes fizikai gépeken virtualizált vendégek. Ebben az esetben az iSCSI már magától értetődő, ha a megosztott diszkek megvalósításán gondolkodunk. Hogyan is lehetne mondjuk Fibre Channel-adaptert illeszteni egy guestbe? Hát sajnos... sehogy.

Mi kell a több fizikai gépes Guest Cluster elkészítéséhez?

Vegyünk három gépet. Kettőből egymástól függetlenül lesz gazdagép a virtualizációs környezetben, egyet megtartunk iSCSI target portálnak és tartományvezérlőnek. A dedikált DC létjogosultsága ugyanúgy magyarázható, ahogy az egygépes esetben: jobb, ha azt nem keverjük bele a játékba. Miért nem a gazdagépek akár mindegyike DC? Lehetnek azok is, de az iSCSI target azért legyen külön. A kötekedőknek: akinek van a polcon hardfordítva! Eddig mindkét guest cluster modell esetén úgy kezdtük, hogy a gazdagépre virtualizációs környezetet, majd abba vendégeket telepítettünk, ezekből lettek a cluster node-jai. Most dőljünk hátra és fantáziáljunk! Gondolatban próbáljuk meg a clusterbe illeszteni a virtuális masinát és próbáljuk meg, hogy működik-e úgy, mint bármelyik másik jól nevelt és clusterbe szervezett szolgáltatás! Mozgassuk át a cluster egyik node-járól a másikra... és vissza! Ez lenne a Host Cluster? Ez bizony. Hogy is néz ki ez a gyakorlatban?

Építsünk Host Clustert!

Addig, amíg az előző modelleket javarészt egy Microsoft Virtual PC-vel is meg lehet valósítani, a következő teszt már szigorúan Hyper-V- és Windows Server 2008-specifikus környezetet kíván. Két olyan gépet legalább, amelyek megfelelnek a kritériumoknak: x64, DEP (AMD xD, Intel nX) és virtualizációtámogatás (Intel VT, AMD-V). Ilyen, valljuk be, még az otthoni gépünk is lehet, csak legyen belőle legalább kettő. Szükségünk van továbbá a jól megszokott különálló DC és iSCSI target szerepkörű gépünkre *(2. kép)*. Itt természetesen a Fibre Channel is megél, sőt, teljesítmény szempontjából melegen ajánlott.

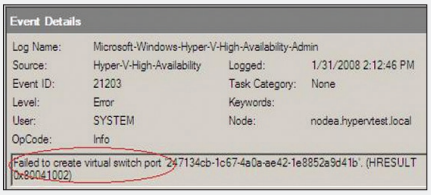
A telepítés részleteivel nem untatnám a kedves olvasót, hiszen aki látott már clustert, gépiesen kattintgatva telepíti a leendő node-okat „egyformára”, lépteti tartományba és konfigurálja a hálózatot. Egyszer csak minden együtt van ahhoz, hogy nekilássunk a Host Cluster építésének. Hogyan?

Nagy vonalakban valahogy így:

1. Telepítsük fel a Hyper-V szerepkört mindkét gépre. Ez gond nélkül megtörténik, még akkor is, ha a hardverünk által támogatott (naná, mi választottuk ezt a gépet!) VT paraméter a BIOS-ban ki van kapcsolva. Ez sok gépen alapértelmezés! A Hyper-V ezt telepítéskor nem vizsgálja, csak az első virtuális masina indításakor. Akkor aztán elég egyértelmű hibaüzenetet kaphatunk, miszerint nem lesz itt semmiféle virtualizáció, ugyanis a hypervisor nem töltődött be. Jó tanács: kapcsoljuk be jó előre a VT-t!

2. A Hyper-V telepítése a Virtuális Switchek konfigurálásával folytatódik. Még egy jó tanács: tehetünk bármit a virtuális hálózattal, de azt a bármit teljesen egyformán tegyük mindkét node-on! Egy karakternyi elgépelés az egyik virtual switch nevében már elég ahhoz, hogy jóval később a *3. képen* látható üzenetet kapjuk.

3. Haladjunk tovább! Konfigurálta közben valaki az iSCSI targetet? Legyen Quorum és néhány adatdiszk, a méretezéskor figyeljünk oda, hogy Windows Server 2008-at telepítünk majd a virtualizációba, és az így létrejövő vhd állomány legalább 6 gigabájt!

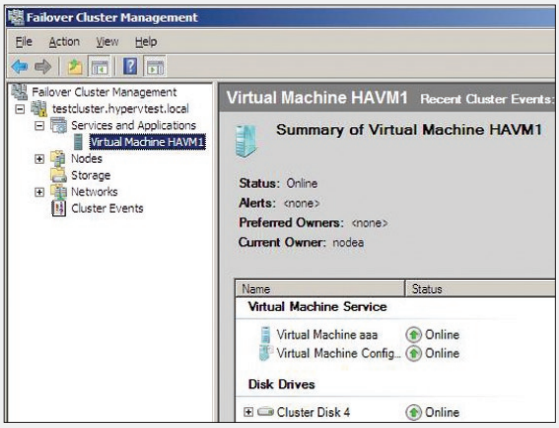


3. kép. Mi is van most a hálózattal?

Az iSCSI initiator – szerencsére – alapértelmezés szerint ott van a node-okon, aktiváljuk és csatlakozzunk a targethez. Járjunk

el pont úgy, ahogy a Windows Serverek korábbi verzióival tennénk, azaz cluster-szerviz nélkül ne lássák a node-ok egyszerre a formázott logikai egységeket a target mögött! Ugye, azért mindkét node-ról látjuk a diszkeket?

4. Jöhet a Failover Clustering telepítése mindkét node-on. Ez egy Feature checkboxának bebillentése, egyszerűen elvégezhető, utána következhet a környezet ellenőrzésének procedúrája (Validate), ez kicsit időigényes, de így legalább meggyőződhetünk a tesztkörnyezet alkalmasságáról.



4. kép. Magasan rendelkezésre álló VM

5. A következő lépésben szülessen meg a cluster! (Nem ez a cikk hivatott pontosan leírni a lépéseket, de annyit meg kell jegyeznem, hogy a folyamat roppant egyszerű, a varázsló teszi a dolgát.) Gyors ellenőrzés: hálózatok OK, diszkek online állapotban, egy tesztcélú applikációs csoportban mozgathatók a node-ok között.

6. Térjünk vissza az egyik node-on a Hyper-V Managerbe (jellemzően azon a node-on, amelyik a megosztott diszkeket tulajdonolja), és készítsük el a virtuális gépünket. Itt a konfigurációs állomány és a virtuális diszk helyére figyeljünk: mindkettőnek a kiszemelt megosztott diszken kell lennie. Ha megvan, telepítsünk bele egy Windows Server 2008-at, és készüljünk fel a finálére. Már csak egy lépés, és készen vagyunk!

7. A virtuális gép beillesztése a Clusterbe egyszerűbb, mint gondolnánk. Induljunk a Configure a Sevice or Application varázslóval a Failover Cluster Management konzolon. Mit szeretnénk clusterbe szervezni? Választható a Virtual Machine, mint resource-típus! Akkor azt. Jó, de melyiket? Nem muszáj az összes virtuális gépünket fürtözni, lehet bármelyik node-nak önálló, saját virtualizációs feladata. Válasszuk azt, amelyik a közös diszkre lett telepítve. Ennek feltétele, hogy a guest legyen kikapcsolva. Sikerült? Kész vagyunk, ha...

8. ...ha sikerül a virtuális gép mozgatása a node-ok között a cluster konzolból. (Na, itt kaphatjuk a fent jelzett virtuális network switch port problémájával kapcsolatos üzenetet, ha valamit elrontottunk.)

Ezzel megcsináltuk a host clustert Windows Server 2008-ban HyperV-vel. Igen, de nem ez az igazi újdonság, ilyet némi fúrás-faragás-hegesztés árán a Microsoft Virtual Server 2005 R2-vel is előállíthattunk, főleg ha a szabadon letölthető „havm.vbs" scriptet is bevetettük. A nagy öröm inkább az, hogy ilyesmivel itt nem kell bíbelődni, az operációs rendszer és a virtualizáció igen szép integrációról tesz (már most) tanúbizonyságot, pedig hol van még az RTM, különösen a Hyper-V végleges változata.

És még valaminek örülhetünk, ami szintén nem egy utólag beillesztett scriptnek köszönhető: ez pedig a Quick Migration.

Quick Migration – az állapot megőrzése

Gondoljunk csak bele, hibatűrő rendszerünk van – viszont jön egy tervezett, de elkerülhetetlenül sürgős beavatkozás, ami miatt csütörtök délben a cluster egyik node-ját le kell állítani. Mi legyen? Ha átmozgatjuk a virtuális gépünket a másik node-ra, akkor számolnunk kell annak leállásával, azaz a benne futó szolgáltatás és az operációs rendszer is jó időre kivonja magát a forgalomból. Ez még fájóbb akkor, ha épp olyan folyamat zajlik a virtuális gépen, amit megszakítani sehogy sem szerencsés, hiszen olyan régen küzd a feladattal, és most elölről kell kezdenie szegénynek...

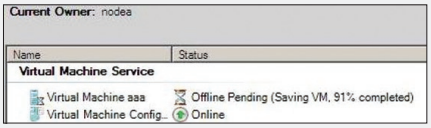
Jó hír: nem kell! Nem kell leállítani, legalább is a szó megszokott „shut down" értelmében semmiképp. Tud Hyper-V állapotot menteni, mielőtt kiiktatnánk a guestet a forgalomból? Persze hogy tud, hiszen ez alapvető tulajdonsága még a Virtual PC-nek is.

Ezt a Faiover Cluster is tudja a Hyper-V-ről, az *5. képen* látható a bizonyíték. Érdekes képernyővel szembesülünk a mozgatáskor!

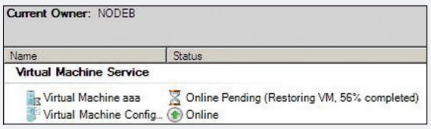
Mindez tényleg azt jelenti, hogy a mozgatást megelőzi az állapot mentése a közös diszkre, ahonnan a másik node – az új tulajdonos – a mentett állapotot olvassa fel. Hogy mennyi időt vesz igénybe? Ez leginkább a diszkkel való kommunikáció sebességétől függ, de a mi tesztkörnyezetünkben átlagosan az állapotmentés 17, a mozgatás a függőségi viszonyoknak megfelelő leállítással és a másik node-on való újraindítással 5, az állapot visszaállítása (tehát a guest hadrendbe állítása) 15 másodpercig tartott. Az annyi, mint 37 másodperc! Tudunk ennyi idő alatt egy szabályos leállítást és újraindulást produkálni? Úgy gondolom, nem. A Quick Migration funkció rászolgál a nevére.

Quick Migration vagy Live Migration?

Még egy gondolat, ami szorosan illeszkedik ehhez a témához: a virtualizáció és a fürtszolgáltatás kapcsolatára jellemző, hogy együtt milyen leállásokat képesek tolerálni, és persze az is, hogy hogyan. A leállások, amelyeknek tanúi és sok esetben szenvedő alanyai vagyunk, jellemzően kétfélék: tervezettek és meglepetésszerűek.



5. kép. Az állapot mentése...



6. kép. ...és visszaállítása a másik node-on

Előbbire jó előre felkészülünk, és csak akkor nyomjuk meg az átterhelést elindító „nagy piros gombot", amikor komoly esély van arra, hogy a rendszerünkbe szervezett szolgáltatások igen rövid időn belül – és főleg adatvesztés nélkül – ismét teszik a dolgukat. Igen rövid idő? Mennyi is az pontosan? Ha az előzőekben tárgyalt Quick Migration működését megértettük, akkor belátható, hogy ez bizony nagymértékben függ a környezet változóitól.

Ami annyit jelent, hogy bár mozgatáskor

a virtuális gépünk egy kis ideig nem érhető el, de amikor új erőre kap, akkor ott folytatja, ahol abbahagyta. Nem lehetne megúszni köztes idő nélkül? Dehogynem, az eszme megvan, úgy hívják, hogy Live Migration, vagy más néven Hot Migration. Kicsit utána olvasgatva a témának, könnyen rálelhetünk azokra a virtualizációs témájú blogokra, amelyek szerint nemcsak az eszme van meg, hanem az ígéret is: benne lesz a Windows Server 2008-ban – egy későbbi kiadásban. Itt a mozgatás, azaz a host tervezett leállásából adódóan a guest egy másik node-ra való átterhelése közben a kapcsolat a szolgáltatással kliensoldalról nézve nem vagy csak nagyon rövid időre (kevesebb mint egy másodpercre) szakad meg. A megoldást türelmesen és kíváncsian várjuk!

Végül gondoljunk bele, mi történik tervezhetetlen, meglepetésszerű leálláskor! Jóllehet clusterbe szerveztük a virtuális gépet, és bár a cluster teszi a dolgát, az könnyen belátható, hogy ebben az esetben nem számolhatunk a mentett állapottal és annak helyreállításával. Virtuális gépünk újraindul, és hála a fájlrendszernek, illetve az alkalmazás esetleges recovery mechanizmusainak, majdnem ott folytathatja, ahol abbahagyta. Jó esetben. Reméljük a legjobbakat. És ha nem? Erre bizony készüljünk csak fel, hiszen nincs olyan rendszer, ahol a mentés vagy egy jól átgondolt stratégia vész esetére teljesen felesleges lenne! Ha nem készültünk fel, még mindig ott a lehetőség egy jó kis bitvadászatra. Vagy marad a varázslat.

Végítélet

A virtualizáció jelentősége és jövője megkérdőjelezhetetlennek látszik, főleg ha a magas rendelkezésre állással is párosul. Az üzemeltetők többsége értékeli a kisebb-nagyobb feladatokkal ellátott, különböző gyártmányú, korú és kapacitású szervereinek konszolidációs lehetőségét kevesebb fizikai hardver fölé, főleg akkor, ha az így konszolidált szerverek eszközkezelőkből fakadó hardverfüggősége innentől megszűnik. Melyik rendszergazda vagy fejlesztő ne használna olyan tesztrendszert, amelyik bármikor, pillanatok alatt előállítható, és ráadásul pont ugyanolyan, mint a végleges? Végül essen szó a nagy adatközpontok fizikai gépeinek dinamikus terhelhetőségéről is, quick vagy live migrációval mára már ez sem vízió.

Ami pedig tény: Láthatunk egy RC1 állapotban lévő operációs rendszert egy olyan – sok szempontból megújult – Cluster szolgáltatással, amit nem ez a cikk hivatott feltárni, erről ugyanebben a számban is olvashatunk részletesen. Kipróbálhatunk egy bétastátuszban lévő virtualizációs megoldást, a Hyper-V-t, aminek a belvilágáról szintén nem ebből az írásból kell tájékozódni, de mikrokerneles Type 1-es virtualizációról van szó, és ez bizony teljesítményben és megbízhatóságban sokat ígér! (A Hyper-V-re a teszt során talán egyetlen komoly panaszom lehet: sikerült létrehozni egy virtuális gépet, amit később sehogy sem sikerült letörölni a konzolból. Ennél nagyobb baj bétaszoftverrel ne legyen.) Integráltuk a Clustert és a Hyper-V-t, építettünk több fajta guest clustert, és könnyűszerrel összejött a host cluster Windows Server 2008 x64 full install környezetben. Csináljuk végig legközelebb ugyanezt Server Core-ral is!

Székács András
(andras@edupro.hu), MCT, MCSE, MCTS, Számalk

TÁROLJUNK – OKOSAN!

A központosított adattárolók (storage-ok) világa sokunk számára tűnik titokzatosnak, bonyolultnak és nehezen megközelíthetőnek. Ez a titokzatosság azonban remélhetőleg jelentősen csökken majd, ahogy gyakoribbá válnak az adattároló megoldások a kis- és középvállalati körben is.

Ebben az írásban azokat az eszközöket mutatom be, amelyek a Windows Server kiszolgálók és az adattárolók összekapcsolását egyszerűsítik le, és teszik elérhetővé ezek használatát a különleges ismeretekkel nem rendelkező rendszergazdák számára is.

Storage-egyszeregy

Első lépésként mindenképpen érdemes egy kis elméleti áttekintéssel és fogalommagyarázattal kezdeni az ismerkedést az adattárolókkal. Annál inkább szükségesnek tűnik ez, mert annyira különleges területről van szó, hogy a legtöbb témához kapcsolódó kifejezésnek nincs széles körben elfogadott magyar szaknyelvi megfelelője sem. Már az adattároló kifejezés használata is kompromisszum eredménye – pontosabb kifejezés hiányában használom a Data Storage magyar megfelelőjeként.

Adattárolóinkat többféle szempont szerint csoportosíthatjuk, az egyik legkézenfekvőbb mindjárt az, hogy milyen módon csatlakoznak kiszolgálóinkhoz. A leggyakrabban használt csoport minden bizonnyal a közvetlenül csatlakoztatott adattároló (Direct Attached Storage – DAS), hiszen ez jelen van csaknem minden kiszolgálóban és asztali gépben is. Ebbe a csoportba tartoznak az ATA, SATA és SCSI csatolófelületű belső és külső diszkek. A technológiai megoldás vitathatatlan előnye, hogy az adattároló eszközöket nagy sebességgel érjük el, az átviteli sebesség másodpercenként 80-100 megabájttól akár 640 megabájtig is terjedhet. Ez a sebesség viszont egyedül annak a gépnek áll rendelkezésére, amelyikhez az eszközöket csatlakoztattuk. Kivételnek csak a kétportos külső SCSI-adattárolók számítanak, amelyeket gyakran használnak egyszerűbb fürtök (2-nodes failover cluster) adattárolójaként. Ha további gépek számára szeretnénk elérhetővé tenni a DAS-eszközök tárolókapacitását, akkor azt csak hálózaton, az operációs rendszer nyújtotta protokollon keresztül tehetjük meg, számottevően kisebb sebességgel.

Az adattárolók következő csoportja a hálózati adattároló (Network Attached Storage – NAS). Ezek – beágyazott operációs rendszerüknek köszönhetően – önálló egységként jelennek meg a hálózaton, és valamely népszerű hálózati protokollon (általában CIFS vagy NFS) keresztül érhetők el a felhasználók számára. A komolyabb eszközök már hibatűrő diszkrendszert tartalmaznak, de sebességük lényegesen elmarad a DAS-eszközökétől, hiszen osztozni kell más felhasználókkal a hálózati sávszélességen, és az alkalmazott protokoll is lassító tényező – erről kicsit később még lesz szó. Határozott előnyük viszont a NAS-eszközöknek, hogy a tárolókapacitás független az egyes számítógépektől, és akár egy másik telephelyen is rendelkezésre állhat – az egyetlen követelmény a TCP/IP-kapcsolat és a megfelelő protokollok átengedése a tűzfalakon.

A legkülönlegesebb (és egyben legköltségesebb) adattárolási megoldás az adattárolási hálózatok (Storage Area Network – SAN) alkalmazása. Ebben az esetben ugyanis nem az az elsődleges cél, hogy a végfelhasználók számára közvetlenül biztosítsunk nagy tárolási kapacitást, hanem hogy a kiszolgálóink érjenek el nagy tárolási kapacitásokat, nagy sebességgel és szükség esetén megosztott módon. Az így létrejött tárhelyet persze ki is ajánlhatjuk a felhasználók számára egy fájlkiszolgáló esetén, de az esetek többségében inkább kiszolgálóoldali alkalmazásoknak adjuk át, például adatbázisok tárolására vagy fürtözött rendszerek közös tárhelyeként. A leggyakrabban használt technológiai megoldás a SAN-eszközök esetén az optikai hálózatok és a gyors SCSI-diszkrendszerek együttes alkalmazása. Az optikai hálózat akár másodpercenkénti 10 gigabit átviteli sebességet is képes nyújtani több száz méteres (súlyosabb pénztárca esetén akár 100 kilométeres) távolságra is. A leggyakrabban alkalmazott FCP

(Fibre Channel Protocol) protokoll pedig a jól ismert SCSI protokoll egy változata, amely blokkszintű, nagy sebességű elérést biztosít a diszkekhez (a leggyakoribb 2 vagy 4 gigabites hálózatok esetén ez 250, illetve 500 megabit névleges átvitelt jelent).

Az optikai hálózatra épülő adattárolási rendszerek egyik legnagyobb hátránya a magas kiépítési költség. Ennek ellensúlyozására fejlesztették ki és szabadalmaztatták 2003-ban az iSCSI protokollt, amelynek alapelve rendkívül egyszerű. Az SCSI-parancsokat és az adatokat, amelyeket a diszkrendszernek akarunk küldeni, csomagoljuk TCP/IP-csomagokba, és küldjük át a hagyományos Ethernet hálózaton! Így – némi teljesítményáldozat árán – megtakarítható a drága optikai hálózat kiépítése, az adattárolási hálózatot a meglévő (lehetőleg) gigabites hálózatunkon létre tudjuk hozni. Természetesen ezt a hálózatot gondosan el kell különíteni a felhasználói hálózattól (például VLAN-technológiával), és biztosítani kell az adatok biztonságát is, ezért építettek be az iSCSI protokollba IPSec-támogatást. Ráadásul visszakapjuk a NAS-eszközöknél látott rugalmasságot is – az iSCSI protokoll használatával akár telephelyeket, országhatárokat átívelő adattárolási hálózatokat hozhatunk létre, csupán TCP/IP-kapcsolatra és megfelelő tűzfalszabályokra van szükség.

Az iSCSI-technológia alkalmazása elérhetővé teheti a SAN-technológiát olyan vállalatok számára is, amelyeknek a hagyományos SAN kiépítése túl magas költségekkel járt volna. Egyes piaci elemzések szerint az iSCSI-technológia alkalmazására 2007-ben már 1 milliárd dollárt költöttek az amerikai vállalatok, az iSCSI alapú SAN-kapcsolatok száma pedig elérte a 6,5 milliót.

Összefoglalásként helyezzük el a különböző adattárolási megoldások protokolljait az OSI–ISO modellben! Az egyes protokollok elhelyezkedését vizsgálva jól látható, hogy az adatátvitel hatékonysága annál jobb, minél alacsonyabb szinten valósul meg, hiszen az alsóbb régiókban az adatok átvitele blokkszinten valósul meg, szemben a NAS-eszközökkel, ahol az adatátvitel fájlszintű, rárakódik a magasabb szintekre, és onnan visszaalakítás-többlet a számításigénye. Az is igaz viszont, hogy a megvalósítás költségeivel éppen fordított a helyzet: minél magasabb szintű protokollt használunk, annál olcsóbb a megvalósítás, főként mert az alkalmazott technológia szélesebb körben elterjedt.

Mivel az iSCSI viszonylag új és remélhetőleg itthon is széles körben megjelenő technológia, ismerkedjünk meg vele kicsit közelebbről.

Mit tud az iSCSI?

Definíciószerűen fogalmazva az iSCSI olyan protokoll, ami lehetővé teszi a kliensrendszerek számára (ezeket hívja az angol szaknyelv initiatornak), hogy normál TCP/IP-hálózaton keresztül SCSI-parancsblokkokat küldjenek SCSI-adattároló eszközöknek (ezek a targetek). Mindeközben a kliensek a diszkeszközöket úgy látják, mintha helyileg (tehát DAS-ként) csatolt diszkekről lenne szó. Szemben a hasonló szolgáltatást nyújtó optikai SAN-rendszerekkel, az iSCSI nem igényel különleges kábelezést, és a hagyományos hálózati infrastruktúrát használva nagy távolságokra is továbbítható.

Az iSCSI elméletileg bármilyen SCSI-kommunikációt lehetővé tesz a megfelelő szoftveres vagy hardveres átalakítók közbeiktatásával, a gyakorlatban azonban a két legelterjedtebb alkalmazási területe az adattárolási rendszerek konszolidálása (szétszórt adatok központosított tárolása) és e rendszerek katasztrófatűrővé tétele az adattárolási rendszerek tükrözésével a telephelyek között.

Az iSCSI-kliensek elsődleges feladata, hogy az SCSI-parancsokat IP-csomagokba helyezzék, és ebben a formában továbbítsák az adattároló kiszolgáló felé. Alapvetően két megvalósítási formája létezik: szoftveres és hardveres. A szoftveres változat tulajdonképpen egy kernelszintű eszközvezérlő, ami a hálózati kártyával és az operációs rendszer hálózati komponenseivel együttműködve dolgozik. Jelentős előnye, hogy szinte minden modern operációs rendszerben használható: vagy eleve beépített komponens – mint a Windows Vista és a Windows Server 2008 esetében –, vagy utólag telepíthető csomag, mint a Windows XP és Windows Server 2003 és a szabad forráskódú rendszerek esetében.

A hardveres változat egy PCI-csatolófelületű hibrid Ethernet–iSCSI host bus adapter (HBA) kártya, ahol az iSCSI-kapcsolat felépítése és a kapcsolódó számítások nagy részének elvégzése a hardver és az azt üzemeltető célszoftver (firmware) feladata. Nyilvánvaló, hogy a hardveres megoldás lényeges jobb teljesítményre képes, mert tehermentesíti az operációs rendszert az iSCSI-műveletek számításai alól. Ráadásul egy kiegészítő ROM közbeiktatásával lehetővé teszi az operációs rendszer SAN-ról történő indítását is, így egy iSCSI-kliens akár helyi diszkek nélkül is üzemeltethető.

Az iSCSI adattárolók (targetek) nagyvállalati környezetben általában célhardverek: kifejezetten iSCSI felületű adattárolók vagy hagyományos SAN-eszközök, és eléjük telepített iSCSI felületű optikai átalakítók kombinációja. Az egyszerűbb és így kevésbé költséges megvalósításokban ez gyakran egy hagyományos kiszolgáló, iSCSI-tudással felruházva, mint például a Windows Storage Server 2003.

A klasszikus SCSI-hoz hasonlóan az iSCSI-adattárolók diszkjeit is azonosító számokkal látjuk el, ezek a LUN-ok (logical unit number). Míg azonban az SCSI-nél ez egy-egy fizikai diszk azonosítója, addig az iSCSI

Réteg		Tipikus protokollok	Adattárolási megoldás
száma	neve		
7	Application	SIP, DNS, FTP, HTTP, NFS, NTP, SMTP, SNMP, Telnet, X.400, X.500, CIFS	NAS
6	Presentation	TDI, ASCII, EBCDIC, MIDI, MPEG, MIME, SSL	
5	Session	Named Pipes, NetBIOS, NWLink, X.225, iSCSI	iSCSI, SAN (FC)
4	Transport	TCP, UDP, IPSec, PPTP, L2TP, SPX	SAN (FC)
3	Network	IP, ARP, ICMP, DHCP, RIP, OSPF, IGMP, X.25 (PLP), IPX	SAN (FC)
2	Data Link	802.3 (Ethernet), 802.11a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, FDDI, Fibre Channel, Frame Relay, PPP, Token Ring	SAN (FC)
1	Physical	RS-232, T1, E1, 10BASE-T, 100BASE-TX, DSL, 802.11a/b/g/n PHY	SAN (FC)

1. táblázat. A különböző adattárolókon használatos protokollok helye az OSI-modellben

esetén logikai egységet jelöl, ami feltehetően egy hibatűrő diszkrendszer egy szelete, ezt felajánljuk a kliensek számára. Bizonyos implementációkban az így megjelenített diszk egy virtuális diszk, ami az adattárolón fájlként látható, a kliens felé pedig teljes értékű diszkként. A Windows Storage Server 2003 például kompatibilitási okokból és az árnyékmásolatok egyszerű támogatása érdekében a Microsoft szabványos VHD formátumát használja.

A kliensek és az adattárolók összekapcsolását címzéssel kell biztosítanunk. Három címzési forma szabványos, a leggyakrabban az IQN-t (iSCSI Qualified Name) használják: ez nem igényli az eszköz regisztrációját. A cím egy dátumot (év-hónap) és egy fordított doménnevet, valamint az eszköz azonosítóját tartalmazza például ilyen formában: iqn.2001-04.com.acme:storage.tape.sys1.xyz. A használt rendszertől függően az IQN-t magunk is generáltathatjuk, vagy a doménnevet és az egyedi azonosítót helyettesíthetjük az adattároló IP-címével. A másik két címzési forma regisztrációt igényel, mindkettőt az IEEE szervezet bocsátja ki. Az EUI (Extended Unique Identifier) címzés 64 bites (például eui.02004567A425678D), az NAA (Network Address Authority) 64 vagy 128 bites (például naa.02004567A425678D). Az utóbbi címzési forma teljesen kompatibilis az optikai adattárolókon használatos címzési formákkal, és mindkettő teljesen egyedi azonosító. Ezek a címek az optikai rendszerekben használt WWN (World Wide Name) azonosítók megfelelői az iSCSI-ra értelmezve.

A kapcsolat felépítéséhez általában négy adatot kell használnunk: az adattároló kiszolgáló nevét vagy IP-címét, a használandó portot (az alapértelmezett a 3260-as TCP-port), az eszköz címét valamilyen szabványos formában és opcionálisan az azonosításhoz szükséges jelszót (CHAP secret).

Ezzel máris elérkeztünk a biztonság kérdéséhez, és itt érdemes alaposabban elidőznünk, hiszen a SAN-hálózatok – és így egy iSCSI-ra épülő SAN is – a legértékesebb adatainkat hordozhatják. Korántsem mindegy tehát, mennyire tudjuk biztonságban tartani ezeket az adatokat. Az első és legfontosabb: mivel az iSCSI-kapcsolatok a hagyományos Ethernet hálózatot használják, és TCP/IP-csomagokból épülnek fel, a mi feladatunk, hogy ezt a forgalmat a lehető legjobban elkülönítsük a felhasználói hálózattól, és különösképpen, hogy megakadályozzuk ennek a hálózatnak mindenfajta kommunikációját az internet felé (hacsak nem kifejezetten egy ilyen szolgáltatáshoz szeretnénk kapcsolódni). A legjobb és leghatékonyabb a teljes fizikai elkülönítés (külön kábelezés és switch-ek használata), de az esetek többségében egy pontosan meghatározott VLAN és gondosan beállított tűzfalszabályok is elérik a kívánt eredményt. Ezzel az elkülönítéssel az autentikációra egyelőre kizárólagosan használható CHAP (Challenge Handshake Protocol) közismert sebezhetőségét is számottevően csökkenthetjük. Nagyobb rendszerek esetén szerencsés, ha az azonosításba egy RADIUS kiszolgálót is bevonunk, ezzel csökkenthetjük az egyedi adminisztratív hibák lehetőségét.

Fontos tudnunk azt is, hogy az iSCSI, több más SAN-protokollhoz hasonlóan, nem tartalmaz semmiféle beépített titkosítást, így aki hozzáférhet az iSCSI-hálózat forgalmához, az képes megszerezni vagy akár módosítani is az ott áramló adatokat. Ezt a veszélyt IPSec alkalmazásával háríthatjuk el, bár ezt viszonylag ritkán alkalmazzák, főleg a többlet-számításigény és a konfigurálás bonyolultsága miatt.

Az egyes iSCSI-funkciók operációsrendszer-támogatását a fenti táblázat mutatja be.

Operációs rendszer	Bevezetés ideje	Verzió	Elérhető funkciók
i5/OS	2006. 10.	i5/OS V5R4M0	Target, Multipath
AIX	2002. 10.	AIX 5.2	Initiator
Windows	2003. 06.	2000, XP Pro, 2003, Vista, 2008	Initiator, Target, Multipath
NetWare	2003. 08.	NetWare 5.1, 6.5, & OES	Initiator, Target
HP-UX	2003. 10.	HP 11i v1, HP 11i v2	Initiator
Solaris	2005. 02.	Solaris 10	Initiator, Target, Multipath
Linux	2005. 06.	2.6.12	Initiator, Target, iSER
NetBSD	2006. 02.	4.0, 5.0	Initiator (5.0), Target (4.0)

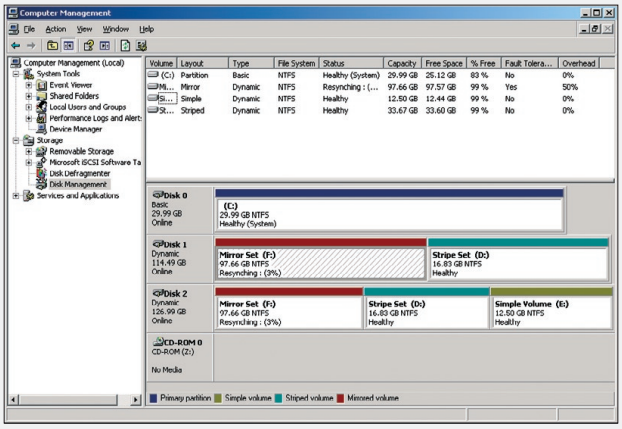
2. táblázat. Az iSCSI támogatása az egyes operációs rendszerekben

Építsünk saját storage-et!

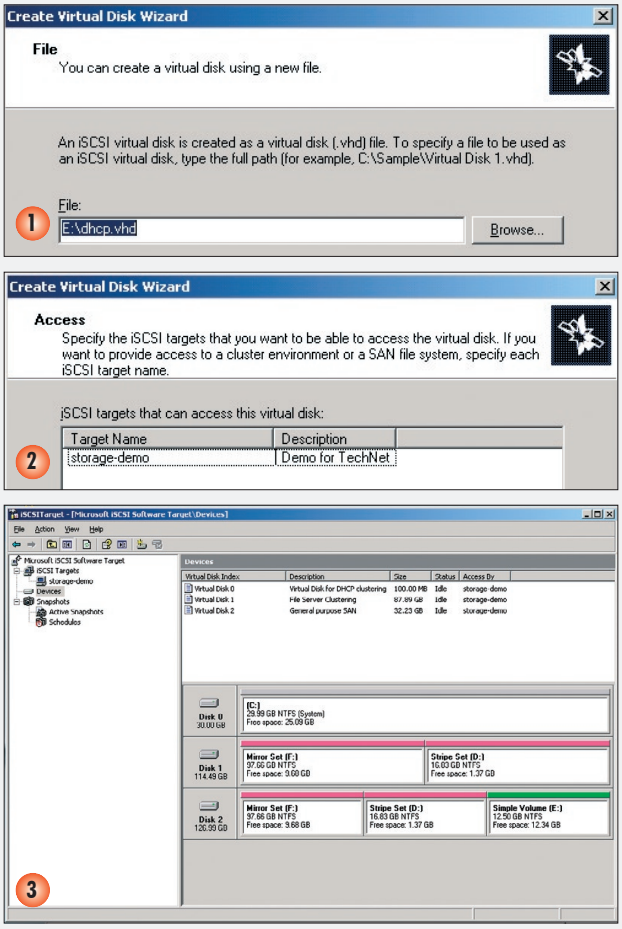
Az elméleti áttekintés után nézzük az iSCSI rendszer egy lehetséges gyakorlati alkalmazását! A következőkben szeretném megmutatni, mennyire egyszerű a kapcsolódás az adattárolóhoz, és a szolgáltatás felhasználásával milyen egyszerűen építhetünk például magas rendelkezésre állású rendszereket. A példában használt eszközök közül a Storage Manager for SANs már a Windows Server 2003 R2-es változatában is telepíthető összetevő (a Storage Explorerrel együtt), míg az iSCSI Initiator a Windows Vista és a Windows Server 2008 beépített komponense, külön telepítést sem igényel. (Korábbi Windows-verziókhoz az iSCSI Initiator ingyenes letöltés formájában elérhető a Microsoft oldalán.)

A cél egy Windows 2008-tartomány felépítése, amiben a DHCP és fájl szolgáltatást fürtözött Windows Server 2008-kiszolgálók nyújtják. A tartományvezérlő érdekességképpen legyen egy Server Core-változat a Windows Server 2008-ból, az adattároló pedig az egyszerűség kedvéért egy Windows Storage Server 2003 R2. Lássunk hozzá!

Az első lépés természetesen a tartomány felépítése és a kiszolgálók telepítése, illetve beléptetésük a tartományba. Mikor ezekkel a lépésekkel megvagyunk, akkor foghatunk neki az adattároló konfigurálásának. Virtuális környezetről lévén szó, elegendő lett volna néhány virtuális diszk fájlt létrehozni és a Storage Server alá csatolni. Most az érdekesség kedvéért egy külső Firewire diszket is csatlakoztattam a géphez, hogy kipróbálhassam, hogyan kezeli a Hyper-V a fizikai diszkeket. (Fizikai diszket csak úgy csatlakoztathatunk virtuális géphez, ha az a gazdarendszer számára offline státuszban van.) A Storage Server telepítése nem bonyolultabb, mint egy átlagos kiszolgálóé, csak az R2-komponensek telepítése után kell még néhány percet várnunk, amíg a megfelelő kiegészítő szolgáltatások települnek egy script segítségével. Persze, aki ilyen rendszert szeretne használni, az sosem fog találkozni ezzel a lépéssel, mert a Storage Server 2003 csak hardverrel



1. ábra. A rendelkezésre álló tárolókapacitás felosztása



2. ábra. A virtuális diszkek létrehozásának folyamata

együtt vásárolható, és ott már elvégezte ezt a műveletet az OEM-gyártó. Az első valós lépés tehát, hogy csatlakozzunk a kiszolgálóhoz, és konfiguráljuk a rendelkezésre álló fizikai diszkeket.

A rendelkezésre álló kapacitásból elég tarka konfigurációt állítottam össze: egy 90 gigabájt körüli RAID1-tömböt, egy 32 gigabájtos kötetet, ami két fizikai diszken helyezkedik el (stripe set) és egy 12 gigabájtos egyszerű kötetet.

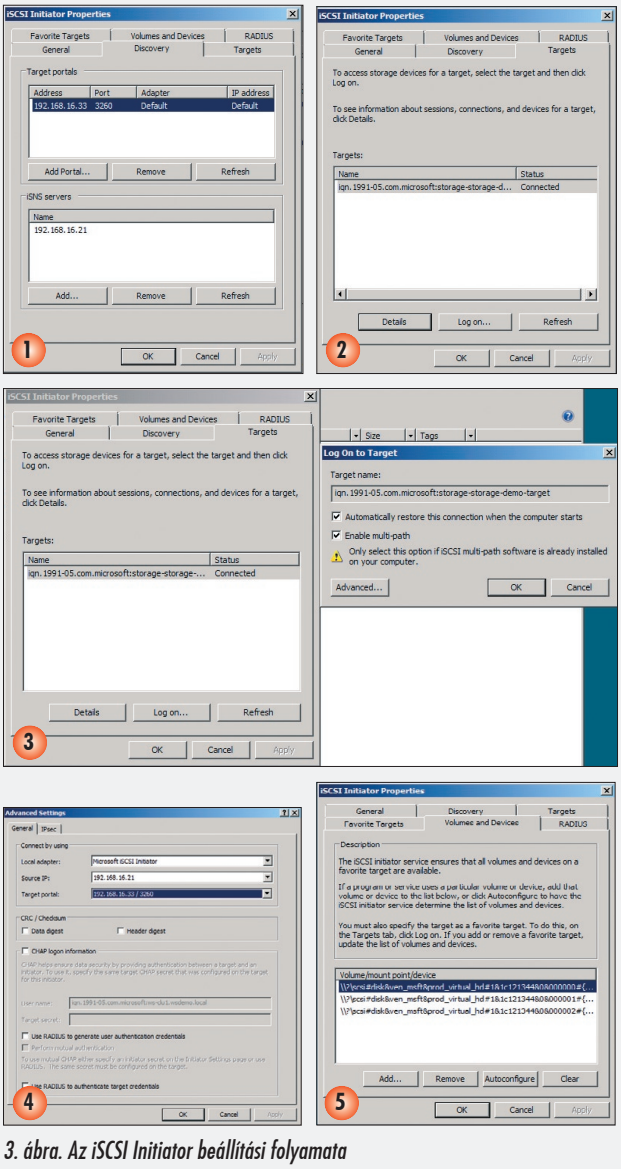
A következő lépés a virtuális diszkek létrehozása és engedélyezése az iSCSI Software Target MMC-ben. A művelet egyszerű, a szokásos módon varázsló vezet bennünket végig a folyamaton. Először meg kell adnunk a virtuális diszk elérési útját és nevét. Ebből kivételesen az elérési út a fontosabb, mert ez dönti el, hogy milyen hibatűrésű fizikai diszkre kerül a virtuális diszkfájl, tehát mennyire lesz védve az esetleges diszkhibákról. Hasonlóan fontos végiggondolnunk, hogy az adott fizikai diszken milyen más virtuális diszkeket hoztunk/hozunk létre, hiszen ez döntően befolyásolhatja rendszerünk teljesítményét. A második lépésben meghatározhatjuk a virtuális diszk méretét, a harmadikban pedig hozzáférési jogot adhatunk a kiszolgálók számára. Mivel még nincsenek kapcsolódó kiszolgálóink, egyelőre adjunk jogot a helyi iSCSI-kiszolgálónak!

A következő lépés a Windows Server 2008-as kliensek csatlakoztatása, mert csak ezután tudunk hozzáférést biztosítani számukra a kiajánlott diszkekhez. Fontos tudni, hogy az SCSI-szabványnak megfelelően minden kliensgép csak a számára engedélyezett diszkekhez férhet hozzá, és az így adott jog kizárólagos, tehát amíg az adott gép használja a diszket, addig más eszköz nem. Ez nem áll ellentmondásban a fürtözött használattal, mert abban az esetben majd a fürt virtuális nevéhez rendelünk hozzá diszkeket, és a fürt bármely tagja hozzáférhet a diszkhez, de ebben az esetben is egy időben csak az egyikük!

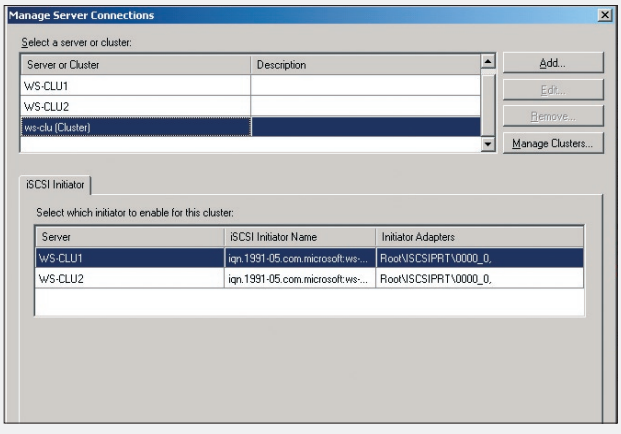
Lépjünk be tehát a Windows Server 2008-kiszolgálókra, telepítsük a Failover Cluster tulajdonságot (ha több hálózati csatolót használunk, akkor a MultiPath I/O-t is!), és állítsuk be az iSCSI-kapcsolatokat! Az iSCSI Initiator első indításakor figyelmeztetést kapunk, hogy a szolgáltatás nem fut (érthető, hiszen a Windows Server 2008-ban alapértelmezés szerint minden, ami nem feltétlenül szükséges, kikapcsolt állapotban van). Engedélyezzük a szolgáltatás elindítását, és jegyezzük meg, hogy ezzel egyúttal a megfelelő tűzfalszabályok is bekapcsolódtak, tehát az iSCS-kliensünk már elméletben képes kommunikálni az adattárolóval.

Az elméletet váltsuk gyakorlatra a kliens beállításával. Az erre szolgáló ablakon csak hat fülecskét látunk, de a különböző gombok alatt azért számos állítási lehetőség rejtőzik. Az alapbeállítások viszont egyszerűek: a Discovery fülön vegyük fel adattárolónkat a targetek listájára (használhatjuk a host nevét, a DNS nevét, vagy az IP-címét)! A Targets fülre átlépve a Refresh gomb hatására meg kell jelennie az adott hoston elérhető iSCSI-targetek listájának (a mi esetünkben az IQN neve jelenik meg). Az alapértelmezett állapot Disconnected, a Log on... gombra kattintva állíthatjuk be a kapcsolat paramétereit: az automatikus újracsatlakozást és a MultiPath engedélyezését, majd az Advanced gombra kattintva a CHAP-jelszót és az IPSec tulajdonságait. Itt dönthetünk arról is, hogy az egész autentikációt inkább egy RADIUS kiszolgálóra bízzuk, ebben az esetben fel kell vennünk gépeinket a RADIUS kiszolgálón is kliensként. Ha mindent jól csináltunk, akkor a Targets fülre visszatérve az adattárolónk már Connected állapotban lesz, ez pedig elegendő, hogy jogosultságot adjunk nekik az adattárolón.

A Storage Serveeen nyissuk meg a Storage Manager for SANs MMC-t, és válasszuk a Manage Server Connections opciót. Válasszuk a Manage Clusters gombot és adjuk meg a csatlakoztatandó fürt nevét (ezt már itt el kell döntenünk, és később majd ezzel a névvel kell létrehoznunk a tényleges fürtöt). A csatlakoztatott kiszolgálók listáján jelöljük be azokat a kiszolgálókat, amelyek a fürt tagjaiként fognak működni, ezzel adhatunk



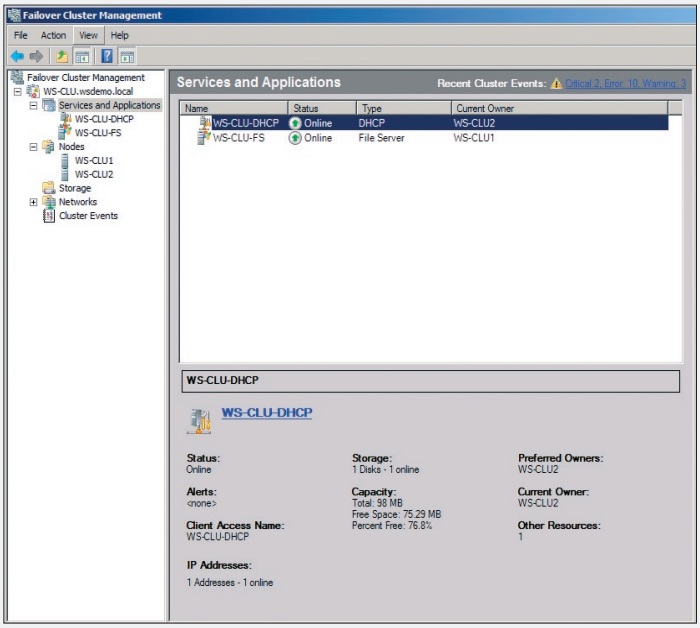
3. ábra. Az iSCSI Initiator beállítási folyamata



4. ábra. A fürt hozzáférésének engedélyezése az iSCSI Targeten

majd hozzáférést a korábban létrehozott virtuális diszkekhez.

A következő lépésben rendeljük hozzá a fürt virtuális nevét a kívánt diszkekhez, amelyek – mint offline és formázatlan lemezek – így hozzárendelődnek a megfelelő kiszolgálókhoz. A kiszolgálókhoz visszatérve az iSCSI Initiatorban ellenőrizzük, hogy az adattárolónk csatlakoztatott állapotban van-e, majd a Volumes and Devices fülre kattintva vegyük fel a köteteket! Ennek legegyszerűbb módja az Autoconfigure gomb használata. Ezt követően az egyik gépen online állapotra kell hoznunk a diszkeket, majd inicializálni és formázni kell őket. Amikor ezzel elkészültünk, akkor a megosztott diszkjeink már rendelkezésre állnak, tehát kezdhetjük a fürt telepítését. A Windows Server 2008 esetén ez a művelet már rendkívül egyszerű, hagyatkozunk bátran a varázslókra. Ajánlom mindenkinek a Cluster Validation riport használatát, mert ha itt nem látunk hibákat, akkor a fürt létrehozása biztosan sikeres lesz. A fürtözés újdonságairól bővebben olvashatnak *Lepenye Tamás* vonatkozó cikkében.



5. ábra. Az iSCSI-adattárolóra épített fürt, működés közben

Ha mindent ügyesen csináltunk, akkor a kiszolgálók telepítése után egy órán belül már figyelhetjük fürtözött kiszolgálóink működését.

Somogyi Csaba
(Csaba.Somogyi@microsoft.com)
Microsoft Magyarország

Hogyan tovább?

A témához rendkívül sok olvasnivalót találhatunk az interneten, csak ízelítőül néhány hivatkozás, ahol a legalapvetőbb információkat találhatjuk meg.

Az iSCSI összefoglalása, sok külső hivatkozással: *http://en.wikipedia.org/wiki/ISCSI*

Az OSI-ISO modell összefoglalása: *http://en.wikipedia.org/wiki/OSI_model*

A SAN összefoglalása: *http://en.wikipedia.org/wiki/Storage_area_network*

A Microsoft iSCSI Initiator letöltési oldala: *http://www.microsoft.com/downloads/details.aspx?familyid=12CB3C1A-15D6-4585-B385-BEFD1319F825&displaylang=en*

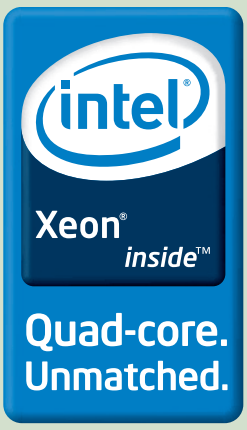
Részletes, konkrét iSCSI-alkalmazási forgatókönyveket is leíró dokumentum a Microsoft oldalán: *http://www.microsoft.com/windowsserver2003/technologies/storage/iscsi/deployiscsi.mspx*

David Woodsmall részletes SCSI-gyűjteménye: *http://home.nc.rr.com/woodsmall/SCSI.htm*

A Fujitsu Siemens Computers áttörő IT infrastruktúra-megoldásai éppoly rugalmasan alkalmazkodnak a váratlan helyzetekhez, mint Ön.

A Fujitsu Siemens Computers FlexFrame™ Infrastructure rendszere tökéletesen illeszkedik az adatközponti környezetekbe. Az egyes szoftverfejlesztők által támogatott rugalmas IT-platform dinamikusan rendeli hozzá a szervererőforrásokat az egyes alkalmazásokhoz. A nagy teljesítményű, **négymagos Intel® Xeon® processzorral ellátott PRIMERGY RX300** szerverekre épülő megoldás minden speciális igényt kielégít az alkalmazások támogatása terén. Hiba esetén az érintett alkalmazások dinamikus áthelyezésével tartja fenn a zavartalan működést. Miért is jó ez Önnek? Mert a kivételes rugalmasságnak köszönhetően végre minden energiájával az üzleti működésre koncentrálhat. És ez csak egy a Fujitsu Siemens Computers Dinamikus Adatközponthoz készült innovatív megoldásai közül!

www.fujitsu-siemens.hu

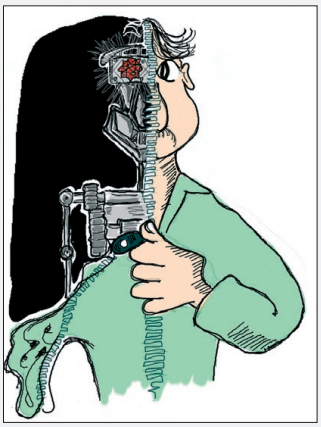


A PARANCSSOR MEGLÓDUL

Múltad a sötét
Ablaküvegen sejlik
Mintha… de mégsem.

Képzeljük el, hogy egy ismeretlen szigeten találjuk magunkat. Éjszaka. Zseblámpa nélkül. Elsőre tuti szerencsétlenkedünk egy csomót, aztán kezdjük apránként megtalálni a járatokat. Valószínűleg nem azokat az ösvényeket fogjuk használni, amelyeket nappal is használnánk – de elboldogulunk ezekkel is. Út szerencsére sok van.

Nagyjából ezt fogja érezni az a rendszergazda is, akit odaültetnek egy Windows 2008 Server Core elé. Command prompt. Semmi más. Ha véletlenül becsukja, akkor hiába kaparászik a Start Menu után – az sincs. Ijedten nyom egy Ctrl-Alt-Del kombinációt – és felcsillan a remény. Egy pici grafikus felület. Jelszóváltoztatás. Task Manager! Huh. Indítsuk el gyorsan a teljes grafikus felületet: explorer.exe. Nincs.



Tényleg csak a command prompt maradt.

Az első sokk után jönnek az emlékek. A netsh… amely csak kávét nem főz. Van? Van. Hurrá! Ki tudunk törni a gépről. De ha a kitörés megy, akkor valószínűleg a bejutás is. Távoli hozzáférések vajon vannak-e? Ez már nem megy saját kútfőből, irány a net. Olvasgatni fogunk.

Sokkal magabiztosabban sétálunk vissza a géphez. Netene, csiba! Ismerlek immár, tudom a titkodat.

Hagyjuk most már magára elképzelt rendszergazdánkat, aki egyre vehemensebben fogja magát belevetni a parancssori élet rejtelmeibe. Boldogulni fog. A feladat csak elsőre ijesztő. Ahogy a szólás mondja: az olvasottság időnként csodákra képes.

Vizsgáljuk meg inkább a koncepciót.

Miért is jó, hogy kidobjuk az operációs rendszerből a grafikus felületet? (Amellyel persze repül egy csomó más is, hiszen izgalmas függőségek léteznek ám egy operációs rendszerben.) Javaslom, inkább fordítsuk meg a kérdést: vajon mi szükség van egy szervertermékben grafikus felületre? Oké, hogy legyenek benne nagy zöld gombok. Egyéb? Hogy lehessen róla netezni? Hamis. Hogy lehessen szerveralkalmazásokat futtatni, menedzselni? Nos, igen. Ekkor tényleg kell. De csak azért, hogy egy vagy több szerverfunkciót – DNS-szerver, DHCP-szerver, tartományvezérlő, fájlszerver – futtassunk rajta, valójában nincs szükségünk grafikus felületre. Igen, tény, hogy kényelmesebb kattogtatni. De mekkora árat fizetünk érte?

- Grafikus felület nélkül sokkal egyszerűbb hardver is elegendő a feladatra. Előszedhetjük a spájzból a régi vasakat (erősebb PII, közepes PIII), immár nem kell ezeket bagóért elsóznunk más operációs rendszert futtató barátainknak. 512 MB RAM és 5-6 GB merevlemez elég a teljes funkcionalitású Server Core futtatásához. Méghozzá Windows 2008-tudással!
- Pont olyan részek hiányoznak az operációs rendszerből, amelyek kedvenc betörési célpontoknak számítanak. Márpedig ha nincs az a komponens, nincs rajta keresztüli sebezhetőség sem.
- Ha nincs komponens, nem kell foltozni sem. Kevesebb patch, kevesebb fejre állás. Kevesebb restart.
- Ha kevesebb komponens fut a szerveren, értelemszerűen jóval kisebb a szoftverhiba lehetősége is. A megbízhatóság az egekbe szökik.
- Végül van egy olyan fogalom, hogy granularitás. Network-szinten ez azt jelenti, hogy külön vason üzemeltetjük mondjuk a tartományvezérlőt, másikon a DHCP-szervert és így tovább. Ez eddig, teljes értékű szerverrel, horrorisztikus erőforrás-pazarlás volt.

Jelzem, hogy éppen csak karcoltuk a felszínt ebben az írásban. A konkrét megvalósítás, a kezelhetőség, a kerülőutak mind-mind érdekes témák, különösen az öreg motoros adminoknak.

Eme rövid írás a Windows Server 2008 képességeit bemutató karikatúra-sorozatunkból származik, ahol tömören, lehetőség szerint emlékezetesen mutatjuk meg, miért is forradalmi az új szerver-operációsrendszer. A karikatúrák a www.microsoft.hu/technet/rss.aspx?kampany=karikatura linken érhetőek el, RSS-ben.

Petrényi József
(petrenyi.jozsef@sao.hu)
SAO-Synergon, MCSE+M, MCITP, MVP

A GAL és a Free/Busy

Hajlamosak vagyunk megfeledkezni róluk, hiszen csak úgy működnek, nem zavarnak sok vizet. Pedig… Ha jobban beleássuk magunkat, akkor hamarosan elcsodálkozunk azon, hogy egyáltalán működnek. Az Exchange-fejlesztők is érezték, mennyire sebezhető ez a két rendszer, ezért az Exchange 2007-ben drasztikusan átalakították. Mindkettőt.

Nem, nem arról van szó, hogy úgy vártam volna az Exchange 2007-et már a gyár kapujában, hogy a teherautósofőr vattakabátját rángattam, mi hír van a GAL-ról és a Free/Busy-ről. Őszintén szólva, mindketten nagyon sokáig elkerülték a figyelmemet. Biztosan működnek, vontam meg a vállam.

Egy szerencsétlen projektnek kellett beütnie, hogy kiderüljön, mekkora kavarás is történt ezen a két területen.

Kezdjük az elején: mi is egyáltalán a GAL és a Free/Busy?

Lerántjuk a leplet a GAL-ról

A GAL a Global Address List rövidítése. Ez gyakorlatilag egy címlista. Figyelem! Címlista – nem terjesztési lista. Az előbbi egy LDAP-lekérdezés eredménye, az utóbbi pedig egy AD-csoport jellegű objektum. (Csakhogy sikerüljön kellően összezavarnom mindenkit, létezik olyan, hogy dinamikus terjesztési lista, amikor is a csoport tagsága LDAP-lekérdezés alapján áll össze, dinamikusan.)

Mint tudjuk, címlistából annyi lehet, mint égen a csillag. Pontosabban annyi, amennyit a hálózatunk elbír. Tetszőleges számú LDAP-lekérdezést gyárthatunk, adunk nekik neveket, és már készen is vagyunk. Jogos lehet a kérdés, mi különbözteti akkor meg a globális címlistát (GAL) az egyszerű címlistától? Ha most rosszindulatú lennék, akkor azt mondanám, az, hogy a címlistában egyből megjelennek a változások, a globális címlistában meg nem. Ez sajnos sokszor így van, de azért meglehetősen negatív a megközelítés.

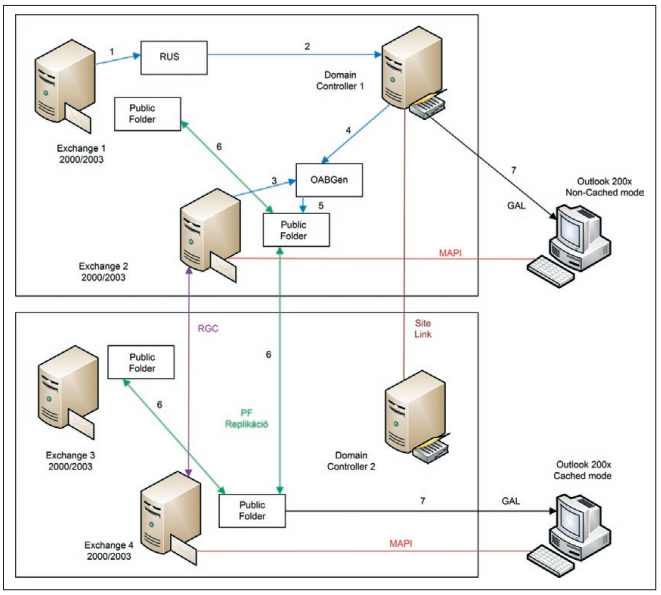
Igyekszem megmagyarázni, de ahhoz mélyebbre kell merülnünk.

Addig oké, hogy LDAP-lekérdezések, de milyen adatbázison? Nyilván Active Directory… de melyik partíció? Elsőre a Domain lenne a megfelelő, de ne feledjük, az Exchange-organizáció erdőszintű, tehát az összes doménpartícióra rá kellene futtatni a lekérdezést. Zűrös. Hol is vannak ezek az adatok egyszerre jelen? Hát a globális katalógusban. Csökkentsük a terhelést, fusson a query csak a GC-n. Csökkentettünk, de azért annyira nem. Faragjunk tovább. Ne egy lépésben történjen a lekérdezés. Legyen egy aszinkron szolgáltatás, amelyik időnként ráfuttatja a lekérdezést a címtárra, majd minden felhasználónál bejegyzi a showInAddressBook tulajdonságba mindazoknak a címlistáknak a DN-jét, amelyeknek a felhasználó is tagja. Természetesen ez egy olyan tulajdonság, mely belekerül a globális katalógus leszűkített adatbázisába is – így a címlista konkrét lekérdezésekor nem kell azt a bonyolult lekérdezést ráküldeni minden alkalommal a GC-re, elég csak a showInAddressList tulajdonságot vizsgálni. Gyorsítottunk? Bizony. Cserébe veszítettünk egy kicsit az aktualitáson, de ez már csak hangolás kérdése. A gond az, hogy még mindig eléggé igénybe venné a globális katalógust az állandó címlista lekérdezése. Vizsgáljuk meg, melyik címlistát kérik le legsűrűbben a kliensek? Hát a globálisat. Akkor vegyük ki ennek a címlistának a legyűjtését ebből a körből, a maradék címlistákat már el tudja látni a GC.

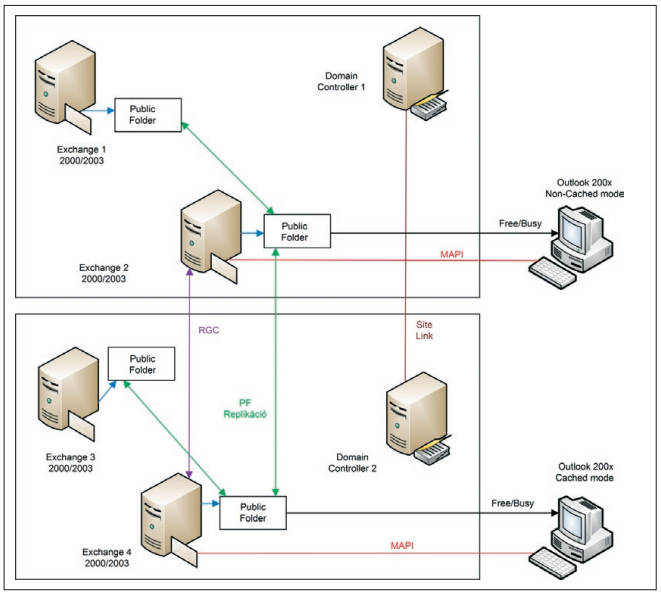
A különböző disztributálási módszerek miatt létezhet az, hogy a változás például az All Address List címlistában már megjelenik, de a Global Address Listben még nem. Legalábbis nem mindenkinél.

Gonosz voltam, mi? Már éppen kezdett érthető lenni a magyarázat, erre megint megcsavartam.

Nos, a helyzet az, hogy nem mindegy, milyen klienssel próbálkozunk, és az a kliens



1. ábra. A GAL terjesztése Exchange 2000/2003 organizációkban



2. ábra. A Free/Busy információk terjesztése Exchange 2000/2003 organizációkban

milyen állapotba van kapcsolva. A kulcs az, hogy ismeri-e a cached módot vagy sem? Amennyiben nem, akkor a GAL terjesztése ugyanúgy történik, mint a többi címlistáé, azaz mindenki a globális katalógust piszkálja a lekérdezésekkel. De ha ismeri... nos, akkor alapvetően változik meg a helyzet.

Vizsgáljuk meg az *1. ábrát*. Látható, hogy a non cached módban üzemelő kliens közvetlenül a GC funkcióval ellátott tartományvezérlőről szedi le a legaktuálisabb globális címlistát.

Az alsó telephelyen viszont már cached módba kapcsoltuk a klienseinket. Most nem térek ki rá, miért jó ez nekünk – a lényeg, hogy megéri, még ha most éppen nem is az lesz a végeredmény.

Az ábra szerint ekkor a kliens – a betárcsázós kliensekhez hasonlóan – a Public Folders system foldereiből olvassa ki a... nem a GAL-t, hanem az OAB-ot. Az OAB (Offline Address Book) tulajdonképpen egy pillanatfelvétel a globális katalógusról, miközben az jobbról előz, és 32 foggal vigyorog. Nézzük részletesebben!

1. Az Exchange szerver aktivizálja azt a bizonyos aszinkron folyamatot. Igen, valóban, a Recipient Update Service-ről van szó, a jó öreg RUS-ról. Ez adja az új felhasználóknak megadott minta alapján az e-mail-címeket, és ez vezeti át a felhasználók adatlapjára, hogy mely címlistáknak is a tagjai.

2. A RUS teszi a dolgát, a változásokat beleírja a hozzá legközelebb eső tartományvezérlő doménpartíciójában lévő adatbázisba, ahonnan azok átvezetődnek a globális katalógusba is.

3. Az Exchange-szerver naponta egyszer belerúg az OABGen eljárásba.

4. Ez az eljárás naponta egyszer lefényképezi a globális katalógust. A fényképet elnevezi OAB-nak.

5. Az OAB-ot belecsomagolja a megfelelő Public Folderbe. (Szerverektől függően más az OAB verziója is, ezek különböző könyvtárakba kerülnek.)

6. Az egyes OAB-folderek Public Folder-replikációval terjednek szét az egész organizációban.

7. Végül a kliens kiolvassa a postafiókjához legközelebb eső Public Folderből az OAB-ot. Ha a postafiókját tartalmazó Exchange-szerveren nincs rajta, akkor a Public Folder Referral alapján elmászik más szerverekre érte.

Vagyis az All Address List _mindig_ friss – már amennyire a RUS az. A Global Address List... hát, az cached módban nem annyira. Mekkora eltérések lehetnek? Borzasztóan nagyok. Nem is csoda, az Exchange összes lusta disznóját bevonták a folyamatba.

Kezdjük a RUS-szal. Mikor aktivizálódik? A jó ég tudja. Kapunk valami hibaüzenetet, ha nem futott le? Persze. Majd. A második szereplő az OABGen. Róla legalább tudjuk, hogy naponta egyszer fut le, alapértelmezésben hajnali ötkor. Jön az újabb rém, a Public Folder-replikáció. Mikor fut le? Amikor kedve van. Maximum annyit állíthatunk – folderenként –, hogy sürgős vagy nem sürgős a replikáció. Alapértelmezésben nem az. Végül jön a cached módba kapcsolt kliens. Mikor kéri le az OAB-ot? Elinduláskor, utána pedig ahhoz képest 24 óránként. Ha feltételezzük, hogy a RUS villámgyors (haha) és a PF-replikáció is felszaggatja a betont (muhaha), akkor is simán összejöhet két nap az OABGen és a cached módba kapcsolt kliens összjátékával.

Durva? Az nem kifejezés. Éppen megérett az újításra.

A Free/Busy előtörténete

Már az ókori görögök is meg tudták különböztetni azt az időt, amikor ráértek csevegni az agorán (free) attól az időtől, amikor éppen más elfoglaltság miatt képtelenek voltak meetinget apprúvolni (busy).

Természetesen náluk is csak akkor működött a rendszer, ha már a szervezkedés során rendelkezésükre álltak ezek a Free/Busy információk. Nagyjából abban az időben ténykedett az Exchange 4.0–5.5 generáció, az például Free/Busy-konnektorokkal oldotta meg a feladatot.

Az Exchange 2000/2003 már annyival volt fejlettebb ennél, hogy – az OAB-hoz hasonlóan – a Public Folderekbe csomagolta a Free/Busy-információkat. Itt speciel nincs különbség cached/non cached mód között, mindenki a nyilvános mappákból eszik.

Látható – kék nyilak a *2. ábrán* –, hogy

amint valaki módosít az Exchange Server Information Store adatbázisában lévő adatain, az egyből beleíródik a Public Folderbe is, ahol a PF-replikáció repíti szét az információt organizációszerte.

Tulajdonképpen ezzel nem is voltak nagy gondok, rendesen működött – eltekintve attól az apróságtól, hogy a kliensek 45 percenként kaptak friss adatokat. Az egyetlen komoly problémát az okozta, hogy a Public Folder halálra ítéltetett, tehát gondoskodni kellett a Free/Busy-információk számára valamilyen más terjesztési módszerről.

Az Exchange Server 2007 színre lép

Nem is akárhogyan. Mondhatni, berúgva az ajtót. Amikor kihajította a RUS-t az ablakon, akkor a pultnál iszogató adminok elismerően bólogattak. Amikor átlyukasztotta a Public Folderek fülét, akkor már kezdte felütni fejét a nyugtalanság. A pánik akkor tört ki, amikor egy sorozattal kinyírta az egyik sarokban kártyázó összes LDAP-lekérdezést.

Hát... akkor most... mi lesz?

A válasz az, hogy OPATH. Egyik lekérdezés helyett a másik. Rossz hír a lengyel logika kedvelőinek, hogy ez a filter már normális. Hasonlítsuk csak össze:

```
LDAP Query: (&(objectCategory=user)
(displayname=IT*))
OPATH: ( ( ObjectCategory -like 'user' ) -and
( DisplayName -like 'IT*' ) )
```

Mindkét lekérdezés legyűjti az összes felhasználót, akinek displayneve úgy kezdődik, hogy IT.

Elsőre nem rossz az új filter, szerintem sokkal olvashatóbb. Külön öröm, hogy el van látva bőségesen operátorral, teljesen C# jellegű a kicsike. Csakhogy. Amíg az LDAP Query közvetlenül tudott hivatkozni a címtárobjektumokra, ez az OPATH-ból hiányzik. Számomra felfoghatatlan okból közéékelődött egy metanyelv. Például nem mondhatom azt, hogy 'PhysicalDeliveryOfficeName', az van helyette, hogy 'Office'. Nem írhatom azt, hogy 'mail', azt kell írnom, hogy 'WindowsEmailAddress'. Miért? Nem tudom.

Nos, mitől is lesz ez itt véresen aktuális? Ugye, azzal kezdtük, hogy a címlisták, beleértve a GAL-t is, egy-egy LDAP-queryből állnak. Azaz még bele sem telepítettük az első

```
16:52:47 Central Europe Standard Time Central Europe Daylight
Time; 07/15/1601 00:36:49 Central Europe Standard Time Central
Europe Daylight Time;
        1> msExchMinAdminVersion: -2147453113;
        1> msExchQueryFilter: (Alias -ne $null -and
((((ObjectClass -eq 'user' -or ObjectClass -eq 'contact') -or
ObjectClass -eq 'msExchSystemMailbox') -or ObjectClass -eq
'msExchDynamicDistributionList') -or ObjectClass -eq 'group') -or
ObjectClass -eq 'publicFolder'));
        1> msExchLastAppliedRecipientFilter: (Alias -ne $null
-and ((((ObjectClass -eq 'user' -or ObjectClass -eq 'contact') -or
ObjectClass -eq 'msExchSystemMailbox') -or ObjectClass -eq
'msExchDynamicDistributionList') -or ObjectClass -eq 'group') -or
ObjectClass -eq 'publicFolder'));
        1> msExchRecipientFilterFlags: 3;
        1> msExchVersion: 4535486012416;
        1> msExchQueryFilterMetadata:
Microsoft.Exchange12.8f91d340bc0c47e4b4058a479602f94c:Rec
ipientFilterType=1;
        6> msExchPurportedSearchUI:
Microsoft.PropertyWell_QueryString={&(mailNickname=*)(|(objectClass=user)(objectClass=contact)(objectClass=msExchSystemMailbox)(objectClass=msExchDynamicDistributionList)(objectClass=group)(objectClass=publicFolder))};
Microsoft.PropertyWell_Items=0; DsQuery_EnableFilter=0;
DsQuery_ViewMode=4868;
CommonQuery_Form=E33FEE83D957D011B93200A024AB2DBB;
CommonQuery_Handler=5EE6238AC231D011891C00A024AB2D
BB;
```

3. ábra. A GAL objektumai

Exchange 2007 szerverünket az organizációba, már meg is állt a telepítés: konvertálj ember, ha jót akarsz!

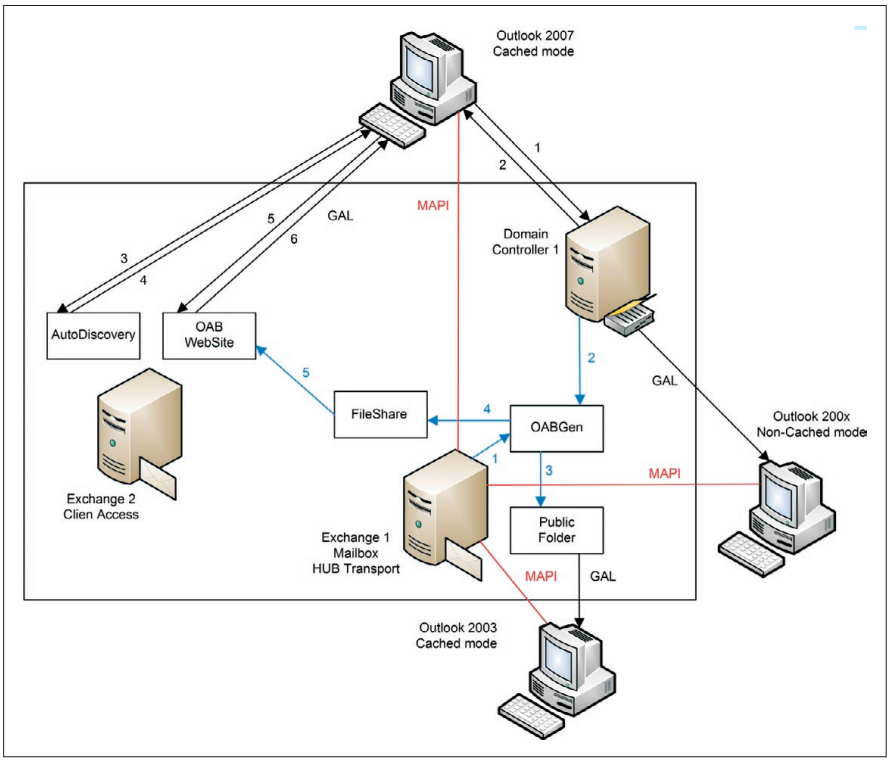
Természetesen lehet manuálisan is. Időmilliomosoknak és mazochistáknak. A legtöbb szokványos címlistához némi internetes keresgéléssel már megtalálhatjuk az OPATH szűrőfeltételt – köztük a GAL-hoz is. Lesznek olyan szűrőlisták, amelyeket konvertálás helyett egyszerűbb lesz összekattogtatni az Exchange 2007 varázslójával (*5. ábra*). Egyedül a régi egyedi címlistákkal leszünk bajban, ott nem ússzuk meg a kézimunkát. Szerencsére itt is van könnyítés, *Bill Long* írt egy remek Powershell-szkriptet, amely a legtöbb LDAP-filtert képes OPATH-filterré konvertálni. (Google: „Bill Long" OPATH convert.)

Ja, természetesen ahol nem működik a varázsló, oda a megfelelő cmdlet kell az Exchange Management Shellben, jelen esetben: set-addresslist, és a -recipientfilter paraméterbe kell belegyömöszölni a filtert.

Tulajdonképpen készen is vagyunk. Pusztán csak figyelmeztetésképpen mondom, hogy ha a set-globaladdresslist paranccsal egyszer sikeresen módosítottuk a GAL-t, akkor akár el is felejthetjük: a Powershell többször nem engedi. Jobb észnél lenni. Vagy gondolkodni. Hol is tárolódnak ezek a lekérdezések? A címtárban. Nézzük meg LDP-vel, mi mindene is van egy GAL-objektumnak?

Láthatjuk, hogy ott virít az msExchangeQueryFilter tulajdonságban az OPATH-filter, ugyanaz valamiért ott van az msExchLastAppliedRecipientFilter tulajdonságban is – és ott figyel az msExchPurportedSearchUI tulajdonságban a régi LDAP-filter is.

Nyilván ADSIEdit-tel az első tulajdonság módosítható. (De hogy ez mennyire lesz összhangban a másik két tulajdonsággal, nem tudom. Élesben nem teszteltem.)



4. ábra. A globális címlista terjesztése Exchange 2007 organizációban

Nos, akkor megvan az új GAL-filter, él a 2007-es organizációban a globális címlista.

A GAL terjesztése az Exchange 2007 organizációban

Már csak el kellene juttatni a kliensekhez, de úgy, hogy ugye nincs RUS, és lehetőleg ne legyenek érintve a Public Folderek sem. Akkor mi az, amink van? Web. XML. És van egy szerepkör, amely ezekben nagyon profi: a Client Access Server, a CAS. Ez az a szerepkör, amelyet sokan úgy azonosítanak, hogy „ja, az owa", majd legyintve kilökik a DMZ-be. Hát nem. Mint az alábbi példákon is látható lesz, a CAS igen rendesen részt vesz az organizáció hétköznapjaiban. (Mindamellett persze tényleg azonos az OWA-val is.)

Száz szónál is szebben beszél egy ábra, inkább nézegessük azt *(4. ábra)*.

Itt alapvetően két folyamot szeretnék részletesen bemutatni. Az első arról szól, hogyan készül el, és hogyan jut el a terjesztési pontra az OAB.

1. Az Exchange-szerver belerúg az OABGen folyamatba. Alapvetően naponta egyszer, de ez átállítható folyamatosra is.

2. Az OABGen lefényképezi a globális címlistát, és legyártja az OAB-verziókat.

3. Az OAB-példányokat kirakja a Public Folderekbe, a régi kliensek számára.

4. Az OAB-adatokból az OABGen legyárt egy XML fájlt is, és ezt kiteszi egy fájlmegosztásba.

5. A CAS szerveren futó OAB website időnként ránéz erre a megosztásra, és felkapja a kirakott fájlt.

Tessék észrevenni, hogy a folyamat itt már nem a RUS-szal indul. Mint írtam, aszinkron RUS immár nincs. Ehelyett rögtön akkor, amikor egy felhasználó adataiban változás történik, és rányomunk az OK gombra – vagy Exchange Management Shell esetén rátenyerelünk az Enter billentyűre –, rögtön kiértékelődnek az organizáció címlistáiban lévő OPATH-filterek, az eredményként kapott címlisták DN-értékei pedig beíródnak a felhasználó showInAddressBook tulajdonságába. (Megjegyzem, ilyen tulajdonsága nemcsak a felhasználónak lehet, hanem mindenkinek, aki e-mail-címet kaphat egy AD-erdőben, azaz tagja lehet a címlistáknak. Részletesebben lásd az 5. ábrát.)

```
Machine: earth | Scope: milkyway.universe
[PS] C:\Documents and Settings\Administrator>get-clientaccessserver | fl


Name                          : EARTH
OutlookAnywhereEnabled        : True
AutoDiscoverServiceCN         : earth
AutoDiscoverServiceClassName  : ms-Exchange-AutoDiscover-Service
AutoDiscoverServiceInternalUri : https://earth.milkyway.universe/Autodiscover/Autodiscover.xml
AutoDiscoverServiceGuid       : 77378f46-2c66-4aa9-a6a6-3e7a48b19596
AutoDiscoverSiteScope         : {Default-First-Site-Name}
IsValid                       : True
OriginatingServer             : earth.milkyway.universe
ExchangeVersion               : 0.1 (8.0.535.0)
DistinguishedName             : CN=EARTH,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=HumanRace,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=milkyway,DC=universe
Identity                      : EARTH
Guid                          : 4bba94ce-99a8-45b9-b1f1-3167074f8aa7
ObjectCategory                : milkyway.universe/Configuration/Schema/ms-Exch-Exchange-Server
ObjectClass                   : {top, server, msExchExchangeServer}
WhenChanged                   : 2007. 12. 16. 13:49:08
WhenCreated                   : 2007. 02. 21. 14:58:54
```

6. ábra. Az Autodiscovery szolgáltatás paraméterei

```
[PS] C:\Documents and Settings\Administrator>get-oabvirtualdirectory | fl


Name                          : OAB (Default Web Site)
PollInterval                  : 480
OfflineAddressBooks           : {Default Offline Address Book}
RequireSSL                    : False
MetabasePath                  : IIS://earth.milkyway.universe/W3SVC/1/ROOT/OAB
Path                          : D:\Program Files\Exchange Server\ClientAccess\OAB
Server                        : EARTH
InternalUrl                   : http://earth.milkyway.universe/OAB
InternalAuthenticationMethods : {WindowsIntegrated}
ExternalUrl                   :
ExternalAuthenticationMethods : {WindowsIntegrated}
AdminDisplayName              :
ExchangeVersion               : 0.1 (8.0.535.0)
DistinguishedName             : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=EARTH,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=HumanRace,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=milkyway,DC=universe
Identity                      : EARTH\OAB (Default Web Site)
Guid                          : c0747f37-dc6e-4c23-96ac-263a79409aa5
ObjectCategory                : milkyway.universe/Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                   : {top, msExchVirtualDirectory, msExchOABVirtualDirectory}
WhenChanged                   : 2007. 02. 21. 15:18:04
WhenCreated                   : 2007. 02. 21. 15:18:04
OriginatingServer             : earth.milkyway.universe
IsValid                       : True
```

7. ábra. Az OAB-website paraméterei

Eljutottunk odáig, hogy az OAB-információk kint vannak a CAS OAB website-ján. De hogyan fognak odatalálni a kliensek?

Ekkor lép be a képbe az Autodiscovery szolgáltatás. Nagyon fontos elem, megérdemli, hogy egy kicsit hosszabban is foglalkozzunk vele.

Amikor Exchange 2007-telepítés előtt preparáljuk a címtárat, létrejön egy úgynevezett Service Connection Point, azaz SCP. Ide van bejegyezve, hogy mely gépeken fut Autodiscovery szolgáltatás. Persze a preparáláskor még nem, de a CAS funkció telepítésekor az Autodiscovery értékei már beíródnak.

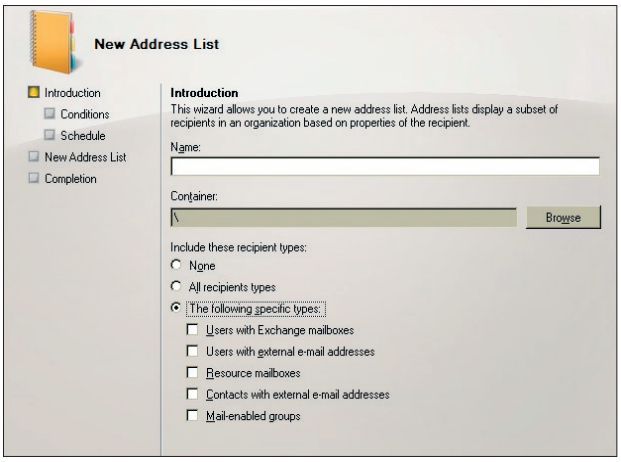
Természetesen ezeket az értékeket módosítani is lehet, nyilván a Shellből *(6. ábra)*.

Tehát amikor egy Outlook 2007-kliens kapcsolódni próbál, akkor azt találja, hogy az Autodiscovery szolgáltatás elérésével kapcsolatos információk – a 6. ábra szerint – a https://earth.milkyway.universe/Autodiscover/Autodiscover.xml fájl letöltésével állnak majd rendelkezésére. (HTTPS ugyan, de az alaptelepítéskor a CAS-szervernek csak self-signed tanúsítványai vannak.)

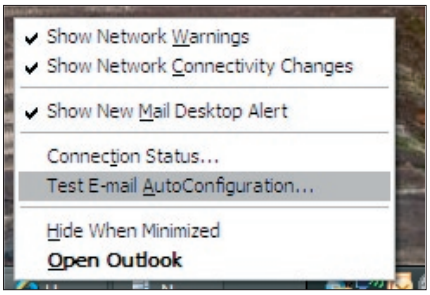
Mit is tud ez az Autodiscovery szolgáltatás? Gyakorlatilag ő a recepciós. Mindenkiről tud mindent, leginkább azt, hogy egyáltalán van-e az illető, és ha igen, akkor hol található. Olyan az Exchange-kliensek számára, mint a Windows-klienseknek a DNS. Hogy egész pontos legyek, a visszaadott XML fájl nagyjából a következő információkat fogja tartalmazni:

- Hol található a csatlakozni szándékozó felhasználó MAPI-profilja (Mailbox Server, login name, autentikációs mód)?
- Hol találhatók az OAB-információk?
- Hol találhatók a Unified Messaging-szolgáltatások?
- Hol fut az Availability webservice (Free/Busy, OOF)?
- Mik az Outlook Anywhere-beállítások?

Csak az első pontról sűrűn teleírt oldalakat lehetne regélni, mennyi könnyebbséget jelent majd ez a rendszergazdáknak... de most kihagyom a ziccert. Koncentráljunk inkább az OAB-elérésre.



5. ábra. Új címlista létrehozásakor választható lehetőségek



8. ábra. Kapcsolódási teszt

Ebben a történetben az Autodiscovery feladata összesen annyi, hogy megmondja a hozzáfordulóknak, merre található az OAB-információkat szolgáltató website.

A *7. ábrán* látható, honnan veszi az Autodiscovery az adatokat. A set-oabvirtualdirectory parancsban lehet az -internalurl/-externalurl paramétereken keresztül befolyásolni, milyen címekről érhető el a CAS-szervereken futó OAB-weboldalunk.

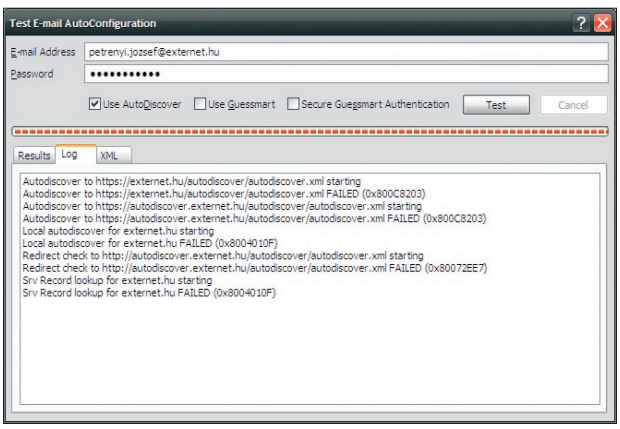
Egy újabb döbbenet. Igen, ez az egész móka működik az internet felől is.

Na de... úgy indult a történet, hogy Active Directory, azon belül SCP-objektum... Az interneten viszont nincs kint a címtárunk. Legalábbis remélem, hogy nincs.

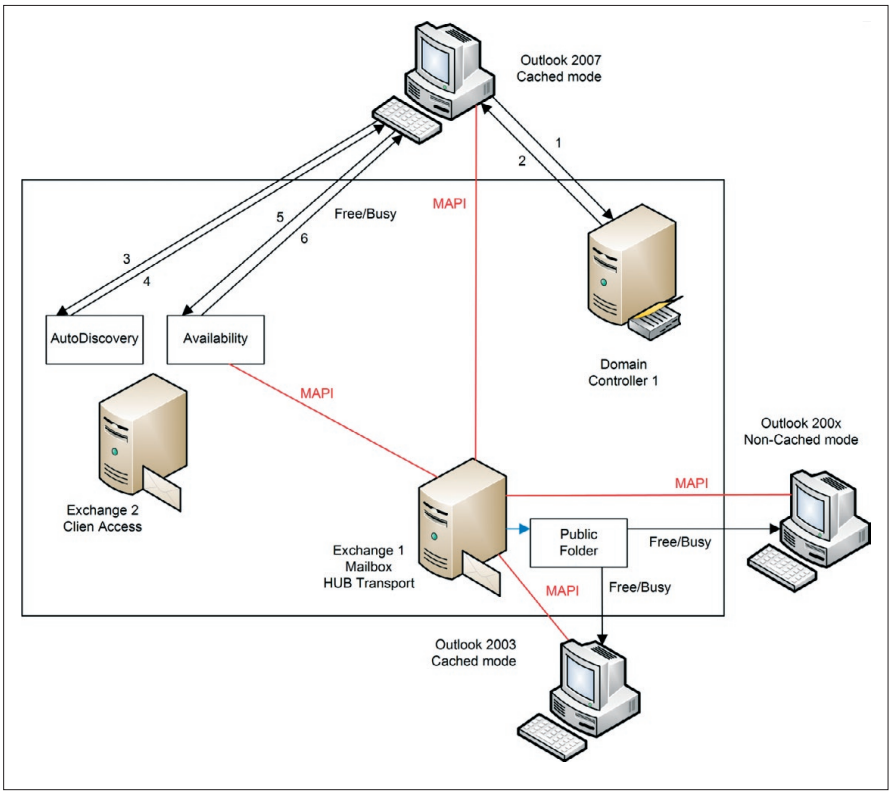
A trükk az, hogy ha az Outlook 2007 nem talál SCP-objektumot, akkor a hasára üt, és bepróbálkozik két címmel. (És ez nemcsak akkor igaz, ha odakint vagyunk, ez történik akkor is, ha például nem tartományi tagként használjuk a gépünket.) Tegyük fel, hogy az e-mail-címem user1.0@cegnev.hu, ekkor a következő címekkel fog kísérletezni *(9. ábra)*:

https://cegnev.hu/Autodiscovery/Autodiscovery.xml

https://autodiscover.cegnev.hu/Autodiscovery/Autodiscovery.xml



9. ábra. Autoconfiguration-teszt



10. ábra. A Free/Busy információk terjesztése Exchange 2007 organizációban

Semmi más dolgunk nincs, mint szerezni egy megfelelő – értsd: valódi, külső – tanúsítványt, majd a fenti címek valamelyikén publikálni a CAS-szerverünk Autodiscovery-weblapját. Természetesen ebben az esetben az egyes szolgáltatásoknál meg kell adni, milyen címeken lesznek elérhetők kívülről. (Lásd a 7. ábrán az -externalurl paramétert.)

Jól elkalandoztunk. Térjünk most vissza a 4. ábrához. Az egyik folyamatot már részleteztük, most akkor vizsgáljuk meg, hogyan is talál el a kliens a weblaphoz:

1. Vagy a címtártól, vagy a DNS-től megkérdezi, hol fut az Autodiscovery szolgáltatás.

2. Megkapja a választ. Vagy a DNS-től, vagy az SCP-objektumtól. (Több CAS-szerver esetén alaphelyzetben véletlenszerű választ ad vissza a DC. De be lehet konfigurálni site-érzékeny válaszra is.)

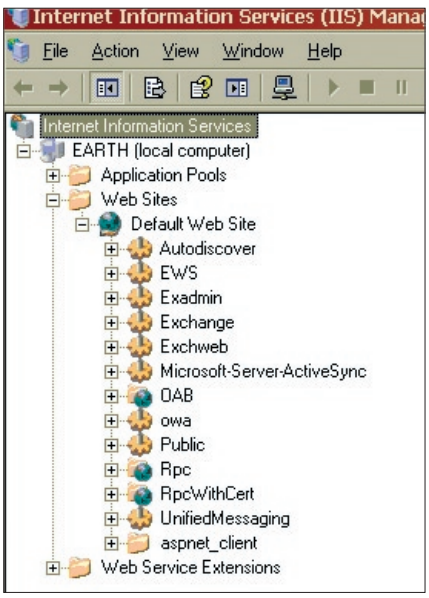
3. Elmegy az Autodiscovery-szolgáltatáshoz, és megkérdezi hol fut az OAB-webszolgáltatás.

4. Az Autodiscovery átküldi neki a részletes választ XML formátumban.

5. A kliens elmegy a megadott címre, elkéri az OAB-adatokat tartalmazó XML fájlt.

6. Az OAB-website odaadja neki.

Ennyi. Nem mondanám, hogy egyszerűbb lett – de minden komponens úgy teker, mint egy versenymalac.

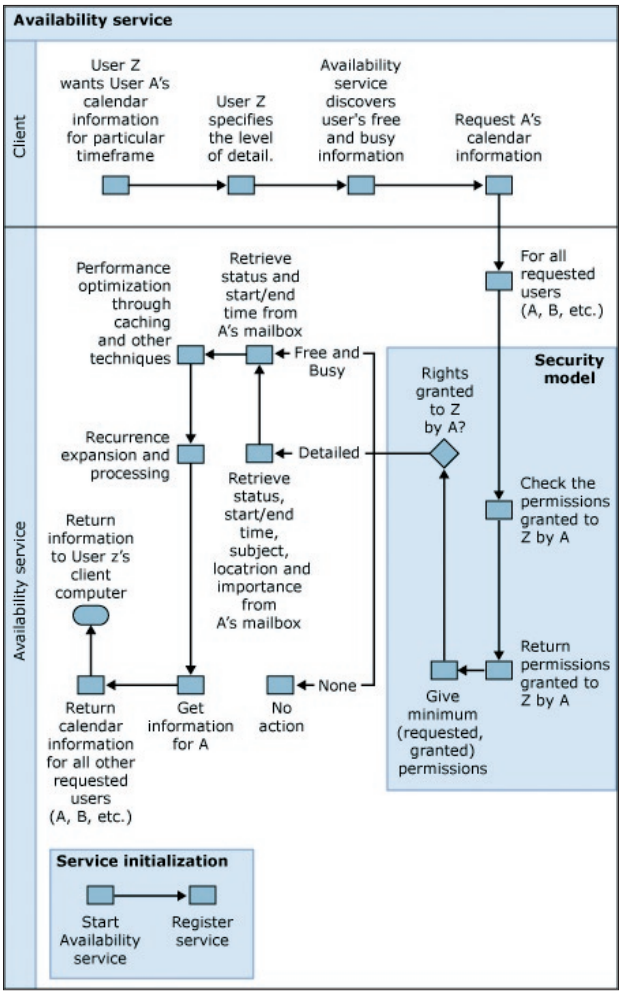


11. ábra. A CAS-szerver webszolgáltatásai

```
Machine: earth | Scope: milkyway.universe
[PS] C:\Documents and Settings\Administrator>get-webservicesvirtualdirectory | fl

Name                            : EWS (Default Web Site)
InternalAuthenticationMethods   : {Ntlm}
ExternalAuthenticationMethods   : {Ntlm}
BasicAuthentication             : False
DigestAuthentication            : False
WindowsAuthentication           : True
MetabasePath                    : IIS://earth.milkyway.universe/W3SVC/1/ROOT/EWS
Path                            : D:\Program Files\Exchange Server\ClientAccess\exchweb\EWS
Server                          : EARTH
InternalUrl                     : https://earth.milkyway.universe/EWS/Exchange.asmx
ExternalUrl                     :
AdminDisplayName                :
ExchangeVersion                 : 0.1 (8.0.535.0)
DistinguishedName               : CN=EWS (Default Web Site),CN=HTTP,CN=Protocols,CN=EARTH,C
                                  N=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPD
                                  LT),CN=Administrative Groups,CN=HumanRace,CN=Microsoft Ex
                                  change,CN=Services,CN=Configuration,DC=milkyway,DC=univer
                                  se
Identity                        : EARTH\EWS (Default Web Site)
Guid                            : 611d1bc3-1e59-43b1-af7b-2413e1d99271
ObjectCategory                  : milkyway.universe/Configuration/Schema/ms-Exch-Web-Servic
                                  es-Virtual-Directory
ObjectClass                     : {top, msExchVirtualDirectory, msExchWebServicesVirtualDir
                                  ectory}
WhenChanged                     : 2007. 02. 21. 15:19:01
WhenCreated                     : 2007. 02. 21. 15:19:01
OriginatingServer               : earth.milkyway.universe
IsValid                         : True
```

12. ábra. Az Availability szolgáltatás konfigurálása



13. ábra. Az Availability szolgáltatás működési vázlata

Ilyenkor a rendszergazda első kérdése: mit tehetek, ha nem működik? Azt már láthattuk, website-oldalon hogyan olvashatjuk ki, illetve módosíthatjuk az értékeket. De mi van akkor, ha valamiért az Outlook mégsem találja a címeket?

A tálcán lévő Outlook ikonra CTRL+jobbklikk akcióval rárepülve a *8. ábrán* látható menüt kapjuk. Itt kiválasztjuk a „Test E-mail AutoConfiguration" menüpontot, a felugró ablakban beírjuk az e-mail-címünket, jelszavunkat, töröljük a GuessSmart opciókat – és tesztelünk egyet.

A 9. ábra be is mutat egy teszteredményt. Remekül látható, hogy az Externet még nem készült fel az Outlook Anywhere-publikálásokra. (Valószínűleg nem Exchange 2007-et használnak.) De látható az is, hogy a kliens mi mindennel próbálkozik, mielőtt feladná.

Amennyiben sikerült volna a csatlakozás, a Results fülön láthatnánk, hogy milyen adatokat kaptunk vissza az XML fájlban. Ezekből rögtön látszik az egyes szolgáltatások elérhetősége – legalábbis az, hogy a kliens mit kap, hol keresse azokat.

A Free/Busy információk terjesztése az Exchange 2007 organizációban

Az eddigiekhez képest a Free/Busy információk terjesztésének elmagyarázása már kellemes lejtmeneti séta lesz. A fontos fogalmakat az előző fejezetben tisztáztuk, itt csak az eltérésekre kell koncentrálnunk.

A részleteket a *10. ábrán* láthatjuk. Vannak ugyan változások, de ránézésre nem túl nagyok: OAB-website helyett például Availability szolgáltatás van. Nosza, vessünk csak egy pillantást a CAS weboldalaira és keressük meg *(11. ábra)!*

Látjuk itt az Availability szolgáltatást? Én igen. De annyira nem magától értetődő. Az Availability szolgáltatás ugyanis nyitott. (Áll egy Availability API-ból és egy erre épülő webservice-ből.) Bárki fejlesztheti saját programot rá. Ebből kifolyólag nem is kapott külön website-ot, hanem az Exchange Web Services (EWS) alatt található meg, services.wsdl néven.

Miután kiismertük, már tudjuk, hogyan kell konfigurálni *(12. ábra).*

Látható, itt is van mind -internalurl, mind -externalurl paraméter – azaz ez is működhet kinti eléréssel is.

Térjünk vissza még a 10. ábrára. Feltételezem, a 4. ábra alapján mindenki számára érthető a működési mechanizmus, legalábbis, ami a kliens hozzáférését illeti. Az adatok begyűjtése viszont némileg más lett: habár kompatibilitási okokból megmaradt a Public Folderbe csomagolás is, de a CAS-szerver, pontosabban az Availability webservice már közvetlenül fordul a Mailbox szerverhez, mégpedig MAPI-n keresztül. A mechanizmust részletesebben a *13. ábrán* tanulmányozhatjuk.

Én legszívesebben nem is tennék hozzá semmit, az ábrán minden gyönyörűen látható.

Mi maradt még a végére? Összefoglalunk. Látható, hogy az új terjesztési módszereknek rengeteg előnyük van: up-to-date információkat szolgáltatnak a klienseknek, méghozzá gyorsan, emellett lehetővé teszik a külső hozzáféréseket is. Ellenben a terjesztési metódus nem lett egyszerűbb, az Exchange-rendszergazdáknak rendesen képbe kell kerülniük, ha nemcsak üzemeltetni akarnak, hanem olykor hibát is elhárítani.

De a legnagyobb hátrányról még nem beszéltem: a fenti metódusok csak akkor működnek, ha szerveroldalon minimum Exchange 2007 van, kliensoldalon pedig minimum Outlook 2007. Minden más esetben a régi terjesztési módszerek maradnak – azaz felkészülhetünk rá, hogy még jó ideig kevert rendszerekkel kell együtt élnünk, ahol mindkét bonyolult rendszer egymás mellett fog működni.

Petrényi József
MCSE+M, MCITP, MVP (petrenyi.jozsef@sao.hu)
SAO-Synergon

Maradjon versenyben!

Windows Server 2008 upgrade tanfolyamok

2008. áprilisától

Windows Server 2008

Kedvező tanfolyami konstrukciók az áttérni vágyó profi szakemberek számára, melyek az új Windows 2008-as minősítésekre is segítenek felkészülni.

Több százezer forint kedvezmény

Startoljon el, regisztráljon most!

SZÁMALK Továbbképzés – Telefon: 203-0304/4122 m.

www.szamalk.hu/tisza/windows2008

SZÁMALK

Az adat soha ne vesszen el!

Dell tárolási és mentési megoldások

DELL - Új generációs szalagos mentési megoldások

A szalagos mentés napjainkban döntő szerepet játszik a tárolási és mentési tervek kidolgozása során; ideális megoldást biztosít tárolási és archiválási folyamatokra. Az LTO-4 technológia bizonyítottan minimális kockázatot, magas szintű megbízhatóságot és rendelkezésre állást biztosít megfizethető áron!

A Dell volt az első a piacon az LTO-4 technológiával; megoldásokat kínál a kis vállalkozások részére, egészen az adattároló központokig. Ez az új meghajtó kategóriájában az első, mely eszköz szintű titkosítást kínál.

Duplázza meg mentési kapacitását és csökkentse az adattárolását a PowerVault™ LTO-4-120 meghajtók és könyvtárak segítségével!

PowerVault™ LTO-4-120 szalagos meghajtó

584.800 Ft

PowerVault™ TL2000 LTO-4 szalagostár

955.000 Ft

PowerVault™ LTO-4-120 szalagos meghajtó

Felülmúlhatatlan teljesítmény és kapacitás

- **Kapacitás:** 800 Gb natív
- **Teljesítmény:** adatátvitel 120 MB/sec
- **Biztonsági jellemzők:** WORM (Wright Once-Read-Many), eszköz szintű titkosítás
- **Interfész:** SAS 3 GB/s, FC 4 GB/s

Az első LTO meghajtó eszköz szintű titkosítással

Az LTO-4 az első szalagos mentési technológia, mely lehetővé teszi az eszköz szintű titkosítást, ezáltal csökkentve az üzleti szempontból kritikus adatokhoz való engedély nélküli hozzáférés kockázatát. A kazetta hordozhatóságának köszönhetően, a központtól távol (off-site) is tárolható. A PowerVault™ LTO-4 megoldások egyaránt védelmet biztosítanak helyszíni (on-site) és egyéb (off-site) adatvesztés ellen.

Iparági standardok

Standardizált LTO technológia biztosítja a kompatibilitást visszamenőleg és a jövőre vonatkozóan is, valamint a szállító semlegességet. Az LTO-4-120 kompatibilis az LTO-3 technológiával (olvassa és írja is az LTO-3 mentéseket), illetve olvasáskompatibilis az LTO-2 mediával.

További információt a (06 1) 270 7614-es telefonszámon, a dell_sales@humansoft.hu e-mail címen vagy a www.humansoft.hu és a www.dell.hu weboldalon kaphat.

IIS7 a Server Core-on és a hosting

A Windows 2008 Server egyik radikális újítása a Server Core konfiguráció, amelynek használatával csak minimális felhasználói felületet kapunk, így igen kicsi erőforrás-felhasználású kiszolgálót építhetünk.

Az IIS7 is üzemeltethető Server Core-on, ennek telepítéséről és konfigurálásáról lesz szó ebben a cikkben. A Server Core az egyik legérdekesebb fejlesztés a Windows-kiszolgálók történelmében, elvégre egy Windows (ablakok) nevű operációs rendszer pont az ablakot dobja le magáról. Nem paradox ez egy kicsit?

Bevezetés

Valójában arról van szó, hogy sokan jelezték a Microsoftnak: Hölgyeim/Uraim, minek nekem Explorer meg Aknakereső, amikor én egy Active Directory-kiszolgálót akarok üzemeltetni? Nem is annyira persze a passzívan diszken levő Pasziánsz zavar minket, hanem azok az állandóan futó szervizek, amelyekre nincs szükség az adott szerepkör futtatásához. És ha már csökkentjük a memóriafelhasználást, minek nekünk GUI, ha jó volt a parancssor 40 éven keresztül a UNIX-okban? Egyesek persze úgy érzik, ez visszafejlődés, ez nem a hippikorszak már, ha egyszer kitalálták a GUI-t, minek nekünk újra parancssor?

Akiknek viszont korlátozottak a hardver-erőforrásaik, és/vagy szeretnek scriptelni, azok örömmel vágnak bele egy új kalandba.

IIS7 telepítése Server Core-ra

De hogyan álljunk neki? Kiindulásként tételezzük fel, hogy van egy frissen telepített Server Core-unk, amire még semmilyen szerepkört nem telepítettünk fel.

Az első (és utána folyamatos) meglepetés az, hogy nincs GUI, így nincs Add/Remove Programs sem a Control Panelen (nincs Control Panel sem, csak egyes appletek működnek). Hogyan kell így telepíteni bármit is? A Package Managerrel, a pkgmgr.exe-vel. A jó öreg checkboxok helyett viszont gépelni kell, de veszettül, hogy összeszedjük a szükséges IIS7-komponenseket.

De előbb engedélyezzük a Remote Administrationt, hogy ne kelljen a gépteremben fagyoskodni:

```
cscript %windir%\system32\SCRegEdit.wsf /ar 0
```

Most már mehet minden távolról, kényelmesen. Leginkább az a jó benne, hogy az interneten olvasott scripteket bemásolhatjuk az RDP-ablakba, nem kell annyit gépelni.

Az alapvető IIS-komponensek telepítése:

```
start /w pkgmgr /iu:IIS-WebServerRole;WAS-
WindowsActivationService;WAS-ProcessModel
```

A start /w[ait] azért kell, mert a pkgmgr.exe azonnal visszatérne, és a háttérben aszinkron módon futna. Mivel azonban semmilyen triviális visszajelzésünk sincs a telepítés állásáról, nem tudnánk, mikor ért véget. A /w miatt a start parancs megvárja, amíg véget ér a pkgmgr processz futása, addig blokkolja a hívót, azaz a Command Promptot.

A /iu az Install Update rövidítése, az adott Windows-komponenst a /uu Uninstall Update kapcsolóval lehetne leszedni.

Milyen csomagokat választhatunk ki? Az oclist.exe segítségével megnézhetjük a Windows Foundation Package tartalmát, hogy ebből mi van és mi nincs telepítve:

```
Installed:IIS-WebServerRole
  |
  |-- Not Installed:IIS-FTPPublishingService
  |       |
  |       |-- Not Installed:IIS-FTPServer
  |       |
  |--     Installed:IIS-WebServer
  |       |
  |       |--     Installed:IIS-ApplicationDevelopment
  |       |       |
  |       |       |-- Not Installed:IIS-ASP
...
```

Szép, konzolon kirajzolt fa, tisztára Norton Commander-nosztalgiám van tőle. ☺

Ebből a listából tehát kinézhetjük, mit lehetne még feltelepíteni.

Tegyük fel, szükségem van még a Windows Authenticationre, az lemaradt az előbb.

```
start /w pkgmgr /iu:IIS-WindowsAuthentication
```

Egy másik gépről böngészővel ránézve már látszania kell a demó-főlapnak. A Core-on

nincs Internet Explorer sem, habár, mondjuk, egy third-party böngésző éppen el tud rajta futni. De ez nem illik egy Server Core-hoz.

Mi érhető el a Core-on?

Miden, ami nem igényel .NET Framework-öt. Így ezek sajnos nem mennek:

- IIS-ASPNET
- IIS-NetFxExtensibility
- IIS-ManagementConsole
- IIS-ManagementService
- IIS-LegacySnapIn
- IIS-FTPManagement
- WAS-NetFxEnvironment
- WAS-ConfigurationAPI

Azaz megy a klasszikus asp, és megy a php vagy más scriptnyelvek futtatása, a korábbi számban ismertetett FastCGI-vel is.

Fájdalom, de az IIS Manager .NET Framework (WinForms) alapú, így az is kiesett. De hát ez egy konzolos oprendszer, ugye nem felejtettük el?

De nem térek ki a logikus kérdés elől. Miért pont az ASP.NET-et hagyta ki a Microsoft az IIS7 Server Core-verziójából? Nos, a .NET Framework ablakmentesítése messze nehezebb, mint azt kívülállóként gondolnánk. A legtöbb ember nem is sejti, milyen bizarr helyeken is ablakok mocorognak a háttérben, például hálózati programozásnál, amikor egy deka ablak sincs a közelben. Nem tudom megmondani, hogy egy szervizcsomaggal jön-e ki az ASP.NET-támogatás majd, vagy csak a következő szerverrel (inkább az utóbbi eset a valószínű), de nyilván ez sokakat érdekelni fog majd. Jelen pillanatban szerintem statikus lapok és php-scriptek futtatására fogják legtöbben használni a Server Core-t.

A távoli adminisztráció sem megy, mert ahhoz a Management Service-nek kellene futnia, amit szintén .NET-ben írtak. Azaz, itt az ideje kicsit közelebbi barátságot kötni az appcmd.exe-vel.

Élet IIS-admin GUI nélkül

Derítsük fel, mit kaptunk az alaptelepítésünkkel – az appcmd.exe felhasználásával.

```
H:\Windows\System32\inetsrv>appcmd list sites
SITE „Default Web Site” (id:1,bindings:http/*:80:,state:Started)
```

Remek, van egy website-unk, a jól ismert Default Web Site, amely minden címen a

1. ábra. Életkép a Server Core-on: IIS-alkalmazások adatai

80-as porton érhető el. Milyen alkalmazás van mögötte?

```
appcmd list app
APP „Default Web Site/” (applicationPool:DefaultAppPool)
```

Nézzünk utána, hogyan van beállítva a DefaultAppPool.

```
appcmd list apppool
APPPOOL „DefaultAppPool” (MgdVersion:,MgdMode:
Integrated,state:Started)
```

No, ez nem túl sok infó, de várjunk csak:

```
appcmd list apppool /text:*
APPPOOL
  APPPOOL.NAME:”DefaultAppPool”
  PipelineMode:”Integrated”
  RuntimeVersion:””
  state:”Started”
  [add]
    name:”DefaultAppPool”
    queueLength:”1000”
    autoStart:”true”
    enable32BitAppOnWin64:”false”
...
    [processModel]
      identityType:”NetworkService”
...
```

Ha már unjuk a fekete ablakot nézni, akkor persze át is lehet irányítani a parancsok kimenetét fájlba (meg persze meg lehet változtatni a konzol háttérszínét is):

```
appcmd list apppool /text:* >apps.txt
```

A kapott szövegfájlt aztán megnézhetjük ... notepaddal. Bizony, a notepad fut Server Core-on. Mi következik ebből? Az, hogy közvetlenül is lehet konfigurálni az IIS7-et, a konfigurációs állományain keresztül. Gyors módosításokat garantáltan könnyebb így végrehajtani, mint szétgépelni magunkat a command-ablakban.

Mondjuk, szeretném átköltöztetni a log-könyvtárat a System partícióról egy másikra, hogy DOS-támadás esetén nehogy megtöltsék a rendszerpartíciót, ezzel leállítva a szervert. Appcmd-vel ez így nézne ki:

```
appcmd set config -section:log
/centralW3CLogFile.directory:c:\temp
```

Nem begépelni nehéz ezt, hanem kitalálni, hogyan címezzük meg a módosítandó node-ot az XML-fában.

Ezzel szemben notepadban megnyitva az applicationHost.configot csak át kell írni ezt a sort:

```
<centralW3CLogFile enabled=”true” directory=
”%SystemDrive%\inetpub\logs\LogFiles” />
```

Ezzel csak azt akartam megmutatni, hogy nem feltétlen kell mindent parancssorból megoldani, csak azért, mert Server Core-on vagyunk.

PHP + FastCGI Server Core-on

A PHP futtatásához szükség lesz a CGI-modulra, ebben van a FastCGI-támogatás is. Már tudjuk, mit kell tenni:

```
start /w pkgmgr /iu:IIS-CGI
```

A PHP-interpreter telepítéséhez le kell tölteni a php-csomagot, majd kicsomagolni és bemásolni a megfelelő helyre. Ezek bizony kihívások Server Core-on, hisz nincs sem böngésző, sem shellbe integrált zip program (hisz shell sincs).

Ha megtehetjük, töltsük le és csomagoljuk ki a dolgokat egy másik gépen, és másoljuk fel a Server Core-gépre egy megosztáson keresztül. A PHP xxx Non-thread-safe Win32

binaries PHP zip csomagot (http://www.php.net/downloads.php) töltsük le, hisz pont az az előnye a FastCGI-nek, hogy nem szálbiztos, nincs benne szinkronizáció, de emiatt gyorsabb, a FastCGI az alkalmazásokat úgyis biztonságban, egy szálon futtatja.

Csomagoljuk ki valahová, ez nálam a H:\PHP könyvtár lett.

A PHP-könyvtárban levő PHP.INI-Recommended fájlt át kell nevezni php.ini-re. Ezután az IIS-nek megmutatjuk, hol van a php-futtató:

```
AppCmd set config /section:system.webServer/fastCGI /+
[fullPath='h:\php\php-cgi.exe']
```

Majd a .php kiterjesztéshez beállítjuk a FastCGI-futtatót, és a script interpretert:

```
AppCmd set config /section:system.webServer/handlers /+
[name='PHP-FastCGI',path='*.php',verb='*',modules=
'FastCgiModule',scriptProcessor='h:\php\php-cgi.exe',
resourceType='Either']
```

Teszteljük le a művünket egy hello.php-val, amelyet, mondjuk, notepadben szerkesztünk meg, és a wwwroot könyvtárba mentünk el:

```
<?php echo 'Hello World!'; ?>
```

Az oldalra böngészve (egy másik gépről) máris látható a komplex php-webalkalmazásunk.

És hogy az egész életszagúbb legyen, ha valaki például wordpress nevű blogmotort szeretne Server Core-on futtatni, azt minden további nélkül megteheti, mondjuk MySQL-háttérrel, minimális vason.

Ez az egész Server Core lényege: sallangmentes, minimális konfiguráció egy nagyon jól behatárolt cél érdekében.

Hosting IIS7-en

A következőkben leírtak csak egy része vonatkozik a Server Core-ra, az ASP.NET-specifikus információk egyelőre csak a normál Windows 2008-ra értendők.

A hosting eléggé mostohagyermek volt a Microsoft háza táján, a korábbi IIS-ekkel nehéz volt egyes hosting-feladatokat szépen megoldani. A hosting azt jelenti, hogy valaki hardvererőforrásokat bérel egy hoster cégtől, amelyeket persze valamilyen operációs rendszeren és szoftvereken keresztül akináz ki. Itt most elsősorban a webes tartalom hostingjáról beszélek, de gyakori az adatbázis, a levelezés, a víruskeresés, a biztonsági mentés és egyéb szolgáltatások hostolása is. Webhosting esetén három életképet érdemes külön tárgyalni:

1. Osztott hosting: egy gép erőforrásain sok website osztozik
2. Dedikált hosting
3. Webfarm

Jelen cikkünkben az elsővel foglalkozunk részletesen, a harmadikra pedig még visszatérünk egy későbbi számban.

Osztott hosting

A mai hardverek óriási erőforrás-tartalékokkal rendelkeznek, így egy masina akár több száz kisebb forgalmú website-ot is ki tud szolgálni egyidejűleg. Kivéve, ha valamelyik site kisajátítja magának a gépet. Osztott hosting esetén tehát a kihívás a bérlők közötti erőforrások igazságos elosztása. Milyen erőforrásokról van szó?

Memória. 32 bites világban ez volt az egyik leggyorsabban elfogyó erőforrás. Tételezzük fel, hogy egy gépen 100 felhasználó websiteját hostoljuk. Legyen a maximális 4 gigabájt RAM a gépben, és olyan az alaplapunk, hogy látja az oprendszer az egészet. /3GB kapcsolóval is 1 gigabájt az oprendszeré, így marad nekünk 3 gigabájt. Fejenként ez 30 megabájtot jelent. Ez nem sok ám! Egy kisebb ASP.NET-alkalmazás memóriafelhasználása is simán felszalad 100 megára, azaz könnyen elfogyhat a memória. 64 bites architektúrákon persze lötyögnek az alkalmazások a memóriában, ott már kevésbé gond ez. De még itt is ügyelni kell arra, hogy igazságos legyen a memóriaelosztás az ügyfelek között.

Processzor. Egy végtelen ciklus, és máris intenzíven ki van sajátítva a proci. Az ilyen nyilvánvaló igazságtalanság ellen védenie kell a webszervernek a jól viselkedő webalkalmazásokat a bitorlóktól.

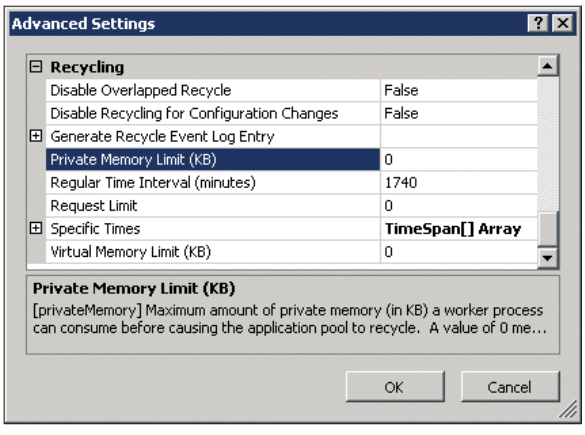
Diszkterület. Egyrészt korlátozni kell tudni a felhasználható tárterületet, másrészt meg kell akadályozni, hogy egymás adataihoz hozzáférjenek a bérlők.

Nézzük, milyen megoldások szolgálják a fenti pontokat az IIS7-ben!

Osztott hosting esetén az a tipikus, hogy minden bérlő részére létrehozunk egy Windows-felhasználót. Ez lehet AD-felhasználó vagy sima SAM-user, első körben ennek nincs jelentősége. Az IIS6-tal szemben ennek a felhasználónak nem kell semmilyen speciális csoporttagságot kapnia, röptében megadja a szükséges tagságot az IIS, amikor indítja az alkalmazást.

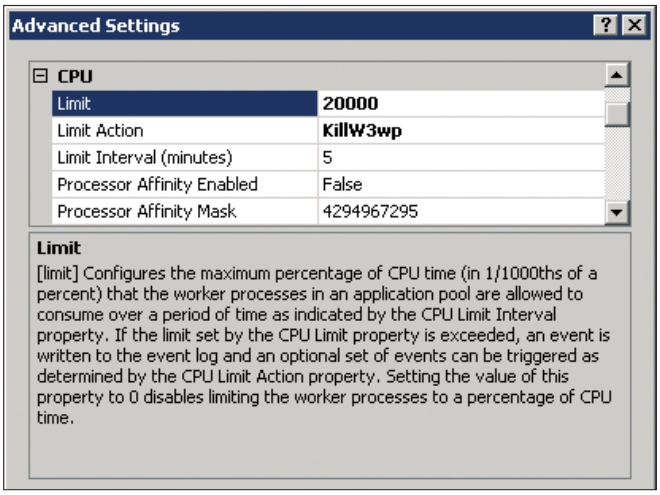
Mindegy egyes webalkalmazás részére létre kell hozni egy Application Poolt. Az AppPool definiálja azt, hogy milyen paraméterekkel indul el és fut a webalkalmazást kiszolgáló worker processz, a továbbiakban wp (w3wp.exe). Tehát minden tárhely egyedi felhasználók nevében, egyedi processzekben fut. Ha valamelyik processz feldobja a bocskort, az nem zavarja a többi bérlő webalkalmazását.

A memória túlzott igénybevételét is képes korlátozni az IIS. Az AppPoolnak meg lehet adni, hogy ha a wp memóriafelhasználása egy beállított méret fölé emelkedik, akkor indítsa újra a processzt *(2. ábra)*. Meg lehet adni virtuálismemória-korlátot és a private memória korlátját is. A private az a rész egy processzben, amit a Windows nem tud megosztani több processz között is. Például a kernel32.dll kódja minden wp-be betöltődik, azaz mindegyik virtuális memóriáját szaporítja, de mivel valószínűleg osztott a processzek között, ezért a private memóriát nem növeli.

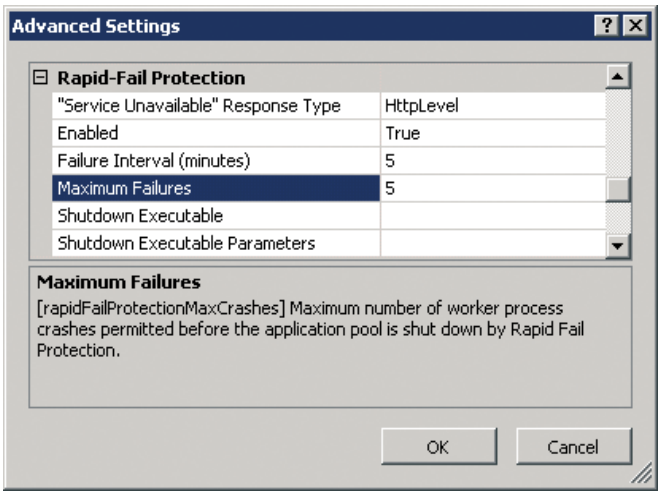


2. ábra. Memóriakorlátozások beállítása

Azért valószínűleg, és nem bizonyosan, mert ha egy másik DLL van betöltve arra a címre, amit fordításkor megadtak a kernel32-nek, akkor az OS Library Loadernek relokálnia,



3. ábra. A processzorhasználat beállításai



4. ábra. Rapid-Fail Protection, az IIS önvédelme sorozatos hibák esetére

módosítania kell a DLL kódját a memóriában, ami így nem lesz azonos a nem relokáltakkal, így nem lehet megosztani.

Vigyázni kell ezekkel a számokkal, mert csalókák lehetnek. Egy 500 megabájtos virtuálismemória-limit látszólag nagyon magas, ennek ellenére egy kisebb ASP.NET-alkalmazás is pillanatokra képes felhízni ekkorára, köszönhetően a lusta Garbage Collectornak és a sok (az előfordítás miatt szerencsére osztott) .NET rendszerkomponensnek. A private memória talán jobban jellemzi, mennyire sokat eszik az alkalmazás. A lényeg, hogy csak tapasztalati úton lehet belőni ezeket a számokat, és lehet, hogy lesznek alkalmazások, amelyeknek egyedi értékek kellenek, nem elég nekik, ami a többségnek elegendő.

Önvédelemből sztrájkolnak a munkások

Mit érzékelnek a wp újraindításból az alkalmazások? Sajnos azt, hogy az in-processz adatok, statikus változók adatai – ASP.NET Cache, ASP.NET Session stb. – elvesznek. Ha valaki kitöltött egy hosszú formot, majd az elküld gombra nyomva visszautasítja az adatok elmentését, mert lejárt (megsemmisült) a Sessionje, akkor bár sokat fog minket emlegetni, de garantált, hogy nem jön vissza többet az oldalra. Emiatt a szolgáltatónak érdemes elgondolkodnia valamilyen out-of-processz tárolási lehetőségen, legyen az adatbázisban tárolt Session vagy maga az adatbázis mint szolgáltatás.

Történelmi adat, de IIS6 esetén az operációs rendszer korlátoltsága miatt legfeljebb körülbelül 60 wp tud csak párhuzamosan futni, ennél többet csak a biztonság rovására lehet engedélyezni (UseSharedWPDesktop).

A processzor kisajátítása ellen beállítható, hogy ha a wp adott ideig (Limit Interval) adott résznél több procit evett (Limit), lőjék le a wp-t. A *3. ábrán* az van beállítva, hogy ha több mint 5 percig 20 százaléknál több procit használ a wp, kigyilkolják azt.

Vigyázni kell vele, mert lehet, hogy mondjuk egy képnézegető alkalmazásnál, ami röptében számol valamit egy nagyobb kép feldolgozása során, túllépi a limitet, és aztán jön a kapuzárási pánik.

A wp önvédelméhez még hozzátartozik az is, hogy ha túl sűrűn és/vagy sokszor leáll hibával a wp, akkor letiltja azt az IIS *(4. ábra)*. Ez egy jó szolgáltatás, másképp, ha nincs engedélyezve, lehet, hogy gyorsan betelik az event log, ha egy alkalmazás állandóan elszáll. ASP.NET-programozók azt gondolják, ó, hát én nem használok unmanaged komponenseket, énmiattam nem szállhat el a wp. Én is azt hittem, míg az élet rám nem cáfolt. .NET 2.0-tól kezdve, ha egy háttérszálban történik kivétel, a teljes managed AppDomaint leállítja a CLR (1.1-ben ez még nem így volt, sunyin elszállhattak a háttérszálak). Ha leáll az AppDomain, leáll a wp.

Ha leáll a wp, azt a Rapid-Fail Protection bajként érzékeli, és elindítja hóhér számlálóját. Még jön 4 felhasználó a következő 5 percben, és máris letiltódik az app, ahonnan már csak a rendszergazda hozhatja vissza.

Háttérszálakat sok esetben használunk, még ha nem is tudunk róla, például Timerek alkalmazása esetén, vagy tudatosan, aszinkron metódushívásoknál delegate-ek használatával. Az a baj, hogy az ASP.NET keretrendszer csak azon a fő szálon kapja el a kezeletlen kivételeket, amin a lapot elindította, a háttérszálakon nem. Tessék erről mesélni a fejlesztő kollégáknak, barátkozzanak a try-catch-csel.

A diszkterület védelme a Windows NTFS beépített Quota rendszere miatt egyszerűen beállítható. Azt kell átgondolni, hogy kötet- vagy mappaszinten állítjuk be a korlátozást? Ha a teljes kötetre, akkor védettek vagyunk az ellen, hogy a webalkalmazás programozottan telerakja a temp könyvtárat vagy bármely más helyet, ahová csak van joga írni. Viszont nem várt módon lehet, hogy kevesebb helyet kap így a bérlő, mert az ASP.NET átmeneti fájlokat ír a rendszerpartícióra, így ha az ugyanazon a köteten van, mint az adatok (nem ajánlott, természetesen), akkor ez is viszi a Quotát.

Teljes elszigetelés

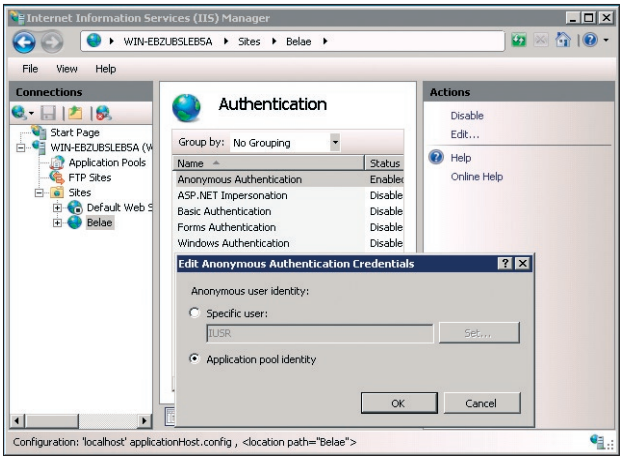
A másik megfontolandó kérdés, hogyan védjük egymástól a webalkalmazások adatait?

Alapfelálásként ajánlottam, hogy minden wp saját account nevében fusson. Az ASP.NET kódok a wp-fiók nevében futnak. Statikus fájlokhoz viszont nem a wp-felhasználónak, hanem az IUSR új beépített felhasználónak kell olvasási jog, mert ezt személyesíti meg a wp alapértelmezett módon.

Ez azonban problémás, mert így az én siteomon futó kód el tudja olvasni a szomszédok tartalmát, mert nekik is ugyanaz az IUSR van beállítva olvasási joggal. Ezért érdemes minden felhasználó esetén átállítani, hogy Anonymous hitelesítés esetén az AppPool-

hoz beállított fiók nevében érje el az IIS a webes tartalmat, így már nem lehet belekukkantani a szomszéd adataiba (*5. ábra*).

Milyen jogok kellenek ezek után az AppPool-felhasználónak a tárhely könyvtárára? Nyilván, hogy oda csak neki legyen joga írni, meg persze a szokásos Systemnek és Adminstrators csoportnak.



5. ábra. Az anonymous felhasználók nem IUSR, hanem a wp felhasználója nevében olvassák a tartalmat

Ez jó, mert az alkalmazás tud adatokat tárolni maga mellett közönséges fájlokban. Rossz viszont, hogy egy rosszul megírt ASP.NET-weboldal segítségével saját ASP.NET-oldalt is írhatnak a fájlrendszerbe, amit távolról meghívva már kódot is tudnak futtatni a gépen. Ebből baj lehet. Nem jó, ha egy weblap maga mellé tud írni.

Ezért szerencsésebb, ha csak olvasási joga van a wp-t futtató fióknak a bérelt könyvtárra. Ebben az esetben viszont ki kell alakítanunk egy olyan könyvárat minden felhasználó részére, ahová van írási joga, de nem érhető el a webszerveren keresztül. Ide írhatják az átmeneti fájljaikat, kis adatbáziskáikat stb.

Ez elég biztonságos megoldás, de akkor még megoldandó probléma a tartalom feltöltése. A feltöltéshez nincs kézenfekvőbb, mint az új FTP-szerver, amit az előző számban alaposan kielemeztem. Amit most át kell gondolni, hogy milyen jogok kellenek a felhasználó könyvtárára, hogy az FTP-n keresztül tudjunk tartalmat feltölteni? Ha Windows-hitelesítést használunk az FTP-szerveren, akkor sajnos beleütközünk az előbb tárgyalt dilemmába, elég-e az olvasási jog a könyvtárra, vagy kell írás is? Windows-hitelesítés esetén kell írásjog, hisz ilyenkor a wp-t is futtató felhasználó nevében írja az FTP-szerver is a fájlokat. Jobb megoldás lehet, ha minden felhasználó kap egy IIS-felhasználót is, és annak engedélyezzük az írást a tárhelykönyvtárra. Ekkor az írás a Network Service nevében történik (az IIS-felhasználó nevében nem történhet, hisz az egy nem létező felhasználó a Windows Security szempontjából), így csak annak kell módosítási jog a felhasználói könyvtárakra. Hogy ne tudjunk írni más könyvtárába, arról gondoskodik az FTP-kiszolgáló User Isolation szolgáltatása.

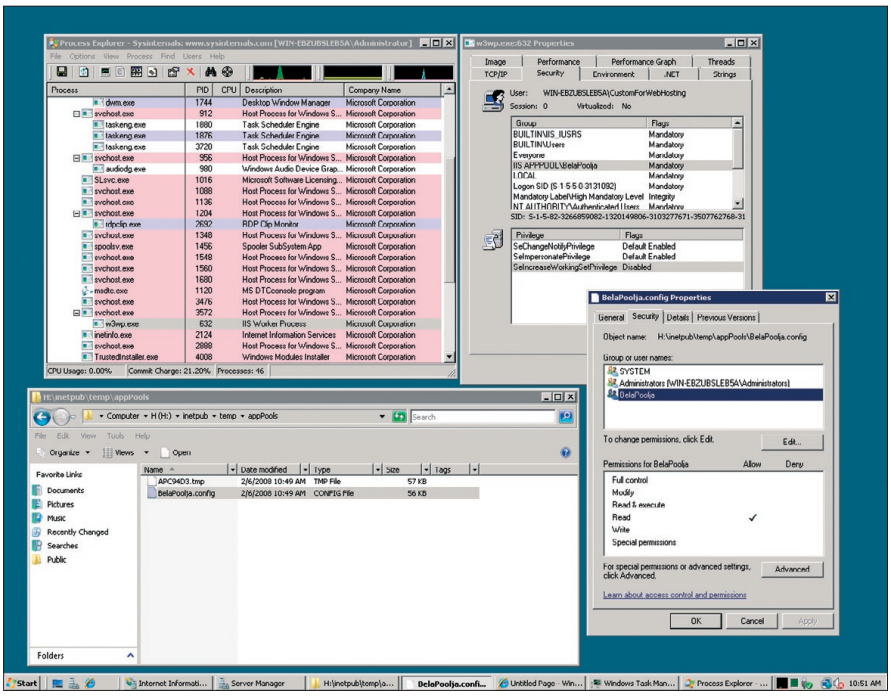
Mint említettem, osztott hosting esetén szinte kötelező minden sitehoz saját AppPool-fiókot létrehozni. Ha mégse tennénk, és mondjuk minden az alap Network Service/IUSR nevében futna, még az ilyen esetekre is van védelem az IIS-ben, hogy legalább a központi konfigot ne tudják szétbarmolni a site-ok, illetve – némi plusz munkával – hogy egymás adatait se tudják elérni. Emésszük ezt! Bár ugyanannak a felhasználónak a nevében fut több wp, mégsem tudják elérni egymás adatait. Hogy oldották ezt meg?

A wp alapban Network Service-ként indul, majd megszemélyesíti az IUSR-felhasználót. Ha valaki kiadja a RevertToSelf API-hívást, akkor visszacsinálta a megszemélyesítést, és máris Network Service-ként futtathat kódot. Illetve, ha valaki beállítja az 5. ábrán látott módon az Anonymous hitelesítést az alsó opcióra, akkor még Revert sem kell.

Ha a közös fióknak, példánkban a NetworkService-nek volna joga írni a központi konfigot, nagy baj lenne. Persze, alapban nincs, ezen nem is szabad változtatni. Hogy biztosan ne firkáljon bele, a következőt teszik. Egyik alkalmazás sem látja az eredeti applicationHost.configot, hanem mindegyik csak egy másolatot lát belőle. A másolat a wp indulásakor a ...\inetpub\temp\appPools könyvtárban keletkezik, és csak az Administrators/System kombónak van módosítási joga rá. A wp-t a következő paraméterekkel indítják el (Process Explorerrel vagy Process Monitorral nyerhető ki ez az infó):

```
w3wp.exe ... -h "H:\inetpub\temp\apppools\
BelaPoolja.config" -ap „BelaPoolja"
```

A trükk most jön. A wp-be induláskor beinjektálnak egy kézzel összerakott SID-et. Ez látható a 6. *ábra* jobb felső részén, a



6. ábra. Egyedi SID a konfiguráció védelmére

Process Explorer mutatja meg nekünk: az IIS APPOOL\BelaPoolja SID. Hangsúlyozom, nincs ilyen felhasználó a Windows felhasználói adatbázisában, ez egy mesterségesen létrehozott custom SID. A 6. ábra jobb alsó sarkában látszik, hogy ennek a SID-nek adnak olvasási jogot (de még ennek se többet) a másolt konfigra. Ezzel az igen fejlett trükkel teljesen elszigetelték egymástól a wp-ek által látott központi konfigurációs adatokat.

Ugyanezt az elszigetelést mi is alkalmazhatjuk a felhasználó webtárhelyének könyvtáraira. A szokásos mappajogosultság-beállítás során használhatjuk az AppPool SID-et, azaz a BelaPoolja-t, és ennek kell olvasási vagy módosítási jogot adni, az egyedi wp-felhasználónál tárgyalt módon.

Azaz, úgy el tudjuk szigetelni egymástól a tárhelybérlők adatait, hogy mégis mind azonos felhasználó nevében futó wp-szel van elérve. Azért ez ügyes. Nem kicsit, nagyon.

Mindezek ellenére én a sokfelhasználós AppPool-modellt javaslom, az valamivel könnyebben kezelhető.

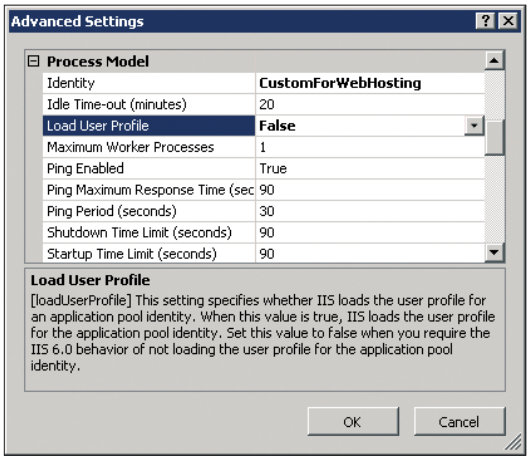
Jogosultságok

Az eddigiekből látható, hogy alaposan át kell gondolni, melyik wp kinek a nevében fut, hogy a lehető legbiztonságosabb módon védjük a felhasználók adatait. Nem triviális a feladat, de kezelhető.

Ha ASP.NET-alkalmazásról van szó, akkor még ráadásul van egy plusz védelmi szintünk, a .NET Framework saját biztonsági rendszere, a Code Access Security. Ez teljesen független az operációs rendszer saját biztonsági rendszerétől, a managed kódnak először ezen kell átmennie, és aztán még jön az oprendszer saját jogosultságellenőrzése is.

A részletek mellőzésével: arról van szó, hogy finoman szabályozhatjuk, milyen műveleteket hajthatnak végre a weblapok programjai. Alapban FullTrust van beállítva, azaz a .NET biztonsági rendszere nem akadályoz meg semmilyen műveletet. Tárhelyszolgáltatók tipikusan lejjebb veszik a biztonsági szintet, általában Mediumra. Ebben a weblapok kódja alapban csak az alkalmazás saját könyvtárába tud írni, máshová nem. Hálózati kapcsolatokat nem tud létesíteni kifelé, unmanaged kódot nem tud hívni (naná, azonnal hatástalan lenne a CAS), és még jó pár egyéb szigorítás, azaz semmilyen veszélyes dolgot nem tud művelni. A pontos jogosultsághalmaz persze testre szabható, amire sokszor szükség is van.

Például Medium esetén nem engedélyezettek az OleDB-szolgáltatón keresztüli adatelérések, így például Access adatbázist nem tud az ügyfél használni. Persze, jó oka volt erre a Microsoftnak, hisz egy bugos OleDB provider natív kódjára nem érvényes a CAS, így bármit megtehet a gépen (az operációs rendszer biztonsága persze rá is vonatkozik, erről már volt szó). A hálózati elérés korlátozása is zavaró lehet, hisz így például egy online RSS-olvasót sem lehet írni. Természetesen lehet engedélyezni akár egyedi címekre, akár mindenre, hogy ki tudjon szólni az alkalmazás.



7. ábra. Az Application Poolt futtató fiók profile-betöltésének szabályozása

Egyes ügyfelek teljesen jogosan szeretnének használni valamilyen unmanaged komponenst is, például valamilyen saját üzleti számítást végző COM-komponenst. Ehhez sajnos meg kell adni az Unmanaged futtatási CAS-jogot, ezzel viszont kinyitjuk Pandora szelencéjét, gyakorlatilag már nem építhetünk a CAS-ra. Jól látszik, nem egyszerű kompromisszum ez a használhatóság és a biztonság között.

De gondoljunk arra, hogy nem .NET-web-alkalmazásoknál eleve csak az az operációs rendszer biztonságára alapozhatunk.

Osztott hosting esetén át kell gondolni a konfigurációkezelés kérdését is. Az az ideális, ha a felhasználók mindent be tudnak állítani maguknak, ami nem veszélyes a szerverre vagy a többiekre. Ebben ideális partner az IIS7 modularizált konfigurációkezelése, amelyben nem csak az ASP.NET, hanem az IIS konfigurációja is elosztott, egyedi web.configokkal módosítható. Így az új konfiguráció beállítása egyszerűen egy új web.config felmásolását jelenti a tárhelyre.

Az IIS7-ben precízen beállítható, hogy alkalmazásonként mit lehet módosítani és mit nem. Például letilthatjuk, hogy bekapcsolják a Windows-hitelesítést, mert ha az alkalmazás még meg is személyesíti a távolról belépett felhasználót, akkor remek felületet biztosított a hackereknek az Administrator találgatásos jelszófeltörésére. De gyakran engedélyezzük a Default Document beállítási lehetőséget, hogy ne csak default.htm lehessen a főlap, hanem mondjuk index.php.

A bérelt site konfigurálása azonban nemcsak a web.config kézi módosítgatásával történhet. Az IIS Managert le lehet tölteni már XP-hez is, és ezzel be lehet menni a hoster gépen található tartalomra. HTTPS, azaz titkosított csatornán történik az adminisztráció, a felhasználó saját Windows- vagy IIS-fiókjával. Az admin felület persze a háttérben a személyes web.configot írja.

Egyes alkalmazások építenek az őket futtató felhasználó profiljára, azaz feltételezik, hogy van például könyvtár a lokális adatok, a dokumentumok stb számára. Ezek ugye a profile-ban tárolódnak. Az IIS7 alapban nem tölti be az AppPool felhasználó profilját, mert a legtöbb esetben nincs rá szükség, és jelentősen lassítja a wp indulását. Ha valamely alkalmazás mégis szeretne profilt használni, akkor be lehet kapcsolni ennek betöltését *(7. ábra)*.

Zárszó

A Windows 2008 Server Core érdekes új irányvonal a Windows-termékpalettán, amely ígéretes lehetőség a jövőbeli specializált, kis erőforrás-igényű webalkalmazások számára.

Az IIS7 jól láthatóan erősen fel lett készítve a hosting igénybevételre, így ez az első olyan IIS-verzió, amely kényelmesen használható sok tárhely egy gépen történő kiszolgálására.

Soczó Zsolt
MCSD, MCDBA, ASP.NET MVP
(http://soci.hu)
Research Engineer
Qualification Development Kft.

ethical hacking

Cégük valószínűleg sokat költ biztonsági szoftverekre. De biztos, hogy ez elég ahhoz, hogy értékes adatvagyonukat biztonságban tudják?
Egy tény a sok közül: a CERT 2007-es E-Crime Watch felmérésében résztvett cégek 49%-át érte támadás. Ez 11%-os növekedés az előző évhez képest.

Ethical Hacking a NetAcademiánál!

A NetAcademia Oktatóközpont a világon elsőként etikus hekker minősítést kiadó EC-Council kizárólagos magyarországi képviselője, és egyben Ethical Hacking tanfolyamának hivatalos oktatócége lett. Hallgatóink egy világszerte elismert és egyedülálló tematika alapján sajátítják el az információvédelem új szemléletű és hatékony módjait.

Az Önök cégénél van már CEH szakember?

Az Ethical Hacking tanfolyam elvégzése után a hallgatók CEH minősítést (Certified Ethical Hacker) szerezhetnek. Ez a tanúsítvány a világon mindenütt egyértelműen bizonyítja, hogy a cím birtokosa megfelelő tudással és tapasztalattal rendelkezik a hálózatok és számítógépek biztonsági réseinek feltárásában és a hatékony információvédelem kialakításának területén.

C|EH
Certified Ethical Hacker

A tanfolyam legközelebbi időpontjai: március 31., április 21.

Az Ethical Hacking tanfolyam elvégzése a CISA, CISM és CISSP minősítéssel rendelkező hallgatóknak 30 CPE pontot ér.

További információért kérjük, látogasson el honlapunkra (www.netacademia.net/ethical), vagy keresse Szántó Zoltánt (1/472-1214).

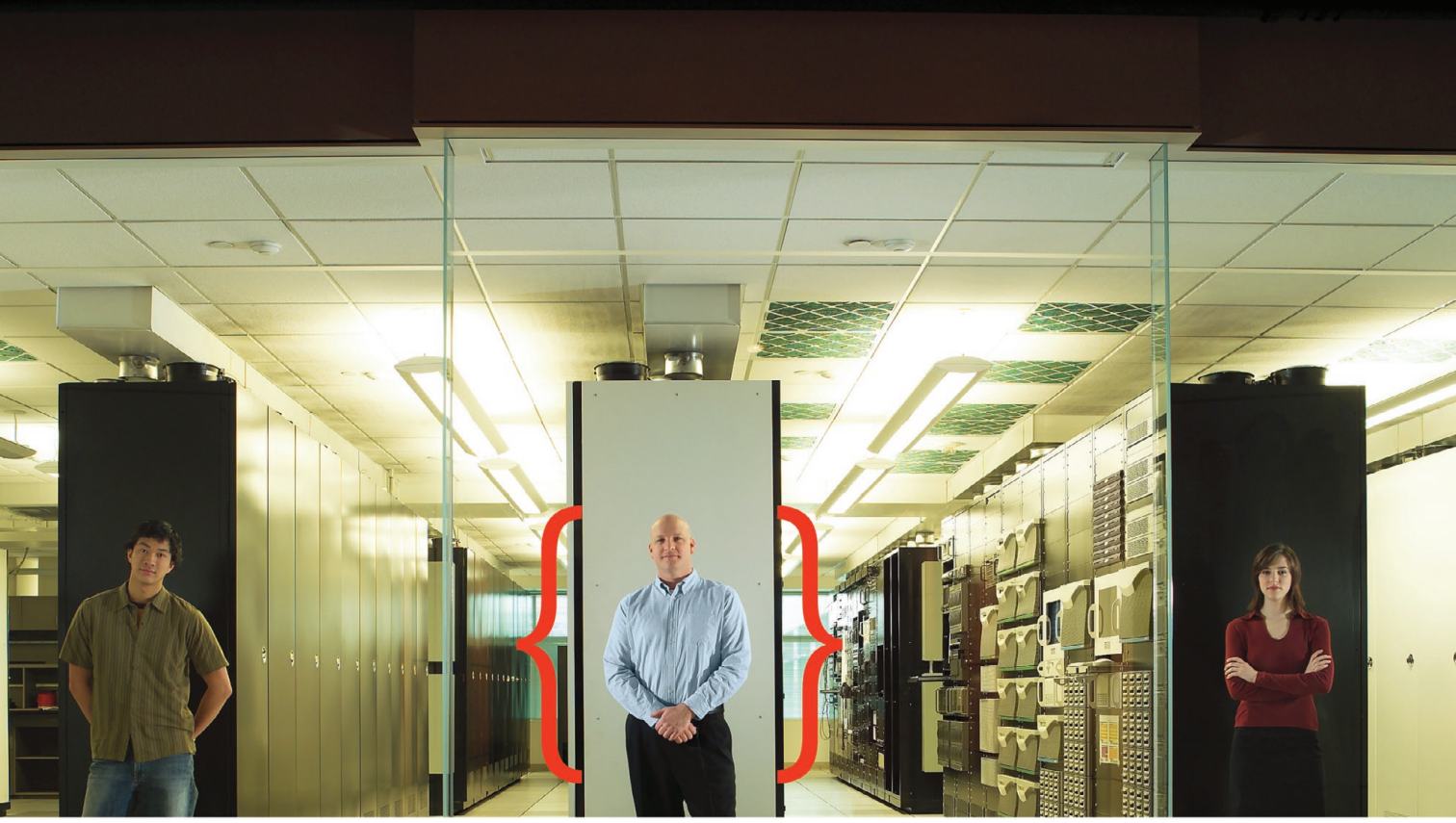
Ethical Hacking Konferencia

A NetAcademia 2008. április 24-én, az országban első alkalommal Ethical Hacking Konferenciát tart. A gyakorlati példákkal színesített minitanfolyam jellegű rendezvény ízelítőt ad a rendszereket érő támadásokból, és az ezek elleni védekezésből.
Az elismert szakembergárdát felvonultató konferencia előadói között az EC-Council is képviselteti magát.

További információ és jelentkezés a konferenciára: www.netacademia.net/konferencia

NetACADEMIA
A LEGJOBBAKAT TANÍTJUK

EC-Council | Accredited Training Center



www.microsoft.hu/2008

A HŐSÖK
köztünk {élnek}

Testet ölt a Microsoft szerverek új generációja 2008 tavaszán.
Legyen Ön is jelen, amikor elsőként kilép a magyar közönség elé a Microsoft Windows Server 2008, a Microsoft Visual Studio 2008 és a Microsoft SQL Server 2008. Értesüljön elsőkézből az újdonságokról, találkozzon személyesen a szakértőkkel és próbálja ki a szoftverek új lehetőségeit!

Értesüljön {**az elsők között**}

2008. március 5. – Windows Server 2008 termékbejelentő party és szakkiállítás
2008. március 27. – Visual Studio 2008 termékbejelentés
2008. május 7. – SQL Server 2008 termékbejelentés

Windows Server 2008 | Microsoft Visual Studio 2008 | Microsoft SQL Server 2008