TechNet MAGAZIN

2006. JÚNIUS-JÚLIUS

MÉLYVÍZ, CSAK ÚSZÓKNAK!

Windows Vista™

PILLANTÁS AZ INFOCARDRA
Egységesítheti a webes identitáskezelést

WEBSZOLGÁLTATÁSOK A VADONBAN
Komplex rendszerek együttműködését modellezve

KÉTSZER HÚSZ ÉRV
Az ISA Server 2004 Standard kulcsfontosságú jellemzői

AMIT MÁR MOST ÉRDEMES TUDNI RÓLA:

- FELHASZNÁLÓI SZEMMEL
- MILYENNEK LÁTJA A RENDSZERGAZDA
- HÁLÓZATKEZELÉS ÉS TŰZFAL

ÁRA: 1490 FORINT

9 771586 518005 00525

Microsoft TechNet

Ünnepeljen velünk!

A SZÁMALK Továbbképzés **10 éve** a Microsoft hivatalos oktatóközpontja. Az évforduló alkalmából kedvezmények sorozatával várjuk Önöket.

Microsoft GOLD CERTIFIED Partner

Advanced Infrastructure Solutions
Networking Infrastructure Solutions
Learning Solutions

Tervezzük meg közösen képzéseit június 30-ig,
mi garantáljuk egész évben a kedvezményt!

50% kedvezmény minden tanfolyamunk díjából!

Jelentkezzen június végéig két fővel azonos időpontú, ugyanazon meghirdetett tanfolyamunkra, és a második résztvevő képzési **díját elengedjük,** és Önnek csak a tananyag/licensz díjat kell kifizetnie!* És ezt az előnyt nem csak Microsoft, hanem valamennyi meghirdetett képzésünkön élvezheti!

10% kedvezmény minden Microsoft Press szakkönyvünk árából!

Regisztrált ügyfeleink részére magyar és idegen nyelvű szakkönyveink díjából 10% kedvezményt biztosítunk.*

Hosszú távon is szeretné ezen kedvezményeket cégénél igénybe venni?

Kérjük, keresse értékesítő és partnermenedzser munkatársainkat, akik szívesen kimennek cégéhez a részletek megbeszéléséhez, és tájékoztatják Önt oktatási megoldásainkról, szolgáltatásainkról, kedvezményekről és támogatási lehetőségekről.

2006-os évre számos új képzéssel várjuk Önöket, melyekre szintén igénybe vehetik akciónkat:
IT vezetői tréningek (ITIL, MOF, MSF) • Visual Studio 2005 • SQL Server 2005 • Microsoft CRM 3.0

*A kedvezmények más kedvezményekkel, akciókkal nem vonhatóak össze, más szolgáltatásra nem válthatóak át és visszavonásig élnek. A kedvezményeket weboldalunkon regisztrált ügyfeleink vehetik igénybe (regisztrációját a tanfolyamoknál, az Online jelentkezés menüpont alatt ejtheti meg). Az akció részletes feltételeit internetes oldalunkon a www.szamalk.hu/tisza címen az Akciók menüpont alatt találhatja, vagy kérjük, keresse munkatársainkat.

SZÁMALK

SZÁMALK Továbbképzés az Ön sikere ... a mi tudásunk

www.szamalk.hu/tisza Cím: 1115 Budapest, Etele út 68. Tel: 203-0304/4120, 4121, 4122 m.

A FORMA ÚJ, A SZÍNVONAL A RÉGI!

Sziebig Andrea
főszerkesztő

A hetedik év gyakran jár együtt valamiféle változással. Elérkezett a TechNet Magazin külső-belső finomhangolásának ideje.

Minden terméknek megvan a maga életciklusa – hajtogatta bőszen egykor volt kollégám. Mindig akkor hozakodott elő ezzel a kijelentéssel, amikor úgy érezte: gyökeres megújulásra van szüksége kedvenc lapjának. Nos, valami hasonló történt a TechNet Magazin esetében is: a Microsoft-hívek körében immár hetedik éve jól ismert lap megújult.

A megújulás jelei elsősorban formaiak és „hátországbeliek", kevésbé tartalmiak. Mivel a kiadvány ezentúl is a szakmának, az informatikával professzionális szinten foglalkozó szakembereknek szól, továbbra is mély technológiai tudást közvetít. Tudjuk jól, hogy az informatikusok kemény magja nem igazán vevő a marketingszlogenekre, így ezek mellőzésére most is biztonszámíthatnak. S a különféle Microsoft-technológiák tolmácsolásához szakavatott, az egyes termékekre, technológiákra specializálódott Microsoft-képesítésű szakemberek közreműködése a garancia.

A lényegi tartalmi jegyek megőrzése mellett külsőre alaposan megváltozott a TechNet: a tartalommal harmonizáló visszafogott elegancia, letisztultság és strukturáltság formai megteremtése volt a szándékunk. A külső-belső finomhangolásokhoz új kiadót is keresett a lap korábbi „gazdája", s választása a Vogel Burda Communicationsre esett. Az ezentúl a mi gondozásunkban készülő kéthavi kiadvány első számát tartják a kezükben. S mi más is állhatna a középpontban ezúttal, mint a Windows Vista: mindaz, amit már most érdemes tudni róla.

TechNet MAGAZIN

SZERKESZTŐSÉG
Főszerkesztő
Sziebig Andrea – *asziebig@vogelburda.hu*
Szakmai lektor
Budai Péter – *i-pbudai@microsoft.com*
Vezető szerkesztő
Varga János – *jvarga@vogelburda.hu*
Munkatársak
Budai Péter – *i-pbudai@microsoft.com*
Microsoft Magyarország, programmenedzser – IT szakmai programok

Fülöp Miklós – *mfulop@microsoft.com*
Microsoft Magyarország, rendszermérnök

Gál Tamás – *gtamas@tjszki.hu*
rendszermérnök (MCT, MCSE, MCSA, MVP)

Kelemen László – *kelemen@hungary.com*

Kovács Zoltán – *kovacsz@szamalk.hu*
Számalk Rt., vezető oktató

Lepenye Tamás – *lepenyet@mal.hu*
vezető rendszermérnök (MCSE)

Mészáros Csaba – *mcsaba@vogelburda.hu*

Moldova György – *v-gyomol@microsoft.com*
Microsoft Magyarország (MCSE+I, MVP, MSS)

Nagy Levente – *nagy.levente@microsoft.com*
Microsoft Magyarország, szoftverfejlesztési szakértő

Simon Ferenc – *simonf@szamalk.hu*
Számalk Rt., Microsoft-partnermenedzser

Tervezőszerkesztők
Bujdosó Anikó – *abujdoso@vogelburda.hu*
Papp Gyula – *gypapp@vogelburda.hu*
Korrektor
Bende Magdolna – *mbende@vogelburda.hu*
Lapterv és címlap
Kocsis Gábor – *emotion@axelero.hu*

Szerkesztőség és kiadó címe:
Vogel Burda Communications Kft.
1077 Budapest, Kéthly Anna tér 1.
Tel.: 888-3400, fax: 888-3499

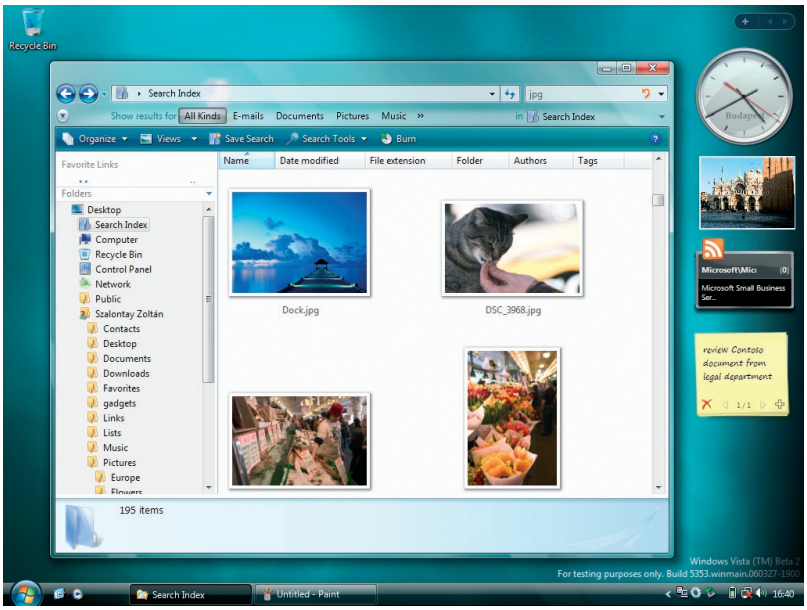
KIADÓ
Kiadja a Vogel Burda Communications Kft.
A kiadásért felel
Carsten Gerlach ügyvezető igazgató
cgerlach@vogelburda.hu
Tel.: 888-3470, fax: 888-3499
Lapigazgató:
Walitschek Csilla
cswalitschek@vogelburda.hu, tel.: 888-3450

MÉDIAREFERENSEK:
Harsányi Erika – *eharsanyi@vogelburda.hu*, tel.: 888-3452
Németh Krisztina – *knemeth@vogelburda.hu*, tel.: 888-3468
Rátóti Sarolta – *sratoti@vogelburda.hu*, tel.: 888-3453
Szendrey Szilvia – *szendrey@vogelburda.hu*, tel.: 888-3455
Fax: 888-3459
Marketing:
Gajdos Barna – *bgajdos@vogelburda.hu*, tel.: 888-3494
Hirdetési koordinátor:
Szőke Erika – *eszoke@vogelburda.hu*
Tel.: 888-3411, fax: 888-3459
Nemzetközi hirdetésfelvétel:
Eric N. Wicha – *ewicha@vogelburda.com*
Vogel Burda Holding
Poccistrasse 11, D–80336 München
Tel.: +49 89 74642-326, fax: +49 89 74642-325
A hirdetések körültekintő gondozását kötelességünknek érezzük, de tartalmukért felelősséget nem vállalunk.

TERJESZTÉS
Terjesztett példányszám: 3000
Előfizethető a terjesztési osztályon és boltunkban
Terjesztési osztály: 1426 Budapest, Pf. 300/39
Fehér Ildikó – *ifeher@vogelburda.hu*, tel.: 888-3422, fax: 888-3499,
Rehó Rita – *rreho@vogelburda.hu*, tel.: 888-3421, fax: 888-3499
Ügyfélszolgálat és bolt: Budapest V., Bajcsy-Zsilinszky út 60.
hétfő–péntek: 8–20 óráig, szombat: 10–16 óráig
Előfizetési díj hat számra:
7599 forint
További információ: 06-80/444-444
Nyomda:
Pauker Nyomdaipari Kft.
1047 Budapest, Baross utca 11-15.
Felelős vezető: Vértes Gábor ügyvezető igazgató
ISSN 1586-5185

Címlapon

A Windows Vista fejlesztése a végéhez közeledik, lapunk megjelenésével egy időben lát napvilágot a második bétaváltozata. A Microsoft rohamléptekkel dolgozik szoftvereinek legújabb generációján



Hírháttér

Biztonság

Internet

Scripting

Infrastruktúra

Alkalmazásplatform

Oktatás

Közösség

Windows Live

Egyre bővül az internetes szolgáltatások köre, a Windows Vista megjelenéséig még további újdonságok várhatók.

Tavaly év végén harangozta be a Microsoft Live nevű stratégiáját, amelynek egyik legfontosabb eleme a Windows Live. Ez egyrészt a korábban MSN néven futó szolgáltatások új márkaneve, másrészt a Windows operációs rendszer funkcionalitását igyekszik kibővíteni az internet irányába. A Microsoft szükségét érezte ugyanis, hogy kihasználja a szoftverterjesztés új megközelítéséből fakadó előnyöket, amelyeknek nem a dobozos szoftverek, hanem a gyakran frissülő, bárhonnan elérhető szolgáltatások jelentik az alapját.

A Windows Live rengeteg apró szolgáltatást fog össze, köztük a www.live.com weboldalt, a Windows Live keresőt, valamint az MSN Messengert is, amelyik új néven, Windows Live Messengerként lesz elérhető a 8-as verziótól kezdve (bétaváltozata már letölthető).

Igény szerint

A live.com egyelőre próbaüzemben működik, mint arra a logó mellett látható beta felirat is utal. A megvalósítás hátterében az áll, hogy a Microsoft kutatásai szerint a számítógép-használók egyre több időt töltenek online, azonban sokukat erősen frusztrálja, hogy az általuk igényelt tartalmakhoz csak sok különálló weboldal meglátogatásával juthatnak hozzá. A live.com képes arra, hogy különféle, általunk megadott és testre szabott oldalelemeket és szolgáltatásokat jelenítsen meg, ezáltal egyfajta internetes kezdőlapként szolgálhat.

Ha a Windows valamely képességéhez kellene hasonlítani, leginkább a munkaasztal internetes megvalósításának tekinthető, mivel egy helyen tárolja a számunkra legfontosabb hivatkozásokat és szolgáltatásokat. Az oldalhoz külső fejlesztők által a legkülönfélébb témákban – a részvényárfolyamok megjelenítésétől a *Chuck Norrisra* vonatkozó információk közléséig – készített minialkalmazásokat a Microsoft Gadgets (http://microsoftgadgets.com) webhelyről lehet telepíteni.

A Windows Live-család folyamatosan új tagokkal bővül, ezek közül az egyik legérdekesebb a Windows Live Toolbar, amely olyan hasznos funkciókkal egészíti ki az Internet Explorer 6-ot, mint például a többlapos böngészés, az RSS-csatornák automatikus észlelése és az adathalászat-ellenes szűrő. Ezek a képességek már eleve benne lesznek a hamarosan megjelenő Internet Explorer 7-ben, de addig is legalább elérhető egy eszköz, ami pótolja a hiányukat.

Természetesen a Windows Live része a Windows Live Search (search.live.com) keresőfunkció is, amely több érdekes újdonsággal hívja fel magára a figyelmet, és egyre használhatóbb találatokat ad.

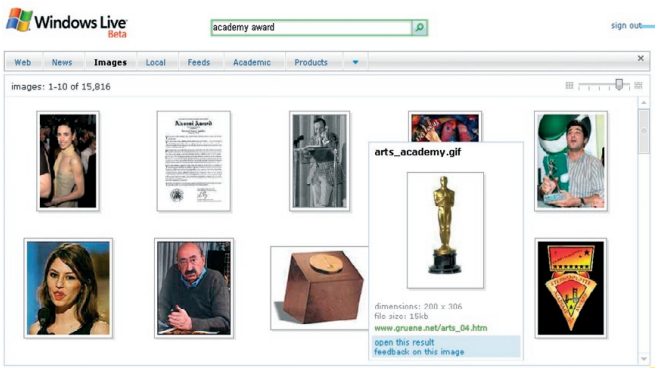
További lehetőségek

Szintén a Windows Live részeként érkezik az új Hotmail-verzió – Windows Live Mail névre fog hallgatni. További érdekes szolgáltatások: kedvenc hivatkozásaink, képeink, állományaink megosztásának lehetősége másokkal, valamint a Windows Live Q&A, amelynek révén több millió internetező tudását vehetjük igénybe kérdéseink megválaszolásához. A Windows Live Local segítségével térképhez köthetünk más jellegű adatokat, így például megjelölhetjük kedvenc helyeinket, leendő összejöveteleink helyszínét, és az információkat megoszthatjuk másokkal.

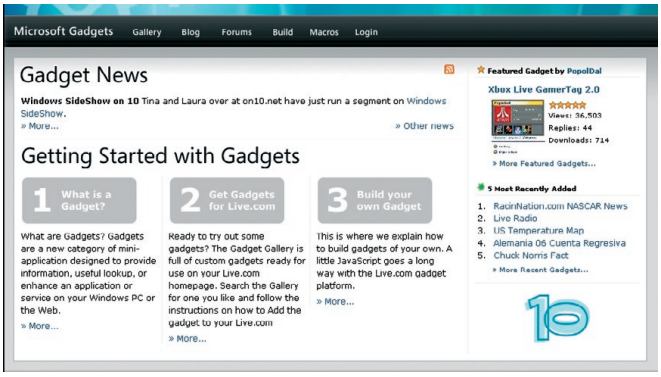
A Microsoft hamarosan elkezdi összeköttetni az egyes szolgáltatásait, hogy azok együtt még többre legyenek képesek. A cél hosszabb távon egy közösségi hálózat kialakítása, amelyben egy szűkebb baráti kör képes lesz csereügyleteket lebonyolítani (Windows Live Expo), meghívókat küldeni, beszélgetni, magasabb szintre emelve ezzel az internet kapcsolatépítő lehetőségeit.

Nem kell különösebb jóstehetség annak megelőlegezéséhez, hogy a jövő egyik legnépszerűbb szolgáltatása a jelenleg még fejlesztés alatt álló Windows Live Drive online tárolási szolgáltatás lesz, amelynek egyelőre még a neve sem végleges. Használói egy virtuális merevlemezen tárolhatják adataikat, amelyekhez bárhonnan hozzáférhetnek.

Mészáros Csaba



Automatikusan megkeresi a keresési szempontnak megfelelő képeket is a Live Search



Microsoft Gadgets: minialkalmazások a Windows Live-hoz

Moduláris felügyelet

Microsoft Management Summit 2006.

Az áprilisban San Diegóban megrendezett Microsoft Management Summit 2006 középpontjában a mai dinamikus IT-környezetekben működő Microsoft-technológiák és megoldások, illetve a cég és más vállalatok platformjain futó szolgáltatások felügyelete állt.

A számos szekcióban áttekintették a Microsoft System Center termékcsaládjának a találkozó idején már elérhető tagjait, többek között a System Management Servert (SMS), a Microsoft Operations Manager (MOM) 2005-öt, a System Center Data Protection Managert, a System Center Capacity Plannert és a Windows Server Update Servicest (WSUS). Gyakorlati bemutatók formájában részletesen foglalkoztak a Windows Server 2003 R2 menedzselésével, a Group Policyvel, a szerverrendszerek felügyeletével és a WMI lehetőségeivel, valamint az eddig Monadként ismert parancsértelmező keretrendszerrel.

A mai heterogén IT-struktúrák menedzselése természetesen nemcsak a System Center-család és a szoftver felügyeletét jelenti. Ennek megfelelően részletesen volt szó a MOM és az SMS Linux, a Unix és a Macintosh rendszerekben elérhető képességeiről; a hardvereszközök és hálózati infrastruktúrák menedzseléséről, valamint a MOM és az SMS más felügyeleti konzolokkal megvalósítható integrációjáról.

A bemutatók és a legjobb gyakorlati megoldások ajánlásai hangsúlyosan az IT-Infrastructure Library (ITIL) üzemeltetési módszertan és az annak alapján kialakított, de még az ITIL-nél is szigorúbb követelményeket támasztó Microsoft Operation Framework (MOF) köré épültek.

A találkozón természetesen új technológiákról és megoldásokról is szó volt; csak felsorolásszerűen néhány fontos bejelentés: MOM V3, SMS V4, SMS R2, System Center Reporting Manager, WSUS 3.0 (béta 1), Windows Vista Management Technologies, és ennek kapcsán a Microsoft Management Console (MMC) 3.0. A MOM v3 egyébként a System Center Operations Manager 2007 nevet kapja majd, az SMS v4 hivatalos elnevezése pedig System Center Configuration Manager 2007 lesz.

További két fontos „családtag”:

- Az IT-életciklus körüli munkafolyamatok szabályozása, az infrastuktúra hardver- és szoftverleltárának kezelése a Service Desk nevű új termék feladata lesz.
- A PowerShell a Monad utódjaként hatékony adminisztratív parancssor- és scriptkörnyezetet biztosít.

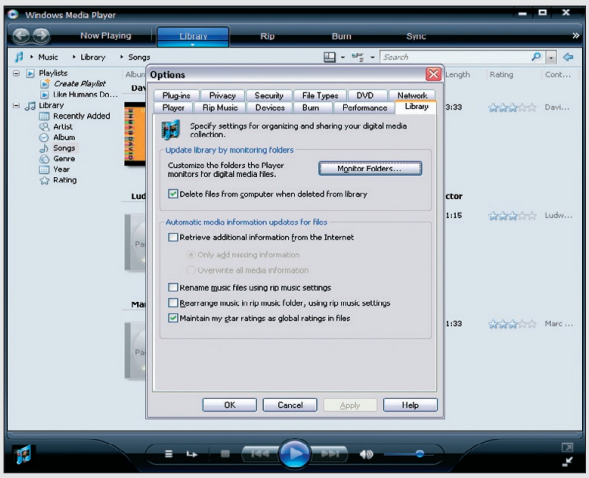
Felügyeleti vonatkozásai miatt itt jelentették be a Microsoft Exchange Server 2007-et, ami több szempontból is menedzselési mérföldkőnek számít. Egyrészt ez lesz az első olyan Microsoft-alkalmazás, amely a PowerShellen alapuló, új automatizáló képességekkel rendelkezik. Másrészt a felügyeletét ellátó Exchange Management Console grafikus felülete teljes egészében az MMC 3.0-ra, funkcionalitása pedig a PowerShellre épül.

Az Exchange 2007 egyébként is jó példája a Microsoft felügyeleti termékeiben is megnyilvánuló markáns „server systemes” filozófiájának, hiszen ez is egy modulokból felépülő integrált szoftverként az IT-műveletek alapstruktúráját biztosítja. A Server System-termékek és -modulok integrációja javítja a kezelhetőséget és a biztonságot, illetve csökkenti a komplexitást és a költségeket. A más platformokkal való együttműködés érdekében minden megoldás támogatja a nyitott ipari szabványokat – hangsúlyosan ideértve az XML-t és a webszolgáltatásokat.

Kelemen László

Sarkos újítások

A Windows Media Player 11 fejlesztői kódnevének megfelelően — Polaris — gyökeres újításokat hoz az eddigi változatokhoz képest; elsősorban a kezelhetőségében. A Windows XP-hez szánt verzió a Vista-kiadásnál valamivel kevesebbet tud, de a bétaváltozatból nyilvánvaló, hogy senkinek sem lesz oka panaszra.



Gyökeres újítások a kezelhetőségben

A „Word Wheel” funkció, a rangsorrendszer és az előnézeti képeken alapuló grafikus felület miatt gyors és egyszerű a keresés a médiatárakban.

A külső eszközök és az internet integrációja egyébként is központi szerepet kapott. Már most száznál is több eszköz felel meg a lejátszó PlayForSure specifikációjának. Ezekkel nemcsak a tartalmak szinkronizálása gyerekjáték, hanem az állományok másolása közben a lejátszó automatikusan elvégzi az eszköz képességeinek megfelelő konverziókat. Az internetközelség példája az MTV együttműködésével május közepétől elérhető Urge szolgáltatás, amelynek köszönhetően kétmilliónál is több szám közül lehet majd válogatni.

Az XP-s kiadás végleges változata nyártól lesz elérhető.

WinHEC: második bétaváltozatok

Idén május 23. és 25. között Seattle-ben rendezte meg a Microsoft a WinHEC-et (Windows Hardware Engineering Conference), ahol a hagyományosan mély, szakmai előadások mellett – mint minden évben – ezúttal is egy sor jelentős bejelentésre került sor.

Az idei WinHEC-en jelentették be mind a Windows Vista, mind pedig az Office 2007 és a „Longhorn" Server második bétaváltozatát. A Vista és az Office bétáihoz június legelejétől bárki hozzájuthat, és a jelenlegi információk szerint továbbra is tartható a végső megjelenés időpontja mindkét termék esetében. A „Longhorn" Server azonban továbbra is zárt bétaprogram keretében lesz elérhető.

Szerverbejelentések

A legérdekesebb bejelentések a szerverplatform környékén történtek. *Bob Muglia*, a szerverüzletág vezetője elmondta, hogy a „Longhorn" Server (végleges neve még nincs a szoftvernek) 2007 második félévében érkezik meg, és ezt megelőzi még egy harmadik bétaverzió ez év végén. Mostantól a „Longhorn" Server konkrét képességeiről is egyre több szó esik majd. Ami már tudható, hogy a szerver még inkább szerepkör alapú lesz, ezenkívül elérhető lesz belőle egy grafikus felhasználói felület nélküli változat, a „Longhorn" Server Core, ami gyakorlatilag egy parancssorból vezérelhető Windows Server. A Microsoft elemzései szerint egy ilyen, GUI nélküli operációs rendszer patchelési igénye közel 60–70 százalékkal csökken, azonban egy ilyen szerver csak bizonyos szerepkörök futtatására lesz képes.

Ugyancsak konkretizálódott végre, hogy mikor és milyen formában számíthatunk a hypervisor alapokon nyugvó virtualizációs technológiára. Az első, csak zárt körben, partnerek által tesztelhető béta ez év végén lesz elérhető, a kész szoftvermodul pedig 90 nappal a „Longhorn" Server végleges verziójának megjelenése után érkezik, Windows Virtualization néven. Magát a hypervisor-stacket nagyon picire és hatékonyra sikerült megírni, az egész réteg mindössze 100 kilobájt körüli méretű lett.

Mozgatás, finomhangolás

Ehhez kapcsolódik, hogy hivatalosan is bejelentették – a korábban már egyszer kiszivárgott – System Center Virtual Server Manager; ez a virtualizált operációs rendszerek automatizált, aktuális teljesítménytől, terheltségtől és az igényektől függő mozgatására, finomhangolására lesz képes. Ugyanennek a szoftvernek köszönhetően a virtuális gépeket nagyobb adatközpontokban is kényelmesebben tudjuk használni.

Az is kiderült, hogy a Windows Deployment Services – a kliensek tömeges telepítésére alkalmas technológia legújabb változata – még a „Longhorn" Server megjelenése előtt, a Windows Vistával együtt fog megérkezni, hogy már ekkor kényelmesebb legyen az átállás az új kliensoldali operációs rendszerre.

Budai Péter

Egészségesebben a technológia segítségével

A fenti gondolat jegyében Magyarországon idén 5 intézmény 9 csapata mérte össze tudását a szoftverfejlesztés kategóriában. A legjobbnak a Budapesti Műszaki és Gazdaságtudományi Egyetem „Digital Mania" csoportja bizonyult. A Pocket PC-re épülő, mozgássérülteket segítő megoldásnak köszönhetően a *Jakab Emese, Kapui Ákos, Zöld László* és *Rátkai Zoltán* alkotta négyes képviselhette hazánkat a Mariborban rendezett közép-kelet-európai regionális döntőben.

A 13 diákcsapatból háromnapos versengés után végül a szlovén csapat került ki győztesen.

„Az idén bemutatott ötletek és újítások lenyűgöztek minket – nyilatkozta *Wilfried Grommen*, a Microsoft EMEA üzleti stratégiáért felelős igazgatója. – A 2006-os Imagine Cup régiós döntője ékes bizonyítéka annak, hogy a régió országai képesek olyan innovatív megoldásokat alkotni a szoftver adta lehetőségek segítségével, amelyek később globálisan is felhasználhatóak lesznek, hogy jobbá tegyék az emberek életét."

A Microsoft jövőre is megrendezi a szoftverfejlesztés mellett négy másik kategóriát felölelő Imagine Cup versenyt. A 2007-es vetélkedősorozat az oktatásra koncentrál; a döntőt a dél-koreai Szöulban tartják.

Windows Vista: ahogy a felhasználó látja

Az új asztali operációs rendszer nemcsak az adminisztráció terén nyújt többet, hanem a mindennapi felhasználást is egyszerűbbé teszi – még a rendszergazdák számára is.

A 2006 második felében megjelenő Windows Vista csillogó-villogó felületével rögtön kiváltotta az informatikusok ellenszenvét, akik korábbi tapasztalataikból úgy gondolták, hogy a tetszetős külsejű operációs rendszer funkcionalitásban számukra lényegesen kevesebb újat fog nyújtani. Ebben a cikkben arra keressük a választ, hogy miért érdemes egy rendszergazdának lecserélnie Vistára saját számítógépének operációs rendszerét.

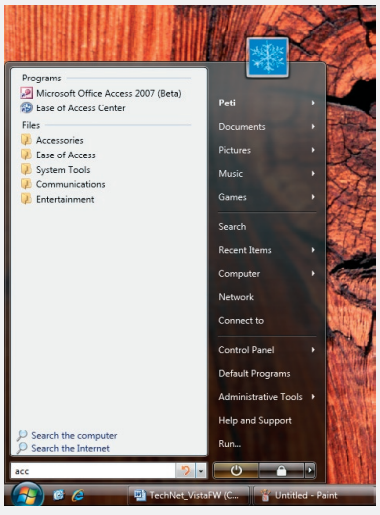
Az alább felsorolandó új képességek mind-mind azt a célt szolgálják, hogy munkánk hatékonyabb lehessen, virtuális munkakörnyezetünk pedig még inkább hozzánk idomuljon. Emellett természetesen a szórakozásra is szüksége van az embernek.

Az információk kezelésének új módjai

Az információs társadalom fejlődésével magunk is infomunkásokká váltunk, számítógépünkön és a hálózaton egyre több és több adatot tárolunk, rendszerezésük és az adattömeg kezelése egyre több értékes időt vesz el az életünkből. A Vista több funkcióval is meggyorsítja a megfelelő információk előkeresését. Ide tartozik többek között az integrált keresőmotor, a kulcsszavak és az értékelés használatának lehetősége, az új intézői nézetek, valamint a virtuális mappák.

Integrált keresés

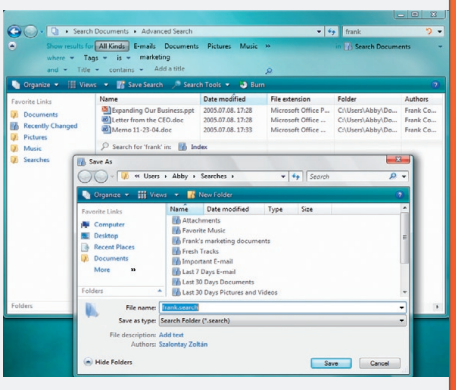
Eddig is tudtunk keresni az adataink között, azonban ez egyrészt idő-, másrészt teljesítményigényes volt (elvégre a teljes merevlemezt átnézni nem megy két perc alatt). Sok szakember számára ismerős lehet a Windows indexelő szolgáltatása, azonban eddig nem volt teljesen világos, hogy mikor és mire használható hatékonyan. A Vistával a keresés a lehető legjobb helyre kerül, közvetlenül a Start Menübe. Ez a kis szövegdoboz egy, akár a teljes számítógépet átnézni képes keresőmotort takar, amely pillanatok alatt „túrja elő” az indexből az általunk keresett tartalmakat (legyen az akár egy Word-dokumentum, egy e-mail vagy esetleg egy zeneszám), mindezt ízlésesen rendszerezve és megjelenítve, a fájl helyétől függetlenül.



Keresés a Start menüben

Kulcsszavak

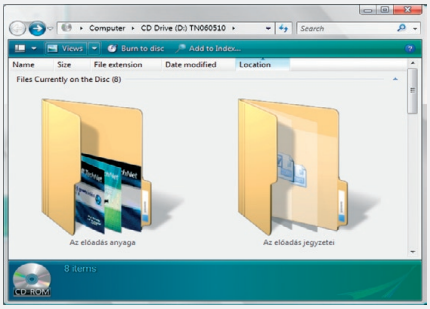
Van, amiben a Vistába épített technológiák többet nyújtanak az eddig külön elérhető szoftvereknél (mondjuk, a Windows Desktop Searchnél): lehetőség van például kulcsszavak használatára. Kulcsszavakat bármely állományhoz tetszőlegesen hozzárendelhetünk (akár már az új mentési dialógusablakokban is), és ezek után a fájlokra nemcsak a korábbi paramétereik (név, hely, méret stb.), hanem az általunk hozzárendelt kulcsszavak alapján is lehet keresni.



Az új intéző

Virtuális mappák

A másik új összetevő a virtuális mappa. Ezek a speciális könyvtárak (hasonlóan az Outlook 2003 keresőmappáihoz) az általunk meghatározott feltételeknek megfelelő fájlokat rendezik egy mappanézetbe. Természetesen amennyiben a feltételeknek megfelelő új fájl kerül a merevlemezre, az is rögtön elérhető lesz ebben

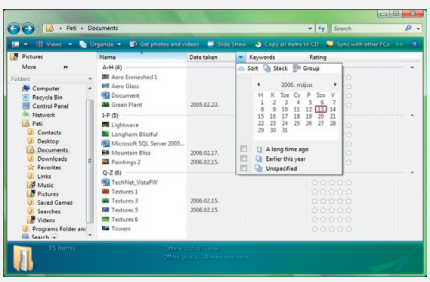


A mappák előnézete

a mappában. Mindez úgy történik (hála a keresőmotor indexelésének), hogy a fájl fizikailag nem „mozdul” a helyéről. (Érdekesség: A virtuális mappák fizikailag mindössze egy XML-fájl formájában léteznek, amely tartalmazza a szűrt keresés végrehajtásához szükséges paramétereket, ezért ezeket tetszőlegesen módosíthatjuk, használhatjuk akár több gépen is.)

Intézőnézetek

A Windows Intéző az az alkalmazás, amit szinte az összes létező tartalomtípus böngészésére használunk (prezentációk, képek, zenék), viszont eltérő típusú tartalmaink más és más beállítást, illetve nézetet igényelnek. Már a Windows 2000 is tartalmazott nézeteket a fájlok könnyebb átlátása céljából, azonban a Vista másképp közelíti meg a rendszer működésének ezt a részét. Az eddigi, egyesek számára komplikált és kötött nézetek helyett



Szűrés és rendszerezés az intézővel

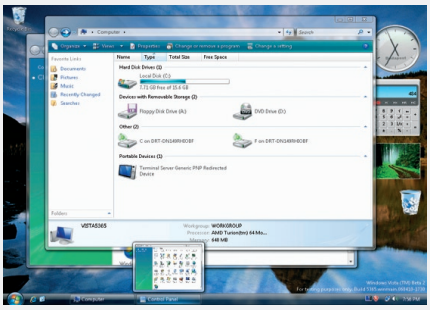
(amelyeket eddig a Nézet menüből értünk el) egy új, dinamikus csúszka kapott helyet az intézőben, segítségével menet közben változtathatjuk a nézetet és az ahhoz kapcsolódó paramétereket (ikonok mérete stb.).

Az intézőben gyakorlatilag bármilyen csoportosítást és rendezést megvalósíthatunk, sőt arra is lehetőség van, hogy úgynevezett halmokat hozzunk létre a megadott csoportosítások szerint. Ezek a halmok azt mutatják, hogy a megadott feltételeknek nagyságrendileg hány állomány felel meg. A Windows Vistában a könyvtárak ikonján azt is láthatjuk, hogy milyen típusú állományok találhatók benne a legnagyobb számban, illetve megjelennek azok előnézetei is.

Aero Glass és Aero Express

A Windows felhasználói felületének újdonságai előtt fontos megemlíteni azt, hogy az újdonságok egy része csak az új felülettel kompatibilis videokártyákkal működik (ilyen képesség például az Aero Glass, a flip 3D és a taskbar-előnézet). A kártyával szemben támasztott követelmény a legalább 64 megabájt videomemória, és a teljes DirectX 9-kompatibilitás, beleértve a pixel shader 2.0 támogatását is.

Mindenesetre az Aero (a Glass és az Express is) megszünteti a legtöbb korábbi grafikus problémát, például az ablakok és a háttér újrarajzolásáért immár a grafikus kártya GPU-ja és nem a rendszer felel. Mostantól az Aeróban gyakorlatilag minden ablak egy 3D-s felület, szinte egy textúra, aminek a mozgatását és transzformálását a DirectX és a grafikus



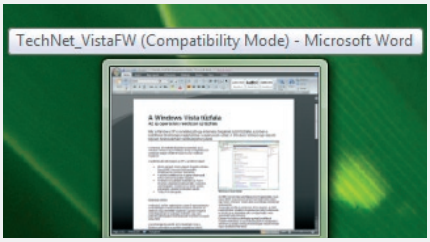
Az Aero Glass felülete

kártyák már nevetve meg tudja oldani, csakúgy, mint a leglátványosabb játékok esetében.

Azokon a rendszereken, amelyek nem rendelkeznek megfelelő hardverrel, az úgynevezett Aero Express felület használható. Az Express esetében szinte csak a látványosabb, pixel shadereket megmozgató effekteket kell nélkülöznünk, ami rendszergazda szemmel nézve nem is biztos, hogy baj. Hozzá kell tenni ugyanakkor, hogy az Aero Glass áttetsző felülete kifejezetten megnyugtató lehet, és pszichésen valóban jobb érzés használni a vele felszerelt rendszert, azonban természetesen ez az első funkció, amit egy informatikus kikapcsol, ha egy kicsit is lassul miatta a gépe (de egyébként megfelelő grafikus hardver esetén ez nem szokott gondot okozni).

Előnézetek, taszkváltás, flip 3D

Ezentúl az ablakok között úgy válthatunk, hogy a megfelelő kiválasztása előtt megtekinthetjük annak tényleges felületét (és a DirectX-nek hála, az kicsiben is pontosan úgy néz ki, és akár mozog is, mint az eredeti ablak tartalma). Ezáltal könnyebben lehet majd például 15 intézőablak közül kiválasztani a nekünk szükségeset. Ez a megoldás két helyen



A taszkok előnézete

jelenik meg, egyrészt a tálcán, az ablak ikonja fölé tolva az egeret, másrészt az új, Alt-Tab-ra előbukkanó ablakban.

Ezt egészíti ki a Windows+Tab gomb megnyomására előcsalogatható flip 3D: a térben egymás mögött elrendezve, eldöntve láthatjuk az ablakainkat. Az ablakok között a kurzorbillentyűkkel tudunk váltani. Az RC1 verzióra azt ígérik, hogy az ablakok szélén már élsimítást is alkalmazni fognak. Még ha nem is fogjuk mindennap használni ezt a funkciót, mégis jól szemlélteti, mire is képes a Windows Vista új grafikus alrendszere.

Windows Sidebar

A Windows Vista talán egyik legérdekesebb újdonsága a Windows Sidebar, ami (beállításától függően) folyamatosan a képernyő jobb oldalán csücsül. A Sidebar meghatározott, XML-re és más, elterjedt webes technológiákra épülő mini-alkalmazások („gadgetek”, kütyük) futtatására képes. A Sidebar segítségével a számunkra fontos adatokat mindig szem előtt tarthatjuk – legyen szó akár hírekről, meccseredményekről, vagy a kedvenc családi fotóinkról – anélkül, hogy minden egyes

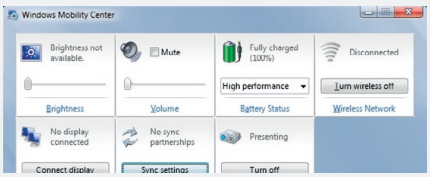
információért egy új böngészőablakot vagy programot kellene nyitnunk.

A Vista már eleve sok beépített kütyüvel érkezik (például slide show képekből, számológép, jegyzettömb, világóra, RSS-olvasó), de semmi sem akadályoz meg minket abban, hogy saját alkalmazásokat fejlesszünk erre a platformra, amelyről a http://microsoftgadgets.com/Build/ címen találhatunk további információkat. Szintén itt böngészhetünk a többiek által már elkészített alkotások között.

Úton: Windows Mobility Center

A hordozható számítógépet használók eddig a laptopokra jellemző, gyakran elvégzett beállításokat (energiagazdálkodási profil, képernyő fényereje, WLAN-kapcsolatok stb.) külön-külön alkalmazásból tudták csak módosítani. A Windows Mobility Center egy helyre fogja össze ezeket a beállításokat.

Újdonságnak számíthat a kapcsolódás a külső projektorra (vezetékes vagy vezetéknélküli kapcsolaton keresztül akár az interneten



Mobility Center

át), valamint a Presentation Settings használata. Ennek a segítségével egy kattintásra tüntethetjük el a személyes háttérképünket, és állíthatjuk vissza a Windows alapbeállításait, valamint kikapcsolhatjuk a képernyővédőt is, hogy egy prezentáció során semmi se zavarhasson minket. Az előadás után ugyancsak egy klikkre térhetünk vissza az eredeti, jól megszokott állapothoz.

Energiagazdálkodás

Ugyancsak újdonságnak számítanak a megújult energiaprofilok. Eddig ezek a beállítások arra terjedtek csak ki, hogy például menynyi idő múlva kapcsoljon ki a monitor, vagy mikor álljon le a merevlemez. A Windows Vista új energiaprofiljainak segítségével feláldozhatjuk a teljesítményt az energiakapacitás oltárán, ugyanis lehetőségünk lesz arra, hogy a „Power Saver" profil használatával a Windows intelligensen „visszafogja" az eszközök teljesítményét, ezzel csökkentve az energiafelhasználást, mindezt szinte észrevehetetlenül, munkát nem akadályozva. Jelentős, akár 25–30 százalékos üzemidő-növekedés érhető el. A Vista ezen túlmenően folyamatosan átmenetet ígér az egyes teljesítményszintek között.

Sync Center

Nagyon gyakran van szükségünk adatokra, melyek a vállalati hálózaton vagy mobileszközeinken (mobil, pendrive, egyebek) találhatók. Eddig (jobb esetben) a Windows XP-ből ismert szinkronizálási funkciót használtuk, amely sajnos átláthatatlanná vált több szerver, több PC, illetve eszköz használata esetén.

A Windows Vista új Sync Centere egyszerre segít áttekinthetően nyomon követni a szervereken, a többi hálózatra kötött számítógépen, valamint a hordozható eszközeinken lévő adatok állapotát és frissességét. Ezenkívül jelzi a szinkronizáció állapotát és az esetleges ütközéseket/problémákat. A Sync Center egyben kiváltja az eddig külön telepítést igénylő ActiveSyncet is.

Windows Collaboration

Ha azonnali fájlcserére van szükségünk, akkor általában a mappák megosztását szoktuk használni, azonban ez egyrészt kényelmetlen lehet, másrészt nem mindig a lehető legbiztonságosabb.

Gondoljunk csak arra, hogy egy másik számítógéppel állományokat megosztva szükségünk van:

- a gépnévre;
- a megosztás nevére;
- egy felhasználónévre és egy jelszóra (amit esetenként nehézkes létrehozni, főleg ha nem azonos tartományban van a két számítógép);
- egy kis szerencsére.

A Windows Collaboration segítségével egyszerűen hozhatunk létre ad hoc wireless hálózatokat, és így könnyedén cserélhetünk adatokat akár 25 felhasználóval/laptoppal egyszerre. A funkciók között a fájlcserén és a dokumentumok közös szerkesztésén kívül a chat, az alkalmazásmegosztás valamint a távsegítség is szerepel. Ráadásul ehhez domén, vagy munkacsoport létrehozására sincs szükség, mindössze hálózati kapcsolatra.

Nincs szükség sem az IP-cím megadására, sem gépnévre, a Windows Collaboration a hálózaton automatikusan megkeresi és kijelzi nekünk az elérhető sessionöket. Az adatok biztonságát a wireless titkosításon túl egy jelszavas védelem is szavatolja, hogy csak az csatlakozhasson a közös munkafelülethez, akit valóban szeretnénk.

Multimédia

A Media Center funkcióinak segítségével lehetőségünk van tv-adásokat nézni (tuner kártyával), ezeket az adásokat rögzíteni, valamint egy elektronikus programajánló (Electronic Program Guide, EPG) segítségével tv-műsort is kapunk hozzá.

Az opcionálisan megvásárolható Media Center Extendernek köszönhetően a számítógépünk képernyőjén kívül akár tv-készülékünkön is élvezhetjük a teljes médiatárunkat vagy az élő tv-csatornákat.

A Media Center eddig csak a Windows XP Media Center Edition részeként volt elérhető, azonban a Vista megjelenésével ez a verzió megszűnik, és a funkció a Home Premium, valamint az Ultimate verziókba kerül át.

Adatainkat ezentúl nemcsak cd-re, hanem dvd-re is egy kattintással írhatjuk ki, és a Vista arra is lehetőséget nyújt nekünk, hogy képeinket valamint videóinkat dvd-video formátumra alakítsuk át. Mindehhez rendelkezésünkre állnak megfelelő effektek, valamint egy teljes menürendszer is.

Media Center

Digitális fényképeinket egy egyszerű, könnyen áttekinthető, ámde professzionális alkalmazásból kezelhetjük, ez azt teszi lehetővé, hogy a fotókat például kulcsszavakkal, úgynevezett tagekkel lássuk el, majd ezek alapján a képeket később egyszerűen, akár a Start menüből, akár a Windows Photo Gallery alkalmazásból hívjuk elő. Természetesen emellett retusálásra is lehetőségünk van, többek között a vörösszem-effektus eltávolítására, a képek vágására, és akár webre is optimalizálhatjuk képeinket.

Moldova György

A RENDSZERGAZDA SZEMÉVEL

Az eddig felhalmozott tapasztalatok és a rendelkezésre álló információk alapján nyugodtan kijelenthető: a Windows Vista sok kellemes meglepetést tartogat a rendszergazdák, üzemeltetők számára is.

Üzemeltetői vonatkozásban a Windows Vista újdonságainak jelentős része a minden körülmények között fontos biztonsággal kapcsolatos. Itt kell megemlíteni például az UAC-t (User Account Control), ami a felhasználói (és rendszergazdai) hozzáférés korlátozását jelenti; a Security Centerbe beépült kém-, illetve reklámprogramok elleni eszközöket; az új tűzfalat, ami egy sajátos megközelítés alapján működik például a kifelé haladó forgalom ellenőrzésének tekintetében (http://tinyurl.com/hvtwt). Fontos újdonság a NAP (Network Access Protection) is – ez a VPN-karantén mintájára a helyi hálózati hozzáférést kontrollálja –, és szó eshetne a Windows Defender, az IE7 vagy a Windows Mail biztonsággal kapcsolatos új vagy megújult szolgáltatásairól. Mivel mindezeket e lapszámunk egy másik írása tekinti át, joggal merül fel a kérdés: mi marad? Egyáltalán nem kevés, nézzük tehát először a szintén fontos, hibajavítással és diagnosztikával kapcsolatos elemeket.

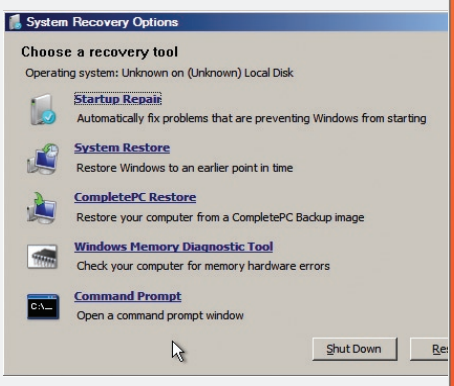
Hibajavítás és diagnosztika

Automatic Recovery. Windows XP-nél egy komolyabb alkalmazás- vagy szerviz-/processzhiba esetén mindig garantáltan szükségessé vált az újraindítás. A Vistában a legtöbb ilyen esetben nincs erre irányuló kiváltó ok, az operációs rendszer automatikusan, a felhasználó értesítése nélkül megpróbálja helyrehozni a hibát, azaz például újraindítani a kérdéses szolgáltatást (a függő szervizekkel egyetemben), a gép újraindítása nélkül. A javítási körben olyan rendszerszintű alkalmazások is benne vannak, mint például a Windows Explorer vagy az IE. Az úgynevezett Restart Manager másik előnye a különböző külső alkalmazások telepítése (vagy például a Microsoft/Windows Update használata) után szükséges újraindítások számának csökkentése, bár ennek az opciónak az eredményessége nem csak a Vistán fog múlni.

Diagnosztika. A Vista több, a háttérben elbújva működő ellenőrzést is végez, többek között a merevlemezzel vagy a memóriával kapcsolatban. Az előbbi esetén a Windows Disk Diagnostics detektálja a lemezhibákat, és értesíti ezekről a felhasználót, majd bevonja a szintén teljesen új Windows Backupot is a mentésbe. A RAM-hibák kiszűrésére immár beépített eszköz szolgál, vagyis ha valamilyen módon kiderül egy ilyen probléma (például észleli a Windows Error Reporting), akkor a Vista felajánlja ezt a vizsgálatot azonnal, vagy a következő újraindításra ütemezve. De manuálisan is elindíthatjuk bármikor az eszközt, például a Windows Boot Managerből (nem a boot-menüből). Háromféle, egyre keményebb módszerekkel dolgozó tesztelési üzemmódja van, és a ciklikusságot, illetve a gyorsítótár használatát is szabályozhatjuk.

Startup Repair Tool. A Vista ezen a néven tartalmazza a Recovery Consol utódját, amely azonban funkcionalitásban és „kézreállásban" jóval többet nyújt, mint az annak idején egyébként valóban forradalminak számító RC. Az eszköz a Vista DVD-n található, manuálisan is elindíthatjuk, de ha egy indítási hiba jelentkezik, teljesen automatikusan elindul, detektál és javít. Mit? Eszközmeghajtó-hibákat, a hiányzó vagy a hibás rendszerindítási konfigurációt vagy a meghibásodott lemezeket. A javítás után természetesen naplózza az eseményt. Manuális indítás esetén innen is elérhetjük a memória-ellenőrző alkalmazást vagy például a System Restore-t.

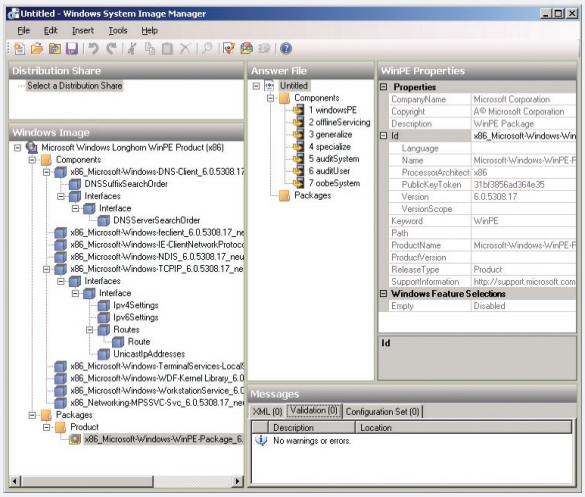
Nem kevésbé fontos terület a telepítés – és különösen a nagyobb hálózatokban alkalmazandó sokszoros telepítési formák – témaköre. A RIS, az ADS, az Xpe technológiák



Hibajavítási lehetőségek manuális indítás esetén

és image-ek után egy újabb, az SMS-ben már némileg megismert formátum a WIM (Windows Imaging Format) az, amelyet a Vista tömeges telepítésénél használhatunk. Néhány fontos jellemzője:

- állomány alapú, hardverfüggetlen image;
- „izmos” tömörítés – a RIS-ből ismerős duplikált állománytárolási forma, valamint az LZX (a nagy állományokhoz) vagy az Xpress (a gyors tömörítéshez) tömörítési algoritmus használata;
- szeletelhető (.SWM) és rendszerindításra is alkalmas formátum, amelyben ráadásul lehetőség van több image egy állományban való tárolására;
- offline kezelés, azaz bővíthető/szűkíthető tartalom (praktikusan driverek, frissítések stb.) új image készítése nélkül;
- maradhatnak állományok a célköteten, mivel ennek a formátumnak a használata előtt vagy használata során nem szükséges törölni az adott kötetet.



Egy image a Windows System Image Managerben

A Vistában egy speciális alkalmazás, a Windows Automated Installation Kit (WAIK) részeként elérhető Ximage áll a rendelkezésünkre a .WIM-ek kezeléséhez, amelynek alapvető műveletei (például APPEND, APPLY, CAPTURE, DELETE, DIR, EXPORT, INFO, SPLIT, MOUNT(RW), UNMOUNT stb.) a parancssorból adhatók ki (tehát GUI-eszköz nincs). Az Ximage persze WinPE alól is használható lesz.

Természetesen a WIM támogatása széleskörű lesz, a Vista setupján kívül natívan támogatja a Windows Deployment Services (amelyet a RIS utódjának szánnak, és ismertetése külön is „megérne egy misét”), valamint az SMS v4 is.

A WAIK majdnem teljesen ugyanazokból az összetevőkből áll, mint a korábban a rendszerépítők által használt OEM Preinstallation Kit (OPK) utódja, azzal a különbséggel, hogy most már az üzemeltetők számára is elérhetővé válik, és akár a hálózaton keresztüli telepítést is elvégezhetjük vele (viszont a WinPE hiányozni fog a csomagból).

Fontos tudnivaló továbbá az előtelepítések témájában, hogy a Vistában és a „Longhorn” Server esetén egyaránt lényeges szempont volt a moduláris felépítés, azaz a telepítőeszközökkel (például majd a képen látható Windows System Image Managerrel) nagyon részletesen szabályozhatjuk, hogy mely komponensek kerülhessenek fel a végleges rendszerbe.

A harmadik – rendszergazdák számára szintén hangsúlyos – témakör a már működő operációs rendszerek központi kezelése, az események naplózása, illetve az automatizálás.

A WFP utódja

A Vistában a Windows Resource Protection (WRP) technológia lesz hivatott arra, hogy a rendszerállományok, rendszermappák és a regisztrációs adatbázis védelmét megoldja, azaz a nemkívánatos – akár szoftveres, akár a felhasználó által tett – változási kísérleteket negligálja. A WRP biztosítja, hogy csak az elvileg megbízható Windows Installer legyen képes változtatni a felsorolt elemeken.

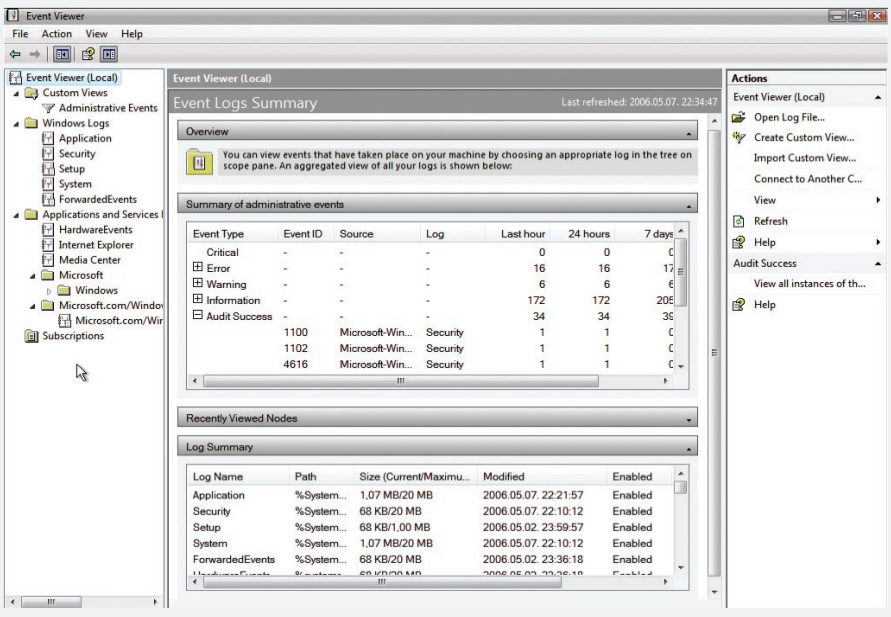
Eseménynapló

A különböző események leírása a Vistától kezdve változik, hiszen az XML-formátumba történő naplózás több és jobban követhető információ tárolását teszi lehetővé. Ezenkívül van még egy fontos újdonság, ugyanis a Task Managerrel karöltve az Event Viewer automatikusan képes eseményfüggő taszkokat futtatni. Az Event Viewer egyébként ezt a lehetőséget leszámítva is erősen megváltozott, lehetőségünk van például központosítani (átirányítani) a naplózást, emellett bonyolult, többszörös lekérdezéseket is végrehajthatunk, illetve nagyon látványos és sokatmondó nézeteket faraghatunk a képernyőnkre.

Automatizálás

Az unalmas, ismétlődő feladatok elvégzése helyett a Vistában számtalan feladatot automatizálhatunk a következő komponensek segítségével.

- Minden lényeges dolgot, amit a GUI-n elvégezhetünk, megtehetjük a parancssorból is, mert az XP-hez képest megint emelkedett a parancsok száma.
- Task Scheduler – felhasználófüggő taszkfuttatás, szimultán futtatás vizsgálata, auto-



Statisztikaözön az Eseménynaplóban

matikus taszkfuttatás az üresjáratokban, beállítható verziófüggőség, a futtatási jogosultságok címtárban tárolása (nem gond többé a jelszóváltozás követése) – mindmind új opció!

- Web Services for Management (WS-Management) – az R2-ben debütáló ipar szterderd, a távoli hardver-, illetve szoftvereszközök kezeléséhez, vagyis a Vista hálózaton keresztüli üzemeltetéséhez (szkriptek, ellenőrző szoftverek stb.).

Csoportházirend

Egy Windows-tartomány esetén ma talán a csoportházirend az egyik leghatékonyabb beépített eszköz a felhasználók, számítógépek és a különböző erőforrások kezelésére, „megfékezésére", illetve az egységes beállítások központi elvégzésére.

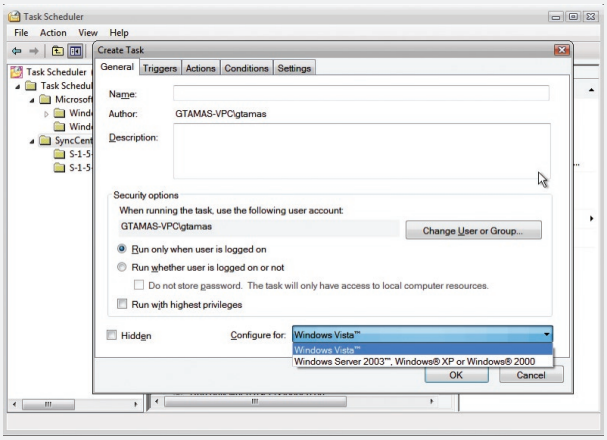
Ezen a területen több változás elé is nézünk a Windows Vista–„Longhorn" Server páros bevezetésével, akár a szabályozható területeket, akár a csoportházirend elemeinek felépítését vagy pedig a sablonok disztribúcióját vizsgáljuk meg.

Kompatibilis lesz? Az új Vista–„Longhorn" Server alapú házirendszabályokat csak ezek alól az operációs rendszerek alól fogjuk tudni szabályozni, mégpedig a Vistába már gyárilag beépített GPMC-vel (Group Policy Management Console). Mivel megjelenik az újfajta sablon (.ADMX), és bizonyos elemek csak ezekből a sablonokból érhetők majd el, ezért muszáj minimum egy Vistáról futtatni a GPMC-t.

De természetesen visszafelé kompatibilisak, így a Windows 2000-ig minden .ADM állomány használható, és nemcsak a gyáriak, hanem az általunk farigcsáltak is. Igazából jelenleg úgy tűnik, hogy a mindennapokban semmit nem fogunk észlelni a csoportházirend használata közben abból, hogy megváltozott a házirend elemeinek felépítése. Amit viszont még tudnunk kell: a csoportházirend nem támogatott minden Vista verzión, hanem csak a következőkön:

- Windows Vista, Small Business Edition;
- Windows Vista, Professional Edition;
- Windows Vista, Enterprise Edition;
- Windows Vista, Ultimate.

ADMX? A Vista–„Longhorn" Server páros esetén is registry alapúak a beállítások, de a standard, az NT4 óta meglévő .ADM (Administrative Templates) állományok XML formátumú, úgynevezett .ADMX kiterjesztésű sablonokra változnak. Ezzel együtt több lehetőség birtokába jutunk, például a különböző nyelvű kliensváltozatok jobb kezeléséhez. Az .ADMX állományok ugyanis két részre „vághatók", egy semleges és egy nyelvspecifikus részre. Ez azt is jelentheti, hogy a rendszergazda a saját angol nyelvű Vistájáról elkészíti az adott GPO-t, majd elmenti a több országra kiterjedő, központi tartományi házirend alá. Egy másik országban, egy másik nyelvű kliensről megnyitva ugyanezt a házirendet, a másik nyelven lehetséges megtekinteni a beállításokat. Ha ezen a nyelven módosítanak a beállításokon, azt az eredeti helyen szintén angolul látja majd az üzemeltető.



Opció opció hátán

A formátumváltással együtt járó másik előnyös változás az .ADMX állományok tárolására vonatkozik. Eddig minden egyes GPO-hoz külön-külön tárolódott el az összes .ADM állomány. A Vistától kezdve egy tartományszintű, közös tárolóhely jön létre a Sysvol megosztáson belül ([sysvol]\policies\policydefinitions), és innentől az összes GPO ebből az egy példányból fog „táplálkozni", így tehát csökken a Sysvol mappára nehezedő nyomás (és persze a replikációs forgalom is).

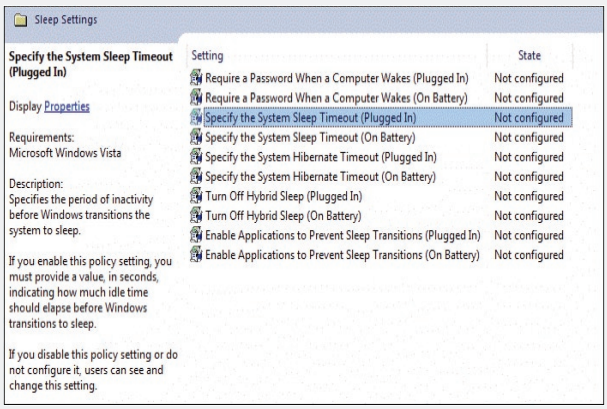
Néhány érdekesebb új házirend-hatókör

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

Blocking Device Installation. Központilag, a Csoportházirenden keresztül tilthatóvá válik az USB-meghajtók, a CD-RW, DVD-RW és egyéb eltávolítható média használata. Írási és olvasási hozzáférés-típusok közül választhatunk, számítógépre, illetve felhasználóra is korlátozhatunk. TS esetén csak számítógépre lehet majd szabályozni.

Assigning Printers Based on Location. Szintén teljesen új lehetőség a nyomtatók szervezet, illetve földrajzi alapon történő hozzárendelése, azaz megtehetjük azt, hogy egy adott nyomtatót egy telephelyhez rendeljünk.

Ha egy mobilfelhasználó érkezik a telephelyre, minden további nélkül „megkaphatja" az adott helyen lévő nyomtatókat. Ha pedig visszatér az eredeti helyre, akkor újra az eredeti nyomtatókat fogja feltelepítve látni.



Felhasználónként és gépenként is szabályozható lesz

Delegating Printer Driver Installation to Users. A rendszergazdák ezután képesek lesznek nyomtató-drivereket is telepíteni a házirendből. Ez egyrészt lehetővé teszi, hogy csak kifejezetten a megbízható driverek kerüljenek fel a gépekre, másrészt nem lesz szükség az idevágó jogok delegálására.

Gál Tamás

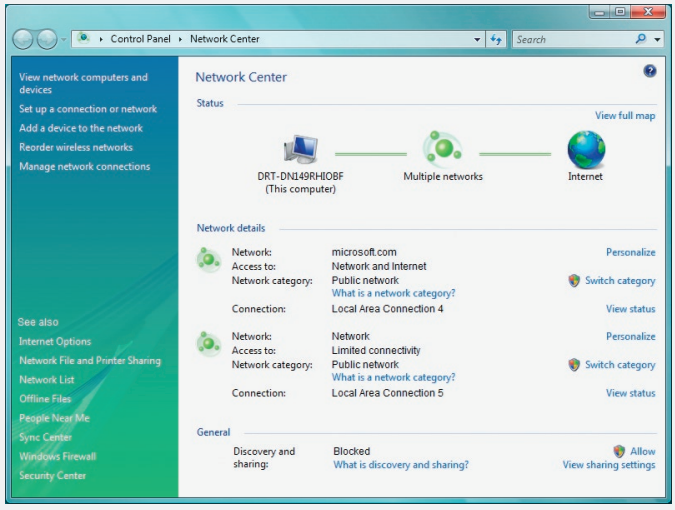
A Windows Vista hálózatkezelési rétege

A Windows Vistában jelentősen megújult a teljes hálózatkezelési réteg, beleértve a TCP-stacket és az azt kiegészítő felhasználói felületen és parancssorból elérhető eszközöket is.

Az új megoldások fejlesztésekor nagy hangsúlyt fektettek a modularitás biztosítására, ezáltal egyszerűbbé válik mind a Microsoft, mind a partnerek számára a hálózati réteg képességeinek bővítése, javítása. Az új stack mindezek mellett teljesítményben is lekörözi a korábbi változatot, lényegesen egyszerűbbé teszi a felmerülő hibák feltárását és megoldását, valamint csökkenti a DoS-támadások lehetőségét.

Network Center, Network Map

Az első szembetűnő újdonság, ha a felhasználói felületről, pontosabban a hálózati kapcsolatok és a vezérlőpult irányából közelítjük meg a Vista új hálózati lehetőségeit, hogy teljesen átalakult a korábbi, mindössze a hálózati adaptereket és azok tulajdonságait mutató ablak. Az új, Network Center névre hallgató felület egy központi helyen ad lehetőséget arra, hogy adaptereinket és alhálózatainkat igényeinknek megfelelően beállítsuk.



A Network Center

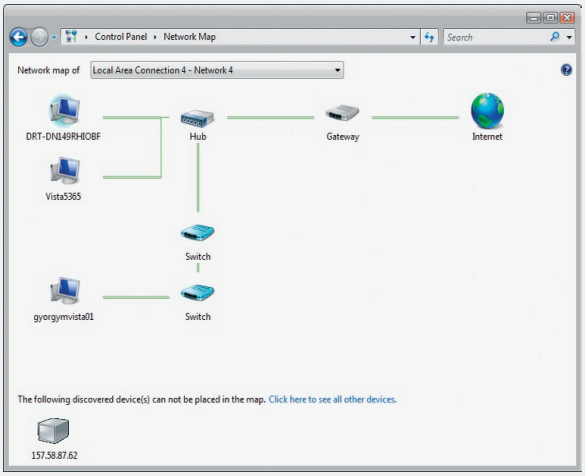
Néhány gyors kattintás után elérhető a Network Centerről a Network Map, ami gyakorlatilag a körülöttünk található hálózati infrastuktúra lenyomata, ahogy azt az adott adapter az általa fogadott, alacsony szintű hálózati protokollok csomagforgalma alapján látja. A Vista képes vizuálisan ábrázolni, hogy milyen routeren, gatewayen, illetve switchen keresztül kommunikálunk a környezetünkkel, és a szomszédos gépek, illetve a kommunikáció biztonsági beállításainak függvényében akár az ezekre az eszközökre kötött további számítógépeket is láthatjuk rajta. Ez lényegesen egyszerűbbé teszi a hálózati környezet feltérképezést, mint a korábbi, adott doménben vagy munkacsoportban lévő gépek nevének egyszerű listázása, ami sokat nem árult el azok helyéről és szerepéről. A feltérképezett gépek és printerek között a Network Explorer segítségével böngészhetünk, ami szintén ezt a hatékonyabb felderítési módszert használja.

A Network Center és a Network Map megjeleníti a hálózati forgalomban kialakult problémákat is, így hibák esetén igazán hamar kideríthető, hogy mi okozza a leállást vagy a sebességproblémákat – segítve azt, hogy kiszűrhessük, melyik hálózati eszköz, csatorna szorul javításra, cserére, vagy éppen melyik kábel az, amit vissza kell dugni a helyére.

A Network Center az általa ismert, gyakori (szoftveres, konfigurációs és kapcsolódási) hibákra igyekszik egyből megoldást is nyújtani, így előfordul, hogy egyetlen kattintással korrigálhatók egyes rosszul beállított paraméterek.

A Vista Network Awareness arra is képes, hogy a Network Mapet alkotó adatokból automatikusan felismerje, ha számítógépünk egy másik hálózatra kerül (pél-

dául ha a munkahelyi laptopot otthonról ismét rácsatlakoztatjuk a vállalati hálózatra). Erről a változásról valamennyi, ez iránt érdeklődő alkalmazás értesülhet, és megtehetik a szükséges lépéseket (például automatikusan átkonfigurálhatják a tűzfalat).



A Network Map

Érdekesség, hogy a csoportházirend beállításai is azonnal érvényre juthatnak ennek következtében kapcsolódáskor, és azok már ekkor, nem pedig a következő ellenőrzési cikluskor lépnek életbe. Mindezek mellett az új Performance Monitor sokkal pontosabban meg tudja mutatni, hogy éppen milyen folyamatok mely portokon kommunikálnak a külvilággal, és mennyire foglalják le a rendelkezésre álló sávszélességet.

Új generációs TCP/IP-stack

A Windows XP és a Windows Server 2003 részeként megtalálható TCP/IP-stacket a Microsoft az 1990-es évek óta alakítgatja, és igyekezett vele lefedni az újonnan felmerülő vállalati és otthoni igényeket is. Azonban az eredeti stack tervezésekor még nem tudtak olyan, ma már hétköznapi technológiákat figyelembe venni, mint például az IPv4 és az IPv6 együttélése vagy éppen a wireless hálózatok, emiatt ezek megvalósítása hagyott némi kívánnivalót maga után.

A Windows Vistával teljesen lecserélődik a TCP/IP-stack – a Microsoft ugyanis úgy döntött, hogy itt az ideje nulláról újraírni valamennyi hálózatkezeléssel kapcsolatos funkciót. Ezt az új réteget egyszerűen csak „újgenerációs TCP/IP-stack”-nek nevezték el. Az új stack modulárisan épül fel, lehetővé téve, hogy később az új hálózati funkciók beépítése ne okozzon gondot, és az esetlegesen hozzáadandó protokollok is ki tudják használni az új stack minden képességét. Eddig például az IPv4 (Tcpip.sys) és az IPv6 (Tcpip6.sys) teljesen elkülönülve élt a rendszerben; az IPv6-driver saját maga valósította meg a szállítási réteget, benne a TCP/UDP-támogatást is, így párhuzamosan fejlődött egymás mellett két, egyébként sokban hasonló protokoll kódja. Mostantól az azonos funkcionalitással rendelkező komponenseket bármely protokoll és stack-rész képes használni, nincs többé felesleges szétválasztás. Ezáltal a TCP/IP-stack könnyebben portolható más rendszerekre is, például Windows CE-re, Windows Embeddedre és akár Xbox 360-ra is.

IPv6 – mi változott?

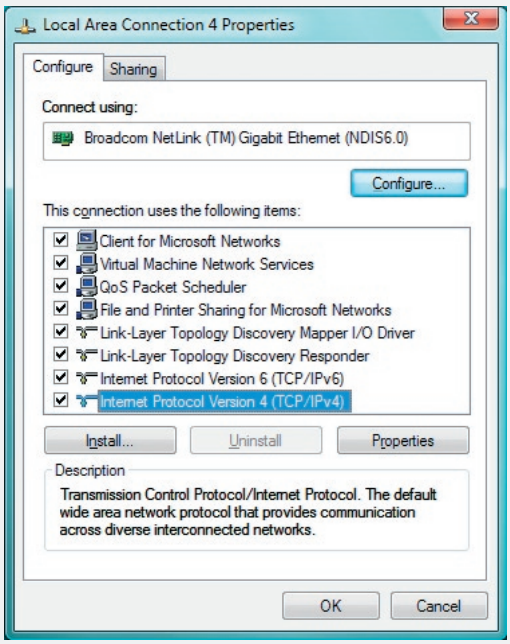
Bár már a Windows Server 2003 is támogatja az IPv6-ot, de mint látni fogjuk, az messze nem tud annyit, mint a Vistában és a „Longhorn” Serverben megtalálható változat. Korábban az IPv6-protokollt külön kellett telepíteni minden egyes hálózati adapterhez, most viszont már valamennyi adapter alapállapotban IPv4- és IPv6-támogatással érkezik. Minden hálózati kártyának egyszerre van IPv4- és IPv6-címe, amit megadhatunk akár kézzel is, vagy használhatjuk a hagyományos DHCP- és az új DHCPv6-szolgáltatásokat az IP-címek automatikus kiosztására.

Az IPv4- és IPv6-címek és -protokollok közti prioritásokat – vagyis, hogy a rendszer milyen sorrendben és melyiken keresztül próbál kommunikálni egy másik hálózati eszközzel – a „The Cable Guy” ezzel foglalkozó cikkében lehet alaposan végigtanulmányozni (http://www.microsoft.com/technet/community/columns/cableguy/cgarch.mspx).

Mindazonáltal elmondható, hogy a két technológia jól megfér egymás mellett, és a Vista igyekszik mindig az újabb, illetve a nagyobb sebességet ígérő megoldást választani – amennyiben lehetséges –, és csak utána nyúl a korábbi IPv4-stackhez.

Immár valamennyi hálózati beállítás elvégezhető grafikus felületről is, nem csak a korábbi parancssori eszközökkel. Az IPv6 végre teljeskörűen támogatja az IPsec-et, nem kell többé a biztonsági hozzárendeléseket és az IPsec biztonsági házirendjeit szöveges fájlokkal és az IPsec6.exe-vel érvényre juttatni, helyette egy kényelmesebb MMC snap-in áll rendelkezésre. Az IPsec-beállítások egy jelentős része már a Windows Vista tűzfalának MMC-felületéről is elérhető. Most már – csakúgy, mint az IPv4 esetében – használható az Internet Key Exchange (IKE), valamint az adatokat AES 128/192/256-tal is lehet kódoltatni.

A Vista IPv6 esetében már lehetőségünk van használni a Multicast Listener Discovery v2-t (MLDv2, RFC 3810), aminek segítségével már IPv6 hostok is részt vehetnek, illetve előfizethetnek multicast hálózati forgalomra, de akár az is megadható, hogy mely forráscímekről legyenek hajlandóak multicast csomagokat fogadni. A másik multicast vonatkozású újdonság a Link-Local Multicast Name Resolution (LLMNR), ez azt segíti elő, hogy az egy alhálózaton található, DNS-szerver nélküli hálózati szereplők megismerhessék egymás hálózati neveit. Ami akkor válik különösen hasznossá, ha ad-hoc, peer-to-peer, wireless hálózatokat alakítunk ki, vagy otthon-



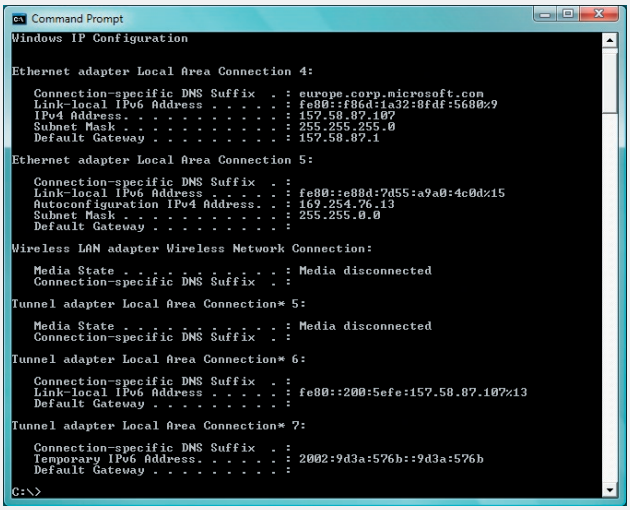
Egy hálózati csatoló beállításai

ni minihálózatot szeretnénk felállítani. Ezt a technológiát nemcsak az IPv6-, hanem az IPv4-hostok is használhatják a TCP/IP-n futó NetBIOS broadcast forgalom helyett.

Szintén újdonság, hogy most már megadhatunk URL-ben IPv6-os hálózati címeket az RFC 2732-nek megfelelően, csakúgy, mint ahogy eddig is használhattunk IPv4 IP-címeket a host nevének megadása helyett. IPv6-os címet például http://[2002:9d3a:576b::9d3a:576b] formában lehet megadni. Ez a szintaxis mind a rendszergazdák, mind az alkalmazásfejlesztők, valamint a felhasználók számára is elérhető lesz.

Az IP-stack egyéb újdonságai

A Windows Vistában külön routing-táblákat lehet megadni minden egyes interface–session pároshoz. Ez azon a problémán hivatott segíteni, amikor az internetelérésre és a VPN-kapcsolódásra külön interfész jön létre (akár egy adapteren is), és ilyenkor alapesetben nemcsak a VPN-forgalom, hanem a teljes hálózati kommunikáció is az újonnan kialakított VPN-interfészen keresztül folyik át. Ilyenkor jelentkezik az, hogy VPN-kapcsolódás után nem érjük el az internetet vagy a saját lokális hálózatunkat, csak a VPN-hálózatot, mert minden csomag a VPN-interfész felé fut tovább. A beállításokat a felhasználókhoz (pontosabban login sessionhöz) külön-külön rendelhetjük hozzá.



Az ipconfig kimenete

Míg a Windows XP és a Windows Server 2003 esetén a rendszer a laza (weak) host modellt támogatta, a Windows Vistában bekapcsolható – és alapbeállítás szerint be is van kapcsolva mind az IPv4- és az IPv6-protokollra – az erős (strong) host modell. No de mi is a különbség a kettő között? A beérkező unicast csomagokról az IP-stack dönti el, hogy azok az adott gépnek lettek-e címezve, és ha igen, csak akkor dolgozza fel azokat. A laza host modell esetében az IP-réteg attól függetlenül feldolgozza a csomagot, hogy az melyik interfészre érkezett. Az erős host modell azonban csak akkor foglalkozik az adott csomaggal, ha az azon az interfészen érkezik, amelyikhez hozzá van rendelve a beérkező csomag címzettjének hálózati címét tartalmazó hálózati tartomány. Az erős host modell megnövelt biztonságot garantál, azonban a laza host modell egyszerűbbé teszi a hálózati kapcsolódások kialakítását.

Az új TCP/IP-stack a beérkező TCP-csomagok feldolgozásának feladatait képes átadni a Network Driver Interface Specification (NDIS) szerint dolgozó miniport drivereknek és hálózati csatolóknak, hogy levegye a terhelést a processzorról és a hálózati rétegről. Ez leginkább a nagy sávszélességgel és hálózati forgalommal rendelkező szerverek esetében lehet fontos. Az NDIS 5.1 és az annál korábbi változatok csak egy processzort tudtak használni hálózati csatolónként, azonban a Receive-Side Scaling (RSS) megoldásnak köszönhetően mostantól a terhelés a többprocesszoros rendszereken is hatékonyabban osztható el.

A Windows Vista folyamatosan figyeli a környező hálózati eszközöket, és igyekszik minden pillanatban azt a beállítást választani a TCP/IP-stacknek, ami a leggyorsabb és leginkább megbízható adatforgalomhoz szükséges (beleértve a TCP-ablakok méretének beállítását is, ezt korábban gyakran kézi finomhangolással kellett optimalizálni). Gyakorlatilag ez a mechanizmus dolgozik a Network Awareness funkciói mögött is, vagyis ez a technológia a több, alkalmanként eltérő hálózatra kapcsolódó eszközök esetében is dinamikusan képes a legjobb beállításokat választani. Akár kézzel, akár automatikusan kerül sor a TCP/IP paramétereinek átállítására, azok egy esetben sem igénylik a rendszer újraindítását, mivel a beállításokat mostantól új helyen és más technikával rögzítik.

Szintén újdonság a Compound TCP (CTCP), ami leginkább a nagy sávszélességgel, de gyakran nagy késleltetéssel működő WAN-hálózatok esetében nyújt jelentős sebességnövekedést. A CTCP lényege, hogy az ezeknek a kritériumoknak megfelelő hálózatok esetében gyorsabban növeli a TCP-ablakok méretét, ezáltal a lehető legrövidebb idő alatt válik kihasználhatóvá a rendelkezésre álló sávszélesség. A Microsoft által elvégzett tesztek szerint a nagyobb állományok biztonsági mentéseinek szállításához szükséges idő WAN-hálózatokon (1 gigabit/s sávszélesség és 50 ms RTT mellett) közel a felére csökkent.

A wireless hálózatok kezelésével is sokat dolgoztak a fejlesztők, hogy javítsanak mind a sebességen, mind a megbízhatóságon, legyen szó IEEE 802.11-, GPRS- vagy UMTS-hálózatokról. Mindezt már korábban kitalált és bizonyítottan hatásos megoldások átvételével valósították meg, amelyek RFC-k formájában el is érhetők (RFC 2582, 2883, 3517, 4138).

Programozás, testreszabhatóság

A Transport Driver Interface továbbra is támogatott az alacsonyszintű kommunikáció programozására, azonban annak leváltására a lényegesen egyszerűbb és nagyobb tudású, Winsock Kernel (WSK) érkezik. Emellett megjelenik a rendszer részeként a Windows Filtering Platform (WFP), ami egységes programozói felületet biztosít a hálózati forgalom szűrésére, feldolgozására és transzformálására. Ennek segítségével végre egy helyen lehet elérni, hogy melyik alkalmazás és folyamat éppen melyik protokollokat és portokat figyeli, valamint a finomhangolható szűrők segítségével könnyebben lehet saját programlogikát építeni rá. A WFP funkcionalitása nagyon jól dokumentált és hivatalosan támogatott is, így garantáltan független lesz a szervizcsomagok megjelenésétől – tehát például az XP SP2 megjelenésekor felmerült, leginkább a hálózati szoftvereknél problémát okozó kompatibilitási problémák a jövőben már nem fognak előfordulni. Természetesen a WFP képes IPv6- és titkosított (például RPC-) forgalom szűrésére is, valamint a szűrők akár user módban is futhatnak.

Budai Péter

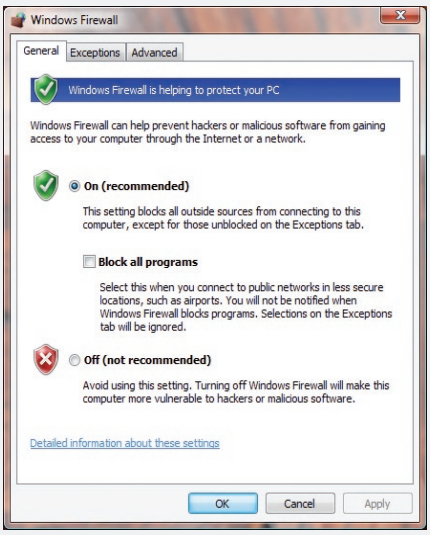
A Windows Vista tűzfala

Már a Windows XP is rendelkezett egy internetes forgalmat szűrő tűzfallal, beállítási lehetőségei azonban meglehetősen szegényesek voltak. A Windows Vistával viszont teljes értékű, profi tűzfalat kapunk.

A Windows XP SP2 tűzfalát mindenki ismeri: egyszerű felület, cserébe nem tolakodó. Figyeli, hogy adott portokon, adott címről jöhet-e befelé forgalom, illetve adott program „hallgatózhat-e" a gépen, és ha már szabad neki ilyet csinálnia, akkor kik szólíthatják meg. Az XP SP2 tűzfala egyetlen esetben dob fel ablakot a felhasználónak: ha a program hallgatózni szeretne. Többeknek ez az egyszerűség nem tetszett, hiányolták a gépet elhagyó hálózati forgalom szűrését, illetve a finomabb beállítás lehetőségét.

A legfontosabb újdonságok az XP-s verzióhoz képest:

- lehetséges mind a kimenő, mind a bejövő forgalom szűrése, bár alapbeállítás szerint a kimenő forgalom szűrése le van tiltva;
- elérhető egy új MMC snap-in a tűzfal speciális beállításainak testreszabására;
- a szűrési beállítások és a gépen alkalmazott IPSec-házirend együttes kezelése;
- kivételek és szabályok beállítása az Active Directory objektumai (felhasználók, csoportok, számítógépek), hostnevek, IP-címek, portok, programok, valamint protokollok szerint;
- teljes IPv6-támogatás.



Windows Vista-tűzfal felhasználóknak

Kétirányú szűrés

A kétirányú szűrés segítségével a bejövő kapcsolatokat is kontrollálhatjuk szabályok létrehozásával, blokkolva az ártalmas vagy ismeretlen forgalmat. Ugyanez védi meg számítógépünket az esetleges fertőzött vagy nem patchelt számítógépek által terjesztett vírusoktól és egyéb kártevőktől.

A rendszergazda ezentúl azt is megteheti, hogy a tűzfalon csak abban az esetben engedélyez bejövő kapcsolatokat, amennyiben rendelkezik a számítógép az összes szükséges biztonsági frissítéssel, valamint az összes, általában vírusok által használt port elérését is tiltja.

A tűzfal ebben a verzióban (a bejövő kapcsolatok szűrését tekintve) két mód egyikében működhet; az adminisztrációs felületen válthatunk közöttük:

- minden bejövő forgalom/kapcsolat tiltása, kivéve a fehérlistán lévők (ez az alapértelmezett);
- minden bejövő forgalom/kapcsolat engedélyezése, a feketelistát leszámítva.

A tűzfal konfigurálása

Eddig a tűzfal konfigurálására a vezérlőpulton egy meglehetősen egyszerű, a rendszergazdák számára nem minden esetben megfelelő alkalmazásban nyílt mód, ami azonban nem kínált sok beállítási lehetőséget, ugyanakkor az átlagos felhasználókat is megvédte: az általuk nem értett opciók hibás beállításával nem csökkenthették számítógépük biztonságát.

A Windows Vistában mindkét felület megtalálható. A szakemberek számára elérhető végre egy MMC-bővítmény is, ahol azt állíthatnak be, amit csak szeretnének.

Az MMC-konzol segítségével nemcsak a lokális, hanem bármely, a hálózaton elérhető számítógépre is rácsatlakozhatunk (jogosultság függvényében), és így akár egy távoli Vista tűzfalbeállításait is átállíthatjuk.

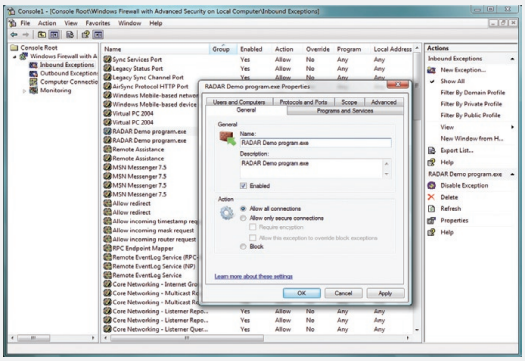
Amennyiben inkább a parancssor hívei vagyunk, a netsh immár tűzfalra vonatkozó kontextussal (netsh advfirewall) is bővült, így a feladatokat ott is elvégezhetjük.

Ezeken kívül több számítógép egyidejű beállítását magától értetődően a csoportházi-

rendből is megtehetjük, ahonnan az eddigi korlátozott lehetőségek helyett minden egyes beállítást elérhetünk.

IPSec-támogatás, Active Directory

A Windows Vista előtt az IPSec és a Windows-tűzfal beállításait külön helyről módosíthattuk, ez pedig időnként ütközésekhez is vezethetett, mivel az IPSec és a tűzfal egyszerre blokkolhat/engedélyezhet forgalmat. Az új



Windows Vista-tűzfal: MMC

verzió egyesíti a két technológiát, így egyszerűbben, egy központi helyről állítgathatjuk ezeket, ugyanazokkal az eszközökkel, ugyanazokkal a parancsokkal.

Azoknál a szabályoknál, ahol előírjuk egyes számítógépeinkre vonatkozóan a kötelező IPSec titkosított kapcsolatot, meghatározhatjuk a jogosult felhasználókat/csoportokat, ezzel is megakadályozva azt, hogy nem jogosult személy érje el a számítógépet a hálózaton keresztül. Ezáltal akár az is megvalósítható, hogy a Windows Vistán futó webszervert vagy egy adott portot/protokollt csak meghatározott, tartományba (domén) autentikált felhasználó vagy csoport érhessen el.

Kivételek forrás- és cél-IP-címek alapján

A jelenlegi tűzfal funkcionalitása a forgalom hatókörének meghatározásáig terjed – megadhatjuk a hálózatnak azt a részét, ahol engedélyezni szeretnénk a forgalmat az adott irányba, de csak a csomag „feladója” alapján. Az új verzióban az IP-csomag feladóján kívül a csomag címzettjére is tudunk korlátozni/szűrni, így a legmélyebb részletekig konfigurálhatjuk az átmenő forgalmat.

A célállomás ellenőrzése esetén további szűréseket végezhetünk DCHP-szerver, gateway, WINS-szerver, valamint DNS-szerverek szerint; ezek a host adataiból kerülnek a szűrőbe. Az XP SP2-ben csak a TCP/UDP-protokollok szűrésére volt lehetőségünk, egyéb típusú forgalom korlátozására nem. A Windows Vistában a protokollszám megadásával vagy a csomagfejléc adatainak manuális megadásával is létrehozhatunk szabályokat.

Apróbb kényelmi funkciókkal is bővült a szoftver. Míg jelenleg, ha éppen egy 250 portból álló tartományt szeretnénk engedélyezni vagy blokkolni, csak pontosvesszők használatával tehetjük meg, a portok egyenkénti felsorolásával (például: 1024; 1025).

A Vista megérkezésével azonban pihentethetjük ujjainkat: a tartományt a kezdő és végport megadásával határozhatjuk meg.

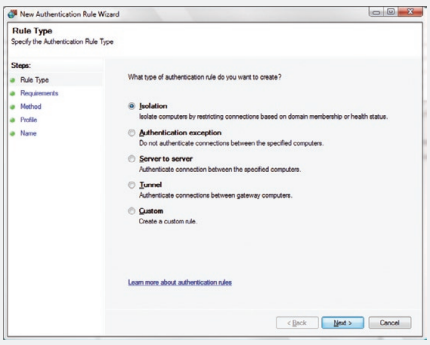
Interfészek, szabályok

Korábban, ha egy hálózati eszközön életbe léptettünk egy beállítást, az minden interfészre vonatkozott. Ezentúl külön-külön kontrollálhatjuk a remote access (VPN) kapcsolatokat is, függetlenül a közvetlen hálózati csatlakozásoktól.

A Windows Vistában már nemcsak a futtatható állományok (.EXE) biztonsági beállításait szabályozhatjuk, hanem akár valamennyi Windows-szolgáltatásunk hálózati hozzáférését is külön-külön korlátozhatjuk.

Megjelent még egy új fogalom a tűzfalban: a hitelesítő szabály.

Az újszerűnek mondható megoldást várhatóan meglehetősen sokan fogják alkalmazni,



A tűzfalszabályok típusai

hiszen ezekkel a kikötésekkel megkövetelhetjük a hozzánk kapcsolódó számítógépektől azt, hogy bizonyos patchekkel rendelkezzenek, esetleg azok is a mi tartományunknak legyenek a tagjai, valamint egyéb feltételeket is szabhatunk, mielőtt hozzáférhetnének a számítógépünkon futó hálózati szolgáltatásokhoz. Ugyanez alatt a menüpont alatt találjuk a tunnel, a server-server és a hitelesítés alóli kivétel szabályait is.

Számítógép-hitelesítő szabályok létrehozása

Izoláció. A Network Access Protection technológia felhasználásával a számítógép egészségi szintjének megkövetelése. Fontos, hogy az egészségi állapotot egyelőre csak Windows Vistát futtató klienseken lehet ellenőrizni, minden egyéb esetben a kivételek kiértékelése nélkül megszakad a kapcsolat, ha ezt bekapcsoljuk.

Kivételek megadása. Azoknak a számítógépeknek a megadása, amelyektől nem követelünk hitelesítést/NAP-ellenőrzést (legacy kliensek).

Server-to-server. Két kijelölt szerverszámítógép közötti kapcsolat védelmére szolgáló szabályok. Ebben az esetben meg kell adnunk azt a két számítógépet (végpontot), amelyek között a kapcsolatot létre szeretnénk hozni, és be kell állítani a hitelesítés módját is.

Tunnel. Tunnelen átfolyó forgalom szabályozása, általában két biztonsági gateway közötti adatcsere esetén.

Egyéni. Ha ezt választjuk, a szabály valamennyi opcióját szabadon állíthatjuk be, és ebben már egyáltalán nem segít nekünk beépített varázsló.

Mint látható, a Windows Vista tűzfalában igen sok az újdonság, így az most már lényegesen jobban megállja a helyét az interneten és a vállalati hálózatokon felbukkanó kártevőkkel szemben, míg rugalmas beállítási lehetőségei révén meg tud felelni a gyorsan változó vállalati igényeknek is. Ezáltal a legtöbb esetben feleslegessé válik harmadik féltől származó tűzfalszoftverek telepítése a Windows Vistát futtató klienseken.

Moldova György

További információ

Network Access Protection:
http://www.microsoft.com/nap/
Windows Vista termékoldal IT szakembereknek:
http://www.microsoft.com/technet/windowsvista/default.mspx

WinFX: menedzselt programozói környezet

A WinFX-szel nemcsak azoknak érdemes megismerkedniük, akik programoznak, hanem azoknak is, akiket érdekel, hogyan is fognak kinézni a következő évek alkalmazásai.

A Windows Vistával fog megjelenni a legújabb menedzselt programozási környezet – a WinFX –, amelynek révén minőségileg új felhasználói felületeket adhatunk majd alkalmazásainknak, miközben szétválasztjuk a design és a programozás műveleteit. Egységes és szabványos kommunikációs infrastruktúrát használhatunk az akár elosztott alkalmazás minden pontján, és az alkalmazásunkat elemi műveletek munkafolyamataként fogalmazhatjuk meg; a műveletek kezeléséhez hathatós segítséget kaphatunk a platformtól.

Windows Presentation Foundation

A felhasználói felület előállítására ma több lehetőségünk is van: a legegyszerűbb a konzolalkalmazás, de itt a grafikai lehetőségekre gyorsan ráunnak a programozók és a felhasználók is. A következő lehetőség a Windows Forms, amellyel már egészen komoly, Windows alapú felületeket készíthetünk. Ha ez nem elegendő, akkor a GDI+ segítségével nekiállhatunk rajzolni, és saját képünkre formálhatjuk a Windows-ablakokat. Akik pedig nagyobb teljesítményre vagy komolyabb grafikai képességekre, például háromdimenziós ábrázolásra vágynak, azok elmerülhetnek a DirectX rejtelmeiben. Szerencsére már ebből is van menedzselt változat, így nem kell elhagynunk kedvenc .NET-es környezetünket, ugyanakkor nem a legkényelmesebb a megoldás: az egyes szinteken egészen más programozói modelleket kell megértenünk és használnunk. Emellett a felület létrehozása során szorosan együtt kell dolgozni a grafikai tervezőnek és a programozónak, mert bármit is képzel el a tervező, azt kódból kell megvalósítani, és nem is minden lehetséges a befektetés ésszerű határain belül.

Mindezekre ad választ a WinFX egyik – és talán leglátványosabb – komponense, a Windows Presentation Foundation (leánykori nevén „Avalon"). A WPF egy új kompozíciós motor a felhasználói felülethez és egy alkalmazásleíró nyelv (az őket támogató infrastruktúrával), amelyek együtt jelentősen egyszerűsítik a szereplők életét – amellett, hogy a lehetőségeiket is kiterjesztik. Ennyi bevezető után nézzük meg a WPF működését a gyakorlatban!

Első WPF-alkalmazásaink

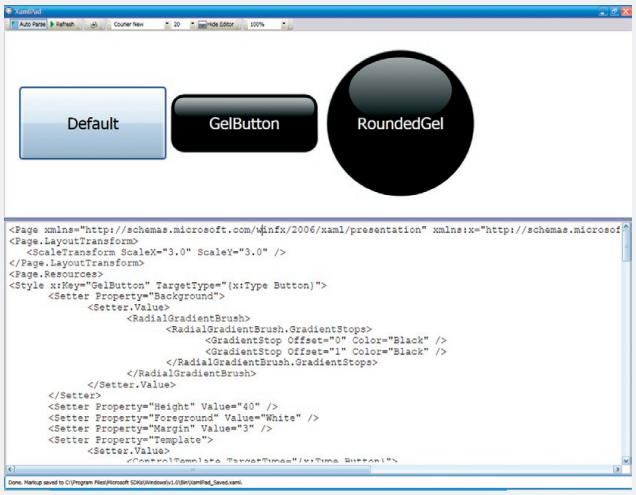
A WPF alatt a felhasználói felületet egy XML-ben megfogalmazott nyelven, az XAML-ben (eXtensible Application Markup Language, ejtsd: zeml) írjuk meg. Ez tartalmazza az elemeket, azok tulajdonságait, sőt még a hozzájuk tartozó animációkat és eseménykezelőket is (ez utóbbiakat mögöttes kódfájlokba is tehetjük). Aki most úgy érzi, hogy ez egy ismerős modell, az nem téved, ez nagyon hasonló a web mai formájához, ahol a HTML jelölőnyelv segítségével definiáljuk a felületet. Még a CSS-nek is megvan a maga megfelelője, ugyanis az egyes vezérlőkre sablonokat (template-eket) húzhatunk, és egészen komoly változtatásoknak vethetjük alá őket. A különbség ott van, hogy az XAML nyelvet nem egy böngésző értelmezi, hanem lefordítódik a .NET köztesnyelvére, és futó kód lesz belőle. A benne definiált összes vezérlő egy-egy objektum, amit C#-ból vagy más kedvenc .NET-es nyelvünkből ugyanúgy elérhetünk és manipulálhatunk. Ez az XAML teljes egészére igaz, tehát mindent, amit megtehetünk XAML-ben, azt megtehetjük kódból is. Az *1. képen* egy ilyen XAML fájlt láthatunk működés közben. Elsőként egy egyszerű gombot rak ki (<Button>Default</Button>), majd ennek definiál két sablont az XAML, amivel szebbé és izgalmasabbá válhat. Ezek csak sablonok, tehát a gomb ugyanaz a gomb-objektum marad, mint az eredeti, eseményekkel és tulajdonságokkal együtt.

A tervezők – Orcas és Expression Studio

Az XAML-forrást kézzel szerkeszteni egy ideig szórakoztató, de idővel unalmassá és kényel-

metlenné válhat. A HTML-t is csak finomhangolásnál szoktuk kézzel szerkeszteni, ha egyáltalán szükséges. A WPF alapú fejlesztéshez több támogató eszköz is tartozik. A programozók számára, a Visual Studio következő változata (ma „Orcas” kódnéven emlegetik) fogja tartalmazni a már megszokott tervezőnézeteket. Ezzel a programozók szemszögéből teljes lesz a kép. A grafikai tervezők számára a Microsoft egy teljesen új termékcsaládot jelentet meg, az Expression Studiót. A csomag három tervezőalkalmazásból fog állni: a Graphic Designerből, az Interactive Designerből és a Webdesignerből. Az első – egy általános célú, vektoros és raszteres grafikai tervezőprogram – bármilyen grafika elkészítéséhez hasznos segítséget nyújt majd.

Jelen cikk szempontjából a legfontosabb tulajdonsága, hogy képes a megszerkesztett ábrákat XAML-be exportálni, és így a megrajzolt elemeket felhasználhatjuk alkalmazásaink felhasználói felületén. Az Interactive Designer segítségével megmozgathatjuk a grafikai elemeket, az XAML segítségével előállítható animációkat és komplex elemeket készíthetünk könnyedén. A fejlesztők és a grafikai tervezők közös nevezője mindig az XAML lesz. A tervezők az Expression Studióval megtervezik az alkalmazások felhasználói felületét, amit a programozók mögöttes kódfájlokból közvetlenül meg tudnak „szólítani” *(2. kép)*.



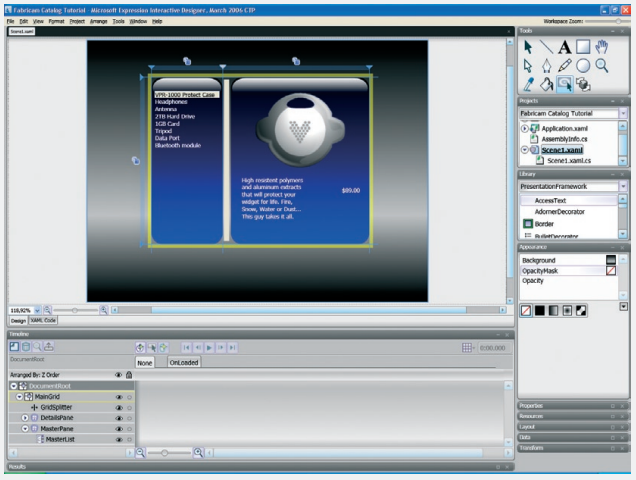
1. kép. Könnyen húzhatunk sablonokat a gombokra

További WPF technológiák

A központi XAML nyelven túl a WPF más újdonságokat is hoz. A számítógépes kijelzők felbontása szakadatlanul nő, egyre többen használnak lcd-kijelzőket, ezért fokozott figyelmet követel annak elősegítése, hogy kényelmesen lehessen olvasni ezekről a képernyőkről. Mivel a WPF vektoros megjelenítésű, a betűtípusok bármilyen nagyításban szépen néznek ki, és a rendszer szükség szerint alkalmazza a ClearType technológiát is a szomszédos pixelekre. A WPF-vezérlőkben elhelyezett hosszabb szöveg esetén a megszokott módon deklarálni kell az elemek elhelyezkedését (például sorkizárt szöveg, úsztatott képek stb.), és a WPF elvégzi nekünk a tördelést, biztosítja az oldalak közötti váltást a betűméret és az ablakméret függvényében. A szebb megjelenítéshez külön erre a célra kifejlesztett új betűtípusokat is tartalmaz a Vista. Ezek egyike a Consolas nevű fix szélességű ClearType betűtípus, ami külön is letölthető a Microsoft honlapjától, és arra fejlesztették ki, hogy a Visual Studióban vagy más fejlesztőeszközben a kódnézet könnyen olvasható betűtípusa legyen.

A szövegeket és más tartalmakat persze tárolni is kell valahogyan. Az informatika egyik régi megoldandó feladata, hogy az egyes alkalmazások egymás adatait értelmezni tudják, a dokumentumok nyomtatáshoz hűen legyenek szerkeszthetők, hosszú távon is megtartsák formájukat, és hatékonyan lehessen archiválni. A WPF tartalmaz egy újfajta, megjelenítésorientált dokumentumformátumot, az XML Paper Specificationt. Ezt a formátumot eleve arra tervezték, hogy a WPF felületű alkalmazásokban megszerkesztett tartalmakat hatékonyan tárolni lehessen. Az XPS formájú dokumentumok egy ZIP tömörített fájlban az Open Packaging Conventions által meghatározott mappahierarchiában tartalmazzák a dokumentum tartalmát, a beágyazott elemeket (például képeket), illetve a hozzájuk tartozó metaadatokat.

A formátum támogatja a digitális aláírásokat, illetve a jogosultságkezelést (Windows Rights Management). A Microsoft honlapjáról XPS nézőprogramot és mintadokumentumokat is letölthetünk.



2. kép. Az Expression Studio Interactive Designer

Windows Communication Foundation

Elosztott alkalmazások fejlesztése során sokszor merül fel a kérdés, hogy az egyes komponensek és rétegek között milyen kommunikációs technológiákat használjunk.

Ma már arra van szükség, hogy alkalmazások és platformok között is átjuttassunk információkat, ezért az objektumorientált megközelítést fel kell adni. Ezt felváltja az úgynevezett szolgáltatásorientált megközelítés, amelynek talán legfontosabb tulajdonsága, hogy a szolgáltatások autonóm egységek, nem tudnak, és nem is tudhatnak egymás implementációs részleteiről. Érdekes következményei vannak ennek akkor, ha egy elosztott alkalmazásban például egy művelet több szereplőjéből az egyik a tranzakció visszagörgetését kéri. Többek között ezzel foglalkoznak a széles ipari együttműködés keretében specifikált WS-* szabványok.

Az alkalmazáskomponensek integrálására az idők során több lehetőség is kifejlődött, és ma ezek közül választhatunk a körülmények függvényében. Ha például elosztott tranzakciók kezelésére van szükségünk, és ezt szeretnénk a Windowsra bízni, akkor COM+-t vagy .NET-es utódját, az Enterprise Servicest használjuk. Ha a megbízható üzenetközvetítés a legfontosabb, akkor

a message queue technológiákra, például az MSMQ-ra esik a választás.

Ha két .NET-komponens közötti kommunikációról van szó, akkor általában a .NET remoting a jó válasz, és ha platformok vagy vállalatok közötti kommunikációról van szó, akkor jöhetnek az XML webszolgáltatások. Ezek közül is az ASMX, ha egyszerűbb RPC-szerű műveletekről van szó, illetve a WS-Enhancements (WSE), ha a WS-* szabványoknak megfelelő fejlett funkciókra (például routing, titkosítás stb.) is szükség van. A lehetőségek széles skálája ilyen esetben általában nem áldás, hanem nehéz feladat, és hosszas vitákat szokott kiváltani a fejlesztők között. A Windows Communication Foundation ebben a rengetegben tesz rendet, és hatékony utódja lesz az összes fenti technológiának, egyesítve azok előnyeit és megpróbálva kiküszöbölni hátrányaikat.

A WCF egyszerű, mint az ábécé. A legfontosabb koncepciók ezekkel a betűkkel jellemezhetők: Address, Binding és Contract. Legegyszerűbben fogalmazva az Address megmondja, hogy kivel szeretnék kommunikálni, a Binding arról rendelkezik, hogy hogyan (például milyen protokollon, melyik porton), a Contract pedig azt határozza meg, hogy mit.

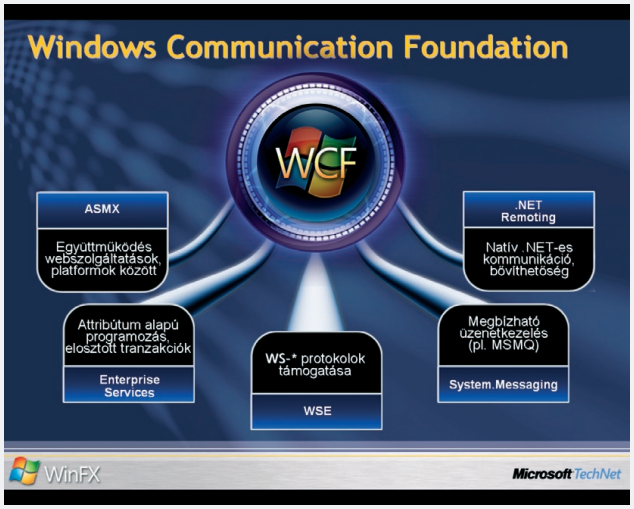
Ez a három együtt ad egy WCF-„endpoint”-ot, és a kommunikáció ilyen végpontok között zajlik. .NET-ben könnyen definiálhatunk contractokat, csak annyi a teendő, hogy megjelöljük az adatstruktúráinkat egy-egy [DataContract], osztályainkat pedig [ServiceContract] tulajdonságokkal. Ezután már csak hostingkörnyezetet kell találnunk, ami lehet akár az ISS szerver, de egy általános AppDomain is. Így a WCF szolgáltatások nem kötődnek az IIS-hez *(3. kép)*.

Windows Workflow Foundation

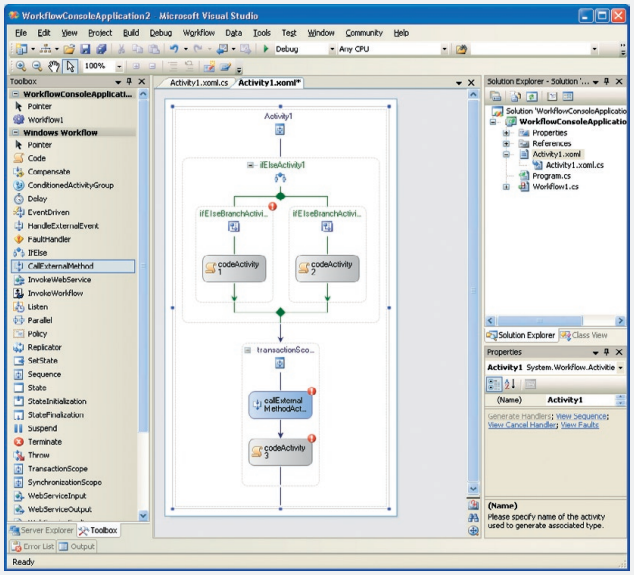
Alkalmazásfejlesztés során többször találkozhatunk azzal az igénnyel, hogy a programunk műveletek halmazát valamilyen előre beállított sorrendben hajtsa végre. Első nekifutásra általában varázslatos elágazási mintákat helyez el a programozó a kódba, de egy idő után felmerülnek olyan kérdések is, hogy például hogyan lehetne hatékonyan átkonfigurálni ezt, vagy mi történik akkor, ha egy hosszan futó folyamatról van szó, és, mondjuk, jó lenne lemezre írni az állapotot, amíg a felhasználó hazamegy aludni. Alkalmazások közötti integráció során erre már születtek nagyon jó megoldások, de az egyes alkalmazások szintjén eddig nem létezett egységes megoldás.

A Windows Workflow Foundation ehhez nyújt platformszintű támogatást. Az egyes munkafolyamatokat és elemeket definiálhatjuk XAML-ben vagy kódban is. Ahhoz, hogy egy munkafolyamat fusson, persze szüksége van egy „gazdára”, aki lehet egy alkalmazás, vagy egy kiszolgáló is, és ezután a workflow-motor levezényli a munkafolyamat működését. A legalapvetőbb munkafolyamatoktól (soros, párhuzamos végrehajtás) egészen komplexekig mindent meg tudunk valósítani, és a platform olyan szolgáltatásokat nyújt közben, mint például a folyamat letárolása (dehydration), ami hosszan futó folyamatok esetén hasznos, amikor várunk valamilyen eseményre, és fölösleges a memóriában tartani a folyamatot. Az XAML-ben történő megfogalmazás az algoritmikus feldolgozás lehetőségét rejti magában, ezt segíti a Workflow Designer, ami a Visual Studióban nyújtja a tervezés lehetőségét, de saját alkalmazásunkba is beépíthetjük.

A munkafolyamatokat különböző processzekben lehet futtatni, így például lehet a gazda az IIS vagy akár a Sharepoint is. A Microsoft Office rendszer következő változata erőteljesen építeni fog a Workflow Foundationre – például a Sharepointra feltöltött dokumentumokra rá lehet majd húzni egy-egy workflowt, és a Sharepoint majd levezényli például a jóváhagyás folyamatát *(4. kép)*.



3. kép. A WCF egyesíti a korábbi módszerek előnyeit



4. kép. A munkafolyamat-tervező működés közben

A WinFX ma

A WinFX a Windows Vistával egy időben fog megjelenni, ma az operációs rendszer fejlesztésével párhuzamosan folyamatosan jelennek meg az úgynevezett Community Technology Preview változatai. Ezek elérhetők a Microsoft letöltőoldalairól, és akár Windows XP-n is kipróbálhatók. Fontos, hogy ha fejleszteni szeretnénk, akkor a WinFX Runtime Components mellé telepítsük a megfelelő Windows SDK-t és a Visual Studio kiegészítéseit is.

Nagy Levente

További információk

http://www.microsoft.com/whdc/xps/default.mspx
http://spaces.msn.com/levispace
http://msdn.microsoft.com/winfx/
http://windowssdk.msdn.microsoft.com/library/

Miért csúszik a Vista?

Aki régebb óta követi figyelemmel a Windows Vista hányattatott sorsát, az már sejtheti, miért is csúszott ennyire sokat, és miért változott olyan sokat az elmúlt évek során. De tényleg: miért is?

Amikor a Microsoft megkezdte a Vista fejlesztését, több célt is kitűzött maga elé, szinkronba állítva azzal, hogy várhatóan milyenek lesznek a számítógépek a rendszer megjelenésekor. Az elemző cégek véleményét és az informatikai piac trendjeit figyelembe véve az iparág és a Microsoft is azt várta, hogy 2005 körül már általánossá válik a többmagos, 6 gigahertzes processzorral, legalább 2 gigabájt memóriával és terabájtos merevlemezzel felszerelt PC. 2004-ben vált mindenki számára világossá, hogy ennek semmi realitása nincs.

A hardverfejlődés megtorpanása

A hardver fejlődése – talán kicsit váratlanul – megtorpant, és 3 gigahertzes órajel feletti processzorokat nemigen sikerült készíteni. Ezt követően még legalább egy évet vártattak magukra a többmagos processzorok, és hatékony kihasználásuk is teljesen új programozási módszerek kidolgozását igényelte. Az órajel növelése lett volna az egyetlen megoldás, hogy a meglévő alkalmazások sebessége kódmódosítás nélkül növekedjen – ugyanis a processzorok belső architektúrájának optimalizálása is elérte a lehetséges határokat.

Dependencia-káosz

Ami még gondot jelentett, hogy a Microsoft megpróbálta a lehető legjobban kihasználni fő erősségét, mégpedig azt, hogy szoftverei hatványozottan képesek kihasználni egymás képességeit. Ez mindaddig kézben is tartható, amíg kész szoftverekre akarunk ráépíteni egy újat. De amikor egyszerre párhuzamosan fejlődik több, egymással keresztül-kasul együttműködő modul, akkor bármelyik csúszása katasztrofális következményekkel járhat a többire nézve is.

Nézzük, mi volt talán a legjelentősebb terület, ami a Vista késéséért is okolható: az új tárolási stack, amit közösen fejlesztettek a .NET 2.0-ban (ObjectSpaces), a WinFS-ben, illetve az azóta elhalálozott Microsoft Business Frameworkben, és részben alapul vették az SQL Server 2005 kódját is.

Biztonság és komplexitás

Időközben egyre több támadás érte a Microsoftot szoftvereinek sebezhetősége miatt, válaszul a vállalat gőzerővel nekilátott a Windows XP SP2 fejlesztésének, valamint kialakított jó pár olyan módszert, amivel elkövetkező fejlesztéseinek biztonságossá tételét igyekezett szavatolni. A harc a minél biztonságosabb Windowsért szintén késleltette a Vista fejlesztését, már csak azért is, mert az SP2 munkálataihoz a Vista-csapatból vontak el ideiglenesen embereket.

Nyilván logikusan következik abból, hogy ha folyamatosan változnak a piaci és felhasználói igények (például a hardverek), valamint ennyire integrált minden rendszerkomponens, akkor azok tervezése, fejlesztése és tesztelése sem mindennapi kihívás. Például gondot jelentett, hogy mindennap előálljon a legfrissebb build valamennyi készülő komponens felhasználásával, és ne kerüljön bele olyan bug a rendszerbe, amitől az egész aznapi build-készítés 90 százaléknál összeomlik.

Megoldás: a Longhorn "Reset"

Két éve, 2004 nyarának egyik hetében *Jim Allchin* megkereste *Bill Gatest*, és elmondta neki, mik az aggályai a Vista fejlesztése körül, beszámolva az itt is említett külső és belső okokról. Mindenki arra törekedett, hogy a problémák mielőbb megoldódjanak, ráadásul ne váljon feleslegessé az addig elvégzett hatalmas mennyiségű munka és annak eredménye.

A hardverfejlődéssel kapcsolatos előrejelzések pontatlanságának következtében a Microsoft kénytelen volt felhagyni azzal a tervével is, hogy a még félkész .NET keretrendszer 2.0-t mélyen integrálja a Windows-kernelbe. Ez az alapok jelentős átalakításával járt, s a Microsoft visszanyúlt a közben fejlesztett Windows Server 2003 SP1 kódjához, ami ekkor már stabilan működött, így jó kiindulási alapot nyújtott a meglévő képességek egy részének ráépítésére.

A maradékot viszont kíméletlenül újra kellett írni, ráadásul a dependenciák minimalizálásával, ami egyben a meglehetősen komplex WinFS eltávolításával is járt.

Végül a .NET 2.0 nagy késéssel megjelent a Visual Studio 2005 részeként, de már ObjectSpaces nélkül, és ekkorra már a Windows-kernel is független volt a keretrendszertől – de ez csak egy példa a sok közül.

Ekkor tették rendbe a Vista napi build-rendszerét, létrejöttek az úgynevezett Quality Gatek, ezek szavatolták, hogy rossz minőségű kód ne veszélyeztethesse a napi build előállítását, mivel a fejlesztő végre sem tudta hajtani vele a check-in műveletet, vagy ha mégis, és gond jelentkezett, akkor az a kód azonnal repült is a Bug Jailbe.

Hol tartunk most?

Mindez már lassan két éve történt. A Windows Vista fejlesztése a végéhez közeledik, e lapszámunkkal egy időben jelenik meg a második béta. A Microsoft láthatóan tanult az elkövetett hibákból, és rohamléptekkel dolgozik szoftvereinek legújabb hullámán, ami már a Live stratégiát is magába szippantotta – de ez már egy másik történet.

Budai Péter

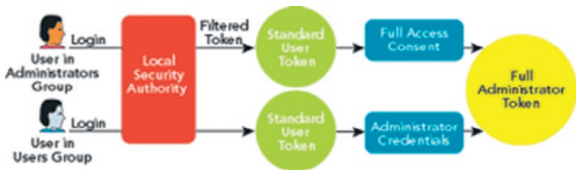
WINDOWS VISTA: BIZTONSÁGI ÚJDONSÁGOK

Mindinkább úgy tűnik, a Vistában érnek be a Microsoftnak azok a biztonsággal kapcsolatos erőfeszítései, amelyek lenyomatait már a korábbi operációsrendszer-szervizcsomagokban (XP SP2, W2K3 SP1) is láthattuk.

Minden komoly szakember a szemének hisz igazán. A változás igen sokrétű, a számtalan új eszköz, megoldás megjelenése mellett a különböző, már ismert komponensek biztonságosságának bővítése, megújulása is számottevő, ami így együtt megfelel a Microsoft ígéretének: a Vista lesz „minden idők" legbiztonságosabb kliensoldali operációs rendszere. Egy szó, mint száz, újra kell tanulnunk rengeteg mindent! Kezdjük a dolgot három – szubjektív alapon kiválasztott – témával: a User Account Controllal (UAC), a Windows Service Hardeninggel és a Windows Defenderrel.

User Account Control (UAC)

A jelentős (és divatos) ellenpropaganda ellenére még mostanság is jellemző szokás Windows-környezetben – akár a munkahelyen, akár otthoni körülmények között – rendszergazdai jogosultsággal ellátni az átlagos felhasználókat, és persze a haladó felhasználókat, illetve a rendszergazdákat meg még inkább. Azaz teljes kontrollt adunk a felhasználóknak, és így szabad utat az emelt szintű jogosultsággal futó vírusoknak, wormoknak, kém- és reklámprogramoknak. Ha üzemeltetőként szeretnénk megoldani ezt a nem túl szerencsés felállást, akkor igazán nagy kihívások elé nézünk, hiszen jelentős mértékben sem az operációs rendszerek, sem az alkalmazások nem segítenek bennünket kijutni ebből a csapdahelyzetből. A jelenlegi körülmények között, a rendelkezésre álló eszközökkel ezt az ellentmondásos helyzetet („minden működjön, de emelt szintű jogosultságot nem adunk") vélhetően nem is lehetséges feloldani. Értelemszerűen a Microsoft is érzi a problémát, ezért a Vistában bevezetendő User Account Control bizonyos esetekben képes lesz megadni a szükséges pluszjogosultságot, de alapesetben minden felhasználó (a Rendszergazdák csoport tagjai is) mindent egy standard felhasználói kontextusban futtat.



Filtered Token és sztenderd token

Az UAC gyakorlatilag a belépés pillanatától kezdve dolgozik. Abban az esetben, ha egy rendszergazdai csoporttagsággal lép be a felhasználó, az LSA (Local Security Authority) szolgáltatás értesíti az UAC-t, és ekkor egy kicsit másfajta, „filtered access token" (a token a felhasználó által bitorolt csoporttagságok halmaza) rendelődik az adott felhasználóhoz, szemben a sztenderd tokennel. Ez utóbbi használatos a Vistában például az EXPLORER.EXE futtatásához (és gyerek-processzeihez, amelyek öröklik a szülő-processz jogosultsági körét). Ha egy átlagos felhasználó lép be, akkor az EXPLORER.EXE alapesetben megkapja „tőle" a neki járó sztenderd tokent. Amennyiben olyan szervizt vagy processzt óhajtunk futtatni, amelyik kívül van a sztenderd token hatáskörén, akkor jön a megerősítéskérés. Az UAC tehát részben a korábbi „Run As..." megoldás mentén halad tovább, de nem nekünk kell már eleve a megfelelő jogosultságú felhasználóval indítani az adott programot (mert ha nem tesszük meg ezt, akkor „csont nélkül" elutasít például az XP), hanem minden olyan alkalommal, amikor szükség van a pluszjogosultságra,

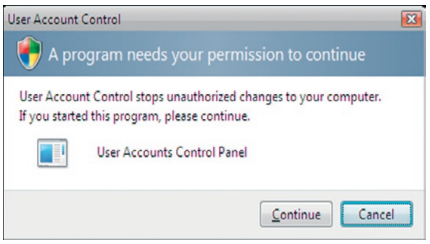
kapunk egy figyelmeztető ablakot, és ebben megadhatjuk az igényelt jogosultsággal bíró fiók felhasználónév/jelszó párost. A helyzet az, hogy gyakorlatilag rendszergazdaként belépve is kőkeményen visszakérdez a rendszer, sőt további két ágra bontja a megerősítést:

1. ha olyan programot indítunk, amellyel lehetséges a rendszerelemek változtatása, illetve

2. ha olyan alkalmazást indítunk, amely telepítéssel jár.

Az UAC rendszergazdaként, illetve felhasználóként

Az UAC részei közül az Application Information Service (AIS) a jogosultságokat, illetve a megerősítést kéri be, és ennek helyessége esetén garantálja a magasabb szintű tokent. A másik fontos komponens a „telepítésdetektáló”, amely az „adatvirtualizáló” részegységekkel együtt lehetővé teszi például a fejlesztőknek, hogy megjelöljék azokat az alkalmazásokat, amelyekhez magasabb szintű jogosultsági kör szükséges, azaz amelyeket az AIS-nak kötelessége lesz (a felhasználói megerősítés után) ellátni a magasabb szintű tokennel, így érve el azt, hogy állandó rendszergazdai csoporttagság nélkül is futtathatók legyenek.



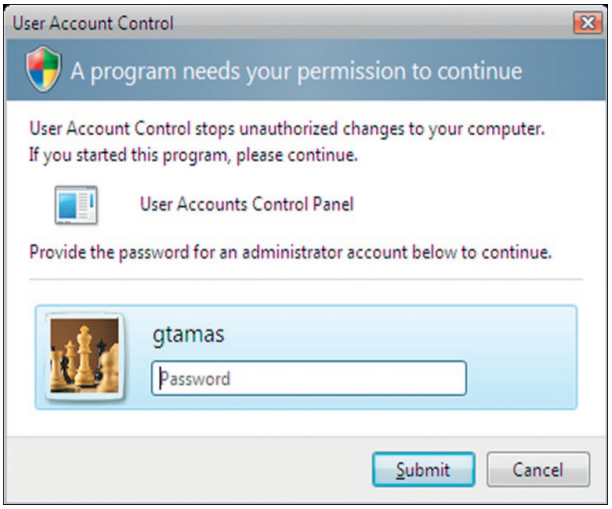
Rendszergazdaként belépve is visszakérdez a rendszer

A tervek szerint üzemeltetőként lesz viszont egy olyan lehetőségünk, amely megengedi, hogy bizonyos, a rendszert kényes szinten érintő alkalmazásokat – amelyek futtatásához ezért szükséges is az admin token – „megjelöljünk”, ezeket a jelöléseket egy alkalmazáskompatibilitási adatbázisba helyezzük, és ezek után a csoportházirend segítségével központilag telepítsük. Végül a felhasználónak már csak egy megerősítést kell majd elvégeznie, és kész is vagyunk a biztonságos alkalmazásfutatással.

Meg kell említeni ugyanakkor, hogy nem kevés vitát vált ki a mostani állapotában az UAC (pillanatnyilag a második bétaváltozat előtti utolsó változattal, az 5381-es verzióval dolgozunk), hiszen eléggé idegesítő sűrűséggel jönnek a figyelmeztetések, ami viszonylag gyorsan arra készteti az embert, hogy ezeket negligálja legalább a rendszergazda részére (a kikapcsolás a házirendből lehetséges, 8 opció van az UAC hangolására). Úgy hallani viszont, hogy ez még bizonyosan változni fog, különösen vállalati környezetben.

Service Hardening

A Windows Service Hardening technológia limitálja a mostanság amúgy is (mondjuk egy Windows NT-hez képest főleg) „sivárabb” feltételek között tobzódó szolgáltatások lehetőségeit, így a szolgáltatások (illetve a szolgáltatásokat kihasználó káros alkalmazások) nehezebben fognak hozzáférni az erőforrásokhoz, mivel csökkennek a jogosultságaik. Ez a gyakorlatban egy többlépcsős korlátozást jelenthet. Az operációs rendszer szolgáltatásfuttató eleme (a Service Control Manager, SCM) például első lépcsőben arra törekszik, hogy az eddig a Local Service-fiók kontextusában futó szolgáltatás az adott helyzetben csak a ténylegesen szükséges jogokat tartalmazó tokent kapja meg, például a „SeTCBPrivilege”-t sosem (ez az operációs rendszer részeként való működést jelentené, azaz akármilyen felhasználó nevében, a jelszó ismerete nélkül engedélyezni – durva volna). Ilyen az XP-ben vagy a Windows Server 2003-ban nincs, a jogosultságra könnyedén ráteheti a kezét egy-egy szolgáltatás.



Felhasználóként belépve szükség lesz a megfelelő jogosultságra

Egy másik példa a szolgáltatások helyzetének változására a SID (Security IDentifier) hozzárendelése minden egyes szervizhez. Ezzel lehetővé válik a részvételük a jogosultsági listákban (ACL), azaz ugyanolyan technika szerint kaphatnak egyesével is jogokat, mint a felhasználók, csoportok stb. Ez az újdonság jól jön még például a Vista-tűzfal kimenő forgalmát szabályozó, szolgáltatásszelektáló résznél is.

Windows Defender

Leánykori nevén Microsoft Windows Antispyware-nek hívták ezt a komponenst, és amióta csak létezik, publikusan letölthető a bétaváltozata, így elképzelhető, hogy sokan ismerik. A nevében hordozta a kizárólagos működési területét, azaz a mára legdivatosabb kártevőket a kém- és az reklámprogramokat irtotta több-kevesebb sikerrel.

Nem olyan régen új – és tegyük hozzá, hogy kivételesen sokkal jobb – elnevezést kapott, amely sokkal jobban jellemzi az azóta alaposan megnövekedett tudását és komplexitását. A Windows Vistában már az elejétől alapértelmezés szerint bent „tartózkodik”, sőt mi több, beköltözött a Security Centerbe is, a „Malware Protection” kategória alá (de a Control Panelből is elérhető). Ettől függetlenül a továbbiakban is letölthető, ingyenesen kipróbálható a második bétaváltozattal (http://tinyurl.com/dyvaw).

A Windows Defender az ugyancsak erre a névre hallgató szolgáltatást használja. Ez a szerviz teszi lehetővé az időzíthető kereséseket, a gépre telepített alkalmazások figyelését (és a Process Explorer kimenetéhez kicsit hasonló listákat is a működő alkalmazásokról, processzekről), a kártevők eltávolítását vagy adott esetben a karanténba helyezésüket.

A felhasználói felületről a szerviz értesítése az RPC-szolgáltatáson keresztül történik, ezzel lehetővé válik sztenderd felhasználói környezetben is a Windows Defender hibátlan működése. A szignatúra-adatbázis frissítése manuálisan és automatikusan is történhet az MU oldalakról, illetve egy ideje hálózatos környezetben, kellemes módon a WSUS szervereken keresztül is.

Gál Tamás

Pillantás az InfoCardra

Sokak számára bosszantó tevékenység a webes űrlapok kitöltése. Az évek során számos segédeszközt készítettek a folyamat felgyorsítására és a jelszavak tárolására, de a monoton ismétlődés még így is zavaró. Ha a felhasználó – saját dolgát egyszerűsítendő – úgy dönt, hogy mindig ugyanazt a jelszót használja, az már egyenesen a biztonság rovására megy.

Az internetes személyazonosság fragmentált kezelése nemcsak kellemetlen, de az internet és a felhasználók lehetőségeit is korlátozza. A Windows Vistában tervezett InfoCard olyan ígéretes eszköz lehet, amely egységesítheti a webes identitáskezelést.

Jelenleg az internetes szolgáltatásoké az egyetlen olyan területet, ahol a technológia kibocsátás előtti képességeit kipróbálhatjuk, de a jövőben működik majd a böngésző alapú webes szolgáltatásokban is.

Az identitás

Hogyan kellene azonosítani a felhasználókat a weben? Mi a helyzet más entitásokkal – a szolgáltatásokkal, vállalatokkal, szervezetekkel, eszközökkel és egyebekkel?

Vegyünk egy képzeletbeli felhasználót! Fontos adatai: neve, címe és kedvenc időtöltései. Az illető hajlandó megosztani ezeket az adatokat másokkal egyes megbízható internetes honlapokon azért, mert ennek fejében valamilyen hasznot remél. Ezeket a dolgokat ő mondja el magáról, másoknak azonban vannak még róla szóló információi.

Példafelhasználónk vásárlóként és eladóként is szerzett magának néhány csillagot az eBayen. Hiába, mert ha bejelentkezik egy másik internetes közösségbe, nincs módja igazolni, hogy megbízható tagja az eBaynek. Elölről kell kezdenie a reputációjának a felépítését, hiszen nincs rá mód, hogy az eBay-azonosságát átvigye az új kompániába. Természetesen bármit állíthat magáról, de senkinek sincs rá oka, hogy higgyen neki. Ugyanakkor az eBayen könnyedén vásárolhat, mert az ottani statisztikák szerint jó fizető. Az aukciós hely ellenőrző rendszere abban a környezetben megfelelő „hivatkozási alap” a számára.

Ebben a megközelítésben az InfoCard olyan lehetőség, amely elfogadhatóvá teszi az illető állításait, ezért a „hivatkozási alapnál” erősebb igazolóeszköznek lehet tekinteni.

Az InfoCard vonatkozásában a digitális azonosság olyan állítások összessége, amelyeket egy digitális személyiség vagy dolog állít magáról, illetve más digitális entitások állítanak róla.

Az illetőnek az InfoCard rendszerben eltérő környezetekhez eltérő identitásai tartozhatnak, és az azokhoz megadott állításoknak sem kell feltétlenül igazaknak lenniük. Ez nem jelent feloldhatatlan ellentétet az InfoCard igazoló szerepével, hiszen ha, mondjuk, egy honlap bekéri példafelhasználónk lakcímét, és ő a saját biztonságának okán hamis címet ad meg, akkor az adott webhely szempontjából a kockázatcsökkentő füllentés még elfogadható lehet.

Az InfoCardok tehát lehetővé teszik több identitás használatát, és azt is megengedik, hogy a felhasználó az eltérő struktúrákhoz más-más identitást alakítson ki.

Posztulátumok

Kim Cameron, az InfoCardot kidolgozó munkaközösség egyik vezetője szerint bizonyos objektív törvényeknek szabályozniuk kell, hogy adott környezetben milyen azonosítórendszer működjön és hogyan.

1. Biztosítani kell a felhasználó ellenőrzési és beleegyezési jogát.

2. Érvényesülnie kell a minimális információ-közzététel elvének: egy adott rendszer a használatához csak a lehető legszükségesebb adatokat kérje be és kapja meg.

3. Az információt kérő félnek legyen igazolható oka az adatkérésre, az önmagát igazolónak pedig legyen meg a joga arra, hogy választhasson az azonosságai közül.

4. Az identitás irányítottságának szabálya szerint egy online vásárlóhelytől két dolgot várunk:

- többirányúságot: minden betérővel világítótorony módjára tudassa, hogy „ő” a vásárlóhely;
- egyirányúságot: ne tegye közzé a személyes adatokat (közben persze azok alapján követheti a felhasználó tevékenységét).

5. Az azonosságrendszerek legyenek egymás számára átláthatóak; legyen egy olyan „rendszerek rendszere” (metarendszer), amely megteremti ehhez a megfelelő absztrakciós alapokat.

6. Érvényesüljön a humán integráció: a végfelhasználó legyen a hitelesítő protokoll végpontja, és legyen minimális a veszélye annak, hogy az azonosítórendszerbe mások is belelássanak vagy beleavatkozzanak.

7. Biztosítani kell a konzisztenciát: az azonosítórendszerek kezelése a használt technológiától függetlenül legyen érthető és a lehetőségekhez képest egységes a felhasználó számára.

Azonosságkezelő metarendszer

Az InfoCard-tranzakcióknak három szereplőjük van:

- az a dolog vagy felhasználó, amely vagy aki digitális reprezentációjában részt akar venni egy tranzakcióban;
- az a szervezet, amely a fenti művelet előtt elkészítette az azonosságot (IP Identity Provider);
- az a rendszer (bekérő fél), amely a művelethez bekéri az identitást.

Az ötödik törvénynek megfelelően az InfoCard-metaszisztéma tartalmazza azokat az alapokat, protokollokat és felületeket, amelyek struktúrájában megfelelően együttműködhetnek egymással a különböző azonosítórendszerek és a szereplők.

A digitális identitás megvalósítása

A digitális azonosító – most már a konkrét InfoCard – kiadását az IP végzi. Az IP ehhez bekéri a saját szempontjainak megfelelő felhasználói adatokat (például: név és e-mail-cím), majd ugyancsak a saját szabályai szerint ellenőrzi azokat. Sikeres ellenőrzés után elkészíti az InfoCardot, ami nem más, mint egy XML-dokumentum.

Fontos, hogy az InfoCard maga semmilyen személyes információt nem tárol, csak azoknak a jellegét – metaadatok formájában –, amelyeket az IP a kiállításkor bekért a felhasználótól.

A szereplők kommunikációja

Anélkül, hogy belemennénk a titkosítás és a protokollok részleteibe, egy példán keresztül mutatjuk be az InfoCard-szisztéma szereplőinek akcióit.

Mondjuk az eBaynek van egy olyan szolgáltatása, amely támogatja az InfoCardot; az eBay a „bekérő fél”.

1. A felhasználó ennek eléréséhez a gépére telepít egy kliensalkalmazást, amely tudja, hogy prezentálnia kell az akciókhoz a felhasználó identitását, de nem tudja, hogy melyiket.

2. A felhasználó (a kliensprogram) megkérdezi az eBayt, hogy milyen InfoCardra van szükség.

3. A válaszban az eBay közli a számára elfogadható protokollt, az IP-k listáját és az adat jellegét (például e-mail-cím).

4. A kliens az eBay válaszát továbbítja a gép InfoCard-rendszerének.

5. Megjelenik egy ablak azokkal a már meglévő kártyákkal, amelyek az eBay kívánalmainak megfelelnek – de csak azokkal, azaz nincs köztük például a munkahelyi InfoCard. Az ablakon feltűnően látszik a bekérő fél hitelesített logója.

6. A felhasználó rákattint a megfelelőnek tartott kártyára.

7. A gép InfoCard-rendszere lekéri az IP-től a kártya azonosságának megfelelő adatokat.

8. Az IP az eBay által előírt protokoll szerint kezelt adatcsomagban visszaküldi az információt.

9. A gép InfoCard-rendszere megmutatja az IP által szolgáltatott adatokat.

10. A felhasználó jóváhagyja az adatok közlését.

11. Az InfoCard-rendszer az előírt formában elküldi az eBaynek a megfelelő adatokat.

A törvények

Az 1. és 2. törvény láthatóan teljesült, de meg kell említeni egy apróságot: a valóságban még az e-mail-címre sincs szükség, hiszen elegendő lehet egy, az IP által kibocsátott PPID (Personal Private Identifier – magánjellegű személyes azonosító), amit a bekérő fél publikus kulcsának a segítségével generálhat az adott felhasználó adott identitásához. A PPID használatával a bekérő félnek egyetlen személyes adatot sem kell kérnie, mégis követheti a felhasználóit. Ennél jobb védelem a személyes adatoknak sem kell.

Ami a harmadik törvényt illeti, egy olyan zárt kört látunk, amelyben egyedül az IP élhetne vissza a felhasználói adatokkal, de nem teszi, mert nem érdeke, másrészt úgyis rájönnének. A negyedik törvény is érvényesült, hiszen ott volt az eBay „több irányba”, minden felhasználónak elküldött logója, a felhasználó gépén az „egyirányú” InfoCard-rendszer pedig nem sugározza szerteszét az IP-től kapott adatokat.

Három szereplő a tranzakcióban

Az ötödik törvényt kipipálhatjuk, hiszen a felhasználó maga választotta az eBayt és az IP-t, azok között sikeres volt a vázolt menetrend szerinti adatcsere, tehát egymás számára átláthatóak voltak. A hatodik törvény is rendben volt, mert a gép InfoCard-rendszere és a felhasználó között nem volt (nem is lehet) további fél. A hetedik törvény is teljesült, mert a felhasználó egy szilárd, transzparens és könnyen kezelhető felépítményt lát.

A reputáció átvitele

A kiindulási probléma megoldása rendkívül egyszerű: ha az eBay egyszersmind IP-ként is szerepelhet, akkor kijelentheti a felhasználójáról, hogy 99,8 százalékban pozitív tapasztalatai vannak róla, és ezt kérésre nemhogy írásba, de olyan „InfoCardba” is adhatja, amellyel más, az eBay „véleményére” adó közösség vagy szervezet számára igazolható a „jó eBay-felhasználó vagyok” állítás.

Kelemen László

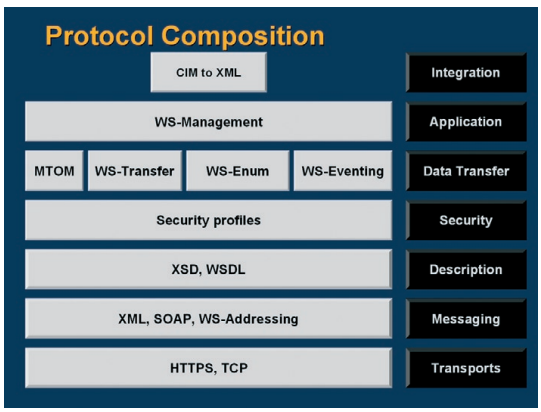
WEBSZOLGÁLTATÁSOK A VADONBAN

A webszolgáltatások kétségkívül nagy hatással vannak a mai és az elkövetkező évek informatikájára, csakhogy – nevüknek köszönhetően – sokan sajnos azonnal webes alkalmazásokra és interneten futó szolgáltatásokra gondolnak. A webszolgáltatások tartalma azonban ennél lényegesen több.

A jelen és a közeljövő informatikájára nagy hatást gyakorló webszolgáltatások ötletének lényege, hogy komplex rendszerek együttműködését modellezzük úgy, mintha autonóm egységek egymással üzeneteket váltva képeznének nagyobb rendszereket – mindehhez pedig könnyen implementálható és szabványos technológiák kapcsolódnak.

Jó-jó, de én nem vagyok fejlesztő

Első látásra az XML webszolgáltatások kizárólag fejlesztői technológiáknak tűnhetnek, de hamar észrevehető, hogy egyre több szervertermékben, és a rendszerintegráció kapcsán is folyamatosan WS-* szabványokba botlunk. A webszolgáltatások ugyanis valójában arra törekednek, hogy egységes, mindenki által elfogadott szabványok képében írják le az elosztott rendszerek és komponensek közti kommunikációt, ezzel képezve egyfajta közös nevezőt az összes már meglévő és a még fejlesztés alatt álló szoftverek és akár hardverek között.



1. kép. A webszolgáltatás rétegei menedzsmentmegoldásokhoz

Képzeljünk el olyan szervereket és akár hardvereket, amelyek – függetlenül attól, hogy milyen platformon futnak, milyen operációs rendszerhez kapcsolódnak – képesek egységes módon jelezni állapotukat a központi menedzsmentszoftvernek. Mindez ma már lehetséges a WS-Management specifikáció révén – és ezt nem a hagyományos értelemben vett internetes szolgáltatások teszik lehetővé. Az sem mellékes, hogy magukat a webszolgáltatásokkal készített szolgáltatásorientált rendszereket is üzemeltetni kell, és ehhez nem árthat ismerni azok hátterét.

A Windows Server 2003 R2 részeként már elérhető a WS-Management specifikáció köré építkező, tűzfalakon keresztül is használható menedzsment-stack, ami nagyon szorosan integrálódik a Windows oldaláról az IPMI-vel és a WMI/CIM-mel, lehetővé téve a rendszerek távoli felügyeletét, azok összekapcsolását egymással, illetve a köztük zajló folyamatok automatizálását. A heterogén rendszerek webszolgáltatásokkal történő menedzsmentjéről a következő számban lesz szó, mindenekelőtt azonban érdemes megismerkedni a technológia alapjaival.

A webszolgáltatások rétegei

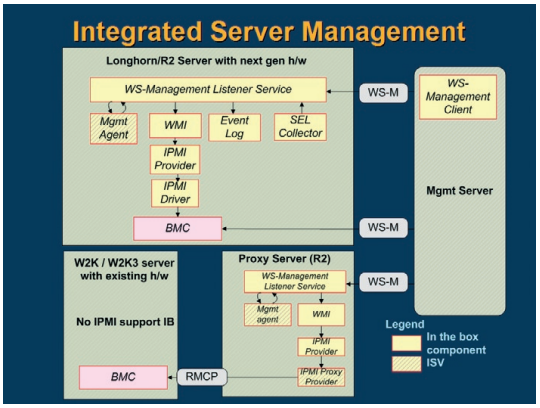
A webszolgáltatásokat alkotó technológiák hasonló módon rétegződve épülnek fel, mint a hálózati protokollok OSI/ISO rétegei *(1. kép)*. A legalsó réteg gondoskodik az üzenetek szállításáról a szolgáltatások között, ami általában HTTPS vagy TCP szokott lenni. A http-protokoll természetesen amiatt kényelmesebb és gyakrabban használt, mert a webes forgalmat a tűzfalakon keresztül is kényelmesen át lehet vele juttatni.

A következő réteg foglalkozik azzal, hogy hogyan épül fel egy üzenet, ami két szolgáltatás között cserélődik, és hogyan ér célba. Ebben a rétegben a legfontosabb technológia a platformfüggetlen XML adatleíró nyelv: lehetővé teszi, hogy bármely két rendszer képes legyen szabványos módon adatokat cserélni egymással, legyen szó akár számokról, szövegekről vagy sokkal komplexebb struktúrákról.

A következő kulcstechnológia ebben a rétegben a SOAP, ami valaha a Simple Object Access Protocolt jelentette, de amióta a webszolgáltatások már többet jelentenek az objektumelérésnél, azóta ez egyezményesen csak SOAP, és nem rövidítés. A SOAP gyakorlatilag a habarcs a többi webszolgáltatás-technológia és a programozási keretrendszerek között. Ez az, ami képes az üzenetküldéseket az általunk kiválasztott protokollokon keresztül továbbítani és forgalmazni, vagyis gyakorlatilag ez felel azért, hogy a másik oldalon álló szoftver megértse a szabványos nyelven érkező üzeneteket, és a saját programozási nyelvének és környezetének megfelelő módon használhassa azt tovább.

Alulról a harmadik réteg alkotja az adat- és szolgáltatásleíró szintet. Az XML-üzeneteket az XML-séma (XSD) segítségével írjuk le, vagyis ez tartalmazza a hozzá kapcsolódó XML-üzenet felépítésének szabályait, illetve azt, hogy milyen adatok kerülhetnek még bele az általunk definiált szabályok értelmében. Szolgáltatásunk képességeit pedig a Web Service Description Language (WSDL) segítségével írjuk le. Ez gyakorlatilag egy olyan interfész, amelyik egyértelműen definiálja a külvilág számára, hogy az adott szolgáltatás mire is képes, milyen parancsokat támogat, milyen paramétereket (és típusokat) fogad, illetve ad vissza. A WSDL szorosan integrálódik az XSD-vel is, mivel a szolgáltatás által feldolgozható adatstruktúrákat gyakran XSD-ben fejezzük ki.

Az összes, ennél magasabban található réteg már sokkal kézzelfoghatóbb szolgáltatásokat valósít meg, bár még azok is csak a leggyakoribb kommunikációs feladatok absztrakciói, nem konkrét, működő szoftverek (például azonosítás, jogosultságkezelés, titkosítás). Azt, hogy azok közül mire is van szükségünk, az adott feladat határozza meg. A *2. képen* látható ábra például azt mutatja meg, hogy az általános rendszermenedzsmenthez milyen további rétegtechnológiák és szabványok szükségesek.



2. kép. A rendszermenedzsmentért felelős technológiák

Szabványosítási kitérő

Miért fontos, hogy szabványosak legyenek a webszolgáltatások? Leginkább azért, hogy a drágán megvásárolt, hosszú évek munkájával kifejlesztett szoftverrendszerek egymással is együtt tudjanak működni, és belőlük még komplexebb rendszereket lehessen képezni. És egyre inkább az a trend látszik, hogy a hardverek is bekapcsolódnak a webszolgáltatásokkal elérhető rendszerek közé, még ha azt a rajtuk futó firmware vagy más szoftver is teszi lehetővé.

A heterogén rendszerek együttműködésének érdekében a legnagyobb informatikai vállalatok létrehoztak egy szabványosítási testületet – ez a WS-Interoperability Organization –, ahol sorra veszik a felmerülő kérdéseket, és együtt specifikálják a webszolgáltatás-világ formátumait és szabályait, hogy az egyes gyártók megoldásai egymással kompatibilisak legyenek.

Milyen szabványok vannak még?

A WS-* szabványok további elemei alapvetően a következő csoportokra oszthatóak: metaadatokkal, üzenetkezeléssel, tranzakciókkal, biztonsággal, az üzenetek megbízható szállításával, adatleírással (XML), menedzsmenttel és üzleti folyamatok kezelésével kapcsolatos specifikációk. Ezek a specifikáció-csoportok a webszolgáltatások különböző rétegeire vonatkozóan tartalmaznak olyan további szabványokat, amelyek mind más-más esetben lehetnek fontosak, mivel a szoftverek közötti kommunikáció eltérő aspektusaival kapcsolatosak.

Lássunk egy gyors példát: a Windows Server 2003 R2 ADFS szolgáltatása (Active Directory Federation Services) a WS-* specifikációk segítségével képes arra, hogy akár HTTPS-en keresztül, XML és SOAP segítségével, biztonságosan kommunikáljon egy másik doménnel (WS-Security), és azzal bizalmi kapcsolatot építsen ki (WS-Trust), majd a WS-Federation szabvány segítségével megvalósítsa a két domén közti átjárhatóságot. Hasonló alapokra építkezik az InfoCard is, ami használja a WS-Federation, a WS-Trust, a WS-Security, a WS-SecureConversation és a WS-MetadataExchange specifikációkat, ezzel gyakorlatilag egy egész világra kiterjedő single sign-ont (SSO-t) valósítva meg.

Mindezek mellett léteznek olyan specifikációprofilok, amelyek a fenti szabványokat kombinálják és egészítik ki azzal a céllal, hogy a lehető leghamarabb lehessen szabványoknak megfelelő eszközöket és internetes webszolgáltatásokat készíteni a segítségükkel. Kitérnek a webszolgáltatások tervezése és implementálása körüli leggyakoribb teendőkre és problémákra. Az egyik ilyen a WS-I Basic Profile, ami általános (főként internetes) webszolgáltatásokkal foglalkozik, a másik pedig a Device Profile, ez olyan ajánlásokat ad, aminek segítségével az erőforrásokban nem bővelkedő hardverek és más, akár szórakoztatóelektronikai készülékek ruházhatók fel a szabványos együttműködés képességével. A Device Profile a lehető legkisebb részhalmaza a WS-* specifikációknak, hogy minél kevesebb erőforrást vegyen el az érintett eszköz valódi teendői elől.

További információk

Specifikációk – *http://msdn.microsoft.com/library/en-us/dnwebsrv/html/introwsa.asp*
Szabványok részletes leírása – *http://msdn.microsoft.com/webservices/webservices/understanding/specs/default.aspx; http://www.microsoft.com/windowsserversystem/dsi/default.mspx*

Szabványos megvalósítás

Bár áttekintésünkben épp csak érintettük a webszolgáltatások komplex területét, vélhetően sikerült felkelteni az érdeklődést a téma iránt, mivel egyelőre igencsak úgy néz ki, hogy ez a technológia mozgatja a kommunikáció jövőjét az informatikában. Lassan, de biztosan látható, ahogy az egyes termékekben sorra jelennek meg a WS-* specifikációk. Következő számunkban visszatérünk a rendszermenedzsment szabványos megvalósításának lehetőségeihez.

Budai Péter

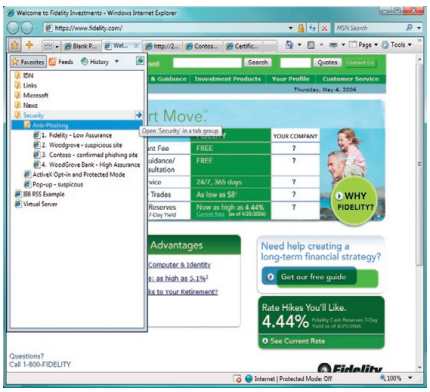
KÉNYELMESEBB, BIZTONSÁGOSABB

A legelterjedtebb böngésző új verziójának második bétakiadása már elérhető és letölthető az internetről.

Az új verzió teljesen újratervezett felülettel érkezik, funkciógombok helyett inkább a megjelenítési felület növelésére törekszik. Ebben sokat segít az is, hogy a keresés az eddigi megoldásokkal ellentétben nem külön eszköztáron kapott helyet, hanem közvetlenül a címsor mellett található meg.

Fülek

Aki eddig tabulált (többfüles) böngészést szeretett volna Internet Explorerben használni, annak telepítenie kellett az MSN Toolbart.



Az IE 7 fülkezelése azonban jóval többet tud a korábbi megoldásnál: lehetőségünk van a nyitott fülek csoportos elmentésére és visszaállítására, ezenkívül akár egy Alt+Tab-szerű, fülek közti váltást elősegítő ablakot is kaphatunk az éppen nyitott weboldalakról, hogy onnan választhassunk közülük. A füleket – ellentétben a Firefoxszal – közvetlenül az adott fül felületéről is bezárhatjuk, nem kell mindig elvinni az egeret az ablak jobb felső sarkába. Fontos információ lehet továbbá a gyorsbillentyűk használóinak, hogy egy linken a középső egérgombbal/görgővel kattintva az automatikusan egy új fülön nyílik meg.

Nyomtatás

Sok netezőnek okozhat gondot a szokásosnál szélesebb weboldalak nyomtatásakor az, hogy a tartalom egy része külön oldalakra kerül, vagy csak egyszerűen elvész (gondoljunk bele például, hogy ez a webre optimalizált táblázatoknál mekkora probléma lehet).

Az Internet Explorer 7 a nyomtatandó oldalakat képes automatikusan olyan méretűvé zsugorítani, hogy az ráférjen a lapra, ezzel elejét véve a lecsúszásoknak, lemaradásoknak. Ezenkívül beállíthatjuk a margókat, valamint testre szabhatjuk a fejlécet és a láblécet is.

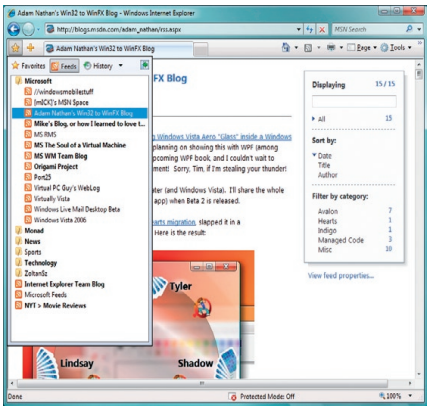
Nagyítás

Amennyiben egy weboldalon nem tudjuk elolvasni a szöveget, vagy egy képet nagyobb méretben szeretnénk megtekinteni, azt az új Nagyítás funkcióval probléma nélkül megtehetjük. Ez a funkció – ellentétben a korábbi böngészőkkel – a teljes weboldalt nagyítja fel, nem csak a szöveg méretét növeli meg.

RSS-csatornák támogatása

Ezentúl kedvenc focicsapatunk eredményeit és a hírportálok híreit is állandóan szem előtt tarthatjuk. Az Internet Explorer felismeri az RSS-csatornákat a böngészett weboldalakon, és nyomban felajánlja azok hozzáadását a kedvenceinkhez. Kérésünkre arra is képes, hogy automatikusan szinkronizálja azok tartalmát, a csatolt fájlokkal együtt.

A szinkronizálásnak hála, offline hírolvasásra is lehetőségünk van. Mindezeken túl az



IE 7 már maga is képes RSS-csatornákat megjeleníteni, és nem egy barátságtalan XML-állományt dob vissza nekünk.

Keresés

Az interneten történő keresésre eddig három lehetőségünk volt:

- navigálás egy keresőoldalra;
- kereső-eszköztár telepítése;
- keresősáv használata.

Ezek mindegyike kényelmetlennek bizonyult, és közülük egyesek még a tartalom elől is foglalták az értékes helyet. Az új felület jobb felső sarkában kapott helyet az új kereső, kényelmesebbé és gyorsabbá téve a munkát. A használni kívánt keresőmotor szabadon kiválasztható, alapértelmezés szerint az MSN Search, a Windows Live Search, a Yahoo! és a Google közül választhatunk, de ezeket utólag egyszerűen, egy kattintásra bővíthetjük más search providerekkel is.

Biztonság

Napjainkban egyre gyakrabban okoz problémát az adathalászat. Az új böngésző automatikusan figyeli a böngészett oldalakat, és adathalászatra (phishing) utaló tartalom esetén figyelmeztet minket. A phishing-szűrő kétséges helyzetekben kérésünkre egy webszolgáltatáson tárolt feketelistával is összehasonlíthatja az éppen meglátogatott oldalt.

Az ezzel kapcsolatos biztonsági figyelmeztetések sokkal határozottabbak lettek, érvénytelen SSL-tanúsítvány vagy adathalászó oldal esetén például a címsor pirosra változik, a megbízható helyeken böngészve azonban egy megnyugtató, zöld csíkkal találkozhatunk.

Az Internet Explorer második bétaverziója már letölthető a http://www.microsoft.com/ie oldalról.

Moldova György

Ahol a technológia és a lehetőség találkozik

Mi már látjuk a jövő tehetséges és lendületes IT szakembereit,

- akik a világ legnagyobb szoftvergyártójánál,
- Magyarország egyik legjobb munkahelyén dolgoznak,
- akiknek a szakmai és személyes fejlődés, a nemzetközi karrierlehetőség, a kihívást jelentő feladatok jelentik az értéket,
- akik a Microsoft technológiája iránti elkötelezettségüket igazán tűzközelből, inspiráló és dinamikus környezetben, egy remek csapat tagjaként élik meg.

Dinamikusan bővülő csapatunk az Ön számára is tartogathat szakmai és személyes kihívásokat!

Látogasson el a www.microsoft.hu/allasajanlatok oldalra!

Szakmai bemutatkozó anyagát aktuális ajánlatainkra és adatbázisunkba is várjuk, az allas@microsoft.hu címre!

Új generációs parancssoros felügyelet

Windows PowerShell: ezt a nevet kapta a keresztségben az a – fejlesztési ciklusának már-már végén járó – parancssoros eszköz, amelyet korábban Monad kódnéven ismertünk.

A PowerShell több, mint egy új szöveges konzol; olyan platform, amelyik megváltoztatja a Windows szerveralkalmazások adminisztrációjáról bennünk eddig kialakult képet. Cikksorozatunkban azt igyekszünk bemutatni, miben más a PowerShell, mint az eddig ismert felügyeleti eszközök.

A Monad születése

Az új parancssoros felügyeleti eszköz ötlete a Windows Services for Unix szolgáltatáscsomagjának fejlesztőiben merült fel. Ők a klasszikus értelemben vett „Igazi Programozók", akik bár már nem Fortranban programoznak, de igazán a Unix-terminálok előtt vannak elemükben. Megszokták, hogy ha szükség lenne rá, bármikor a kezük ügyében van a shell, sőt különféle shellek és scriptnyelvek, amelyek egyrészt az azonnali parancsok bevitelére, másrészt nagyon hatékony shell scriptek létrehozására is alkalmasak.

Igazi Programozóink viszont kényelmetlenül érezték magukat, amikor a Windows előtt ülve keresték azt az eszközt, amivel megoldhatnák az ilyen jellegű problémáikat. Lássuk csak: Command Prompt? – kicsit idejétmúlt, kicsit nehézkes, kicsit korlátolt (bár kétségtelenül a mienk). Windows Scripting Host (WSH)? – nem rossz, nem rossz, az előre gyártott COM-objektumok sokféle probléma megoldásában segítenek, de még mindig nem az igazi.

Egyrészt, a WSH-ból hiányzik az interaktivitás: a hagyományos értelemben vett shellek egyik fontos tulajdonsága, hogy – miközben előre megírt scriptek végrehajtására is alkalmasak, – az eljárásaink lépéseit akár soronként a konzolba pötyögve, azonnal is végrehajthatjuk.

Másrészt, ott van a Windowsban a .NET Framework, egy programozási keretrendszer, amely nagyon sok mindent lehetővé tesz, de egyelőre csak valamelyik .NET-es programozási nyelv használói számára – ráadásul ezek már programok, amelyeket fordítani kell, magyarul ismét elveszítjük az interaktivitás szabadságát.

Kellett tehát egy olyan eszköz, amely – kihasználva a .NET Framework erejét és a meglévő COM-objektumok szolgáltatásait – egyben:

- olyan interaktív, mint a bash vagy a ksh;
- annyira rugalmasan programozható, mint a Perl;
- beágyazható, mint a Tcl;
- olyan célorientált, mint az AS/400 CL vagy a VMS DCL.

A csővezeték (pipe)

A shellben használt parancsok, utasítások egy-egy jól definiált (al)feladat végrehajtására alkalmasak (ezért is hívják őket a PowerShell-világban „parancsocskáknak": cmdlet – ejtsd: kommandlet). Egy konkrét probléma megoldásához általában több parancs együttműködésére, azok sorozatára van szükség, ahol a későbbi parancsok az előző parancsok által már félig feldolgozott adattal dolgoznak. A parancsok közötti adatáramlás eszköze a csővezeték (pipe, |), ami a Unix-ban, DOS-ban egyaránt megszokott és gyakran használt dolog, például:

```
C:\> type boot.ini | more
```

Itt a type parancs kimenetén a boot.ini fájl tartalma jelenik meg (szöveges formában). A | jellel ezt beirányítjuk a more parancsba, amely aztán a neki átadott szöveget oldalakra tördelve jeleníti meg a képernyőn.

A shellek többségének csővezetékében tehát szöveges adat utazik. Ez az esetek egy részében tökéletesen megfelel az igényeinknek, máskor azonban kifejezetten kényelmetlen.

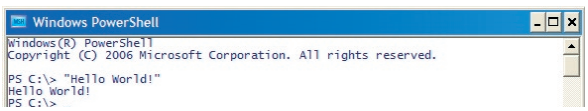
Gondoljunk például arra, hogy hogyan tudnánk kiszámolni egy adott könyvtárban található fájlok méretének összegét! Először is, kiadjuk a dir parancsot:

```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is F892-2F92

Directory of C:\

2006. 03. 10. 01:24                 0 AUTOEXEC.BAT
2006. 03. 10. 01:24                 0 CONFIG.SYS
2006. 05. 08. 14:19    <DIR>          Documents and Settings
2006. 03. 10. 22:25    <DIR>          Inetpub
2006. 05. 11. 08:57               174 MASK.txt
2006. 05. 10. 16:09    <DIR>          Program Files
2006. 05. 11. 08:56    <DIR>          WINDOWS
               3 File(s)            174 bytes
               4 Dir(s)   8 744 857 600 bytes free
```

(Most tekintsünk el attól, hogy az utolsó előtti sorban ez az adat már rendelkezésre áll.) Mit kell tennünk ezzel a szöveges információval? Kell egy intelligencia, ami képes ezt feldolgozni, azaz

- levágja az első és utolsó néhány sort (a fejlécekkel nem foglalkozunk);
- kiszűri azokat a sorokat, amelyekben szerepel a <DIR> szó;
- a maradék sorokban felismeri a dátumot és a fájlnevet, megkeresi azt a pozíciót, ahol (valószínűleg) a fájl hossza található, majd számmá konvertálja azt;
- nem zavarják olyan apróságok, mint a dátum formátuma, a nyelv, a körülményektől függő formázási különbségek stb.

Ha jól belegondolunk, akarva-akaratlanul egy csomó felesleges munkát okozunk magunknak. A dir parancs belül nyilván valamiféle objektumokkal dolgozik (ezek a könyvtárban található fájlokat jelképező objektumok), amelyekből a parancs azután egy emberi fogyasztásra alkalmas, szöveges kimenetet generál.



A Hello World program a PowerShell-ben

A következő parancs ezt a szöveges információt kapja meg, és ebből igyekszik előállítani ugyanazt az objektumhalmazt (vagy annak egy kisebb részét), amit a dir megcsócsált, majd eldobott. Nyilvánvaló a környezetszennyezés.

Ezzel szemben: a PowerShell cmdletek között nem szöveges adat, hanem .NET-objektum (vagy azok halmaza) mozog. Minden cmdlet kimenete .NET-objektum, és a legtöbb cmdlet valamelyik paraméterét képes a bemenő csővezetékből venni. Szöveges formába csak akkor alakul, ha mi ezt kifejezetten kérjük, vagy ha a csővezeték véget ér, és tartalma a felhasználói konzolba csordogál. Egészen addig a pillanatig teljes értékű, megfogható, élő, paraméterekkel rendelkező objektumokkal dolgozunk.

A fenti példa PowerShellben egyébként például így festhetne:

```
PS C:\> Get-ChildItem | Measure-Object -Sum Length

Count    : 3
Average  :
Sum      : 174
Maximum  :
Minimum  :
Property : Length
```

A PowerShell parancsai, a cmdletek

Mielőtt további mélyebb boncolgatásba kezdenénk, szót kell ejtenünk a cmdletekről is általában. A PowerShell nem titkolt célja, hogy a Windowsban idővel kiváltsa az évek óta megszokott parancssoros konzolt. Ennek egyik feltétele a kompatibilitás és a könnyű megtanulhatóság – látni fogjuk, hogy a fejlesztők erre is nagy hangsúlyt fektettek.

A PowerShellben kiadott parancs lehet egy, az elérési útban lévő meglévő alkalmazás (calc.exe), előre elkészített PowerShell-script (hello.ps1), a PowerShell beépített cmdletje (get-help), alias és függvény. Utóbbi kettőről később lesz szó.

Minden cmdlet neve a könnyű, intuitív megjegyezhetőség érdekében ige-főnév formátumú, a főnév mindig egyes számban van, például: get-service. A cmdleteknek még a paraméterezése is „szabványosított”: vannak olyan paraméterek, amelyek minden cmdletben megtalálhatók (például a –Verbose vagy a –Confirm), és a további paraméterek neve is illeszkedik a többi cmdletben használtakhoz.

A legtöbb paraméter értékének megadásakor használhatjuk a joker-karaktereket (get-service –ServiceName p*), de nem kell feltétlenül kiírnunk a paraméter teljes nevét, elég csak annyit, amennyiből már egyértelmű, hogy mire gondolunk (get-service –s p* -ex plugplay). Sőt, miután a –ServiceName paraméter az alapértelmezett, kiírása nem kötelező (get-service p*).

Ráadásul a joker-definíció bármikor lehet reguláris kifejezés is, ami jócskán kiterjeszti a mozgásterünket (get-service [p..s]*).

További információk

Az „Igazi Programozó” – *http://grin.hu/funtxt/vegyes/igazi_programozo.txt*
A shell letöltése – *http://www.microsoft.com/downloads/details.aspx?FamilyId=2B0BBFCD-0797-4083-A817-5E6A054A85C9*

A súgó-cmdlet neve get-help. Ha önmagában adjuk ki, saját magáról jeleníti meg a súgó információt. Érdemes a | more paranccsal együtt használni.

A súgó súgójából kiderül, hogy a get-help * paranccsal listázhatjuk az összes súgótémát, egy-egy témát vagy cmdlet-nevet paraméterként megadva (például get-help get-service vagy get-help about_pipeline) pedig a cmdlet, illetve a téma leírását.

Ha már a súgóknál tartunk, a másik hasznos cmdlet a get-command. Ez a beépített cmdletek listázására szolgál, kereshetünk vele ige, illetve főnév szerint is:

```
PS C:\> get-command -noun service

CommandType Name            Definition
----------- ----            ----------
Cmdlet      Get-Service     Get-Service [[-Name] <String...
Cmdlet      New-Service     New-Service [-Name] <String>...
Cmdlet      Restart-Service Restart-Service [-Name] <Str...
Cmdlet      Resume-Service  Resume-Service [-Name] <Stri...
Cmdlet      Set-Service     Set-Service [-Name] <String>...
Cmdlet      Start-Service   Start-Service [-Name] <Strin...
Cmdlet      Stop-Service    Stop-Service [-Name] <String...
Cmdlet      Suspend-Service Suspend-Service [-Name] <Str...
```

Az eddig megismertekből már kiderült, hogy egy szolgáltatás leállítását kétféleképpen is megtehetjük:

```
PS C:\> stop-service mssqlserver -confirm -force

Confirm
Are you sure you want to perform this action?
Performing operation „Stop-Service” on Target „MSSQLSERVER (MSSQLSERVER)”.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is „Y”):
```

A fent látható példa az általános – Confirm paraméter működését mutatja, ezenkívül – il-

letve a csővezetékkel is megoldhatjuk a dolgot:

```
PS C:\> get-service mssqlserver | stop-service -force
```

Providerek

A rendelkezésre álló beépített cmdletek listája egyébként nem korlátozott. A PowerShell bővíthető egy-egy területre kifejlesztett további szolgáltatásokkal, illetve az ehhez tartozó parancsokkal. Ha kiadjuk a get-psprovider cmdletet, láthatjuk az aktuálisan telepített providerek listáját:

```
PS C:\> get-psprovider

Name        Capabilities          Drives
----        ------------          ------
Alias       ShouldProcess         {Alias}
Environment ShouldProcess         {Env}
FileSystem  Filter, ShouldProcess {C, D, E, F...}
Function    ShouldProcess         {Function}
Registry    ShouldProcess         {HKLM, HKCU}
Variable    ShouldProcess         {Variable}
Certificate ShouldProcess         {cert}
```

Látjuk, hogy a fájlrendszer mellett további adatszolgáltatók is léteznek. Nem minden provider ad új parancsokat a rendszerhez, vannak, amelyek csak egy-egy adattár elérését biztosítják (mint például a környezeti változókat tartalmazó Environment). A Registry provider például a registryhez történő hozzáférést teszi lehetővé – ennek köszönhetően ugyanazokat a cmdleteket használhatjuk a registryben történő navigáláshoz, annak módosításához stb., amelyeket már más területeken megszoktunk.

```
PS C:\> cd HKLM:\SYSTEM\CurrentControlSet\Services\Spooler
PS HKLM:\...\Spooler>
```

A cmdletekre barátságosabb neveket, aliasokat is ragaszthatunk – sőt, a PowerShell alapértelmezésben körülbelül száz aliast előre definiál (lásd: get-alias). A legtöbb régi megszokott DOS-os parancs is alias formájában él tovább, csak néhány példa:

```
PS C:\> get-alias cls,dir,rm,del,type

CommandType Name Definition
----------- ---- ----------
Alias       cls  Clear-Host
Alias       dir  Get-ChildItem
Alias       rm   Remove-Item
Alias       del  Remove-Item
Alias       type Get-Content
```

Az alias egyébként csak a cmdlet nevének lecserélésére alkalmas, azaz nem lehet például paramétereket „bedrótozni” az aliasba – erre más megoldást nyújt a PowerShell. Természetesen saját aliasokat is létrehozhatunk a set-alias segítségével.

Formázás

Arról már volt szó, hogy amikor a cmdletek kimeneteként keletkező .NET-objektumok kiérnek a csővezetékből, szöveges formába konvertálódnak. Ha egymás után kiadjuk a get-service, a get-date, illetve a get-wmiobject win32_computersystem parancsot, mégis különböző jellegű kimenetet kapunk. A get-service eredménye egy táblázat, benne oszlopok a szolgáltatás paraméterei. A get-wmiobject eredménye ezzel szemben soronként tartalmazza az objektum paramétereinek értékeit. Ráadásul abban is biztosak lehetünk, hogy a get-service által visszaadott szolgáltatás-objektumnak háromnál több paramétere van. Végül a get-date egyszerűen csak kiírja a dátumot a konzolra.

Biztosnak látszik, hogy a formázás valamitől függ – és ez így is van. Elsőre arra gondolnánk, hogy a használt cmdlet határozza meg a kimenet formátumát, de a valóság ennek éppen az ellenkezője: a szöveggé konvertálás formátuma éppen attól függ, hogy milyen típusú a konvertálandó objektum, az adat. Ha a PowerShell ismeri a kapott objektum típusát, akkor alapértelmezésben a meghatározott formátumba végzi a konverziót. Keressünk .Format.ps1xml-re végződő nevű fájlokat a Program Files\Windows PowerShell mappában! Ezek tartalmazzák (XML-formátumban) az ismert objektumtípusok leírását és a konvertálás szabályait. Itt formázhatjuk, szűrhetjük a megjelenített attribútumokat, de akár új (dinamikusan számított) attribútumokat is adhatunk az objektumhoz.

```
PS C:\> get-childitem cert:\CurrentUser\My\
Directory: Microsoft.PowerShell.Security\Certificate::CurrentUser\My
Thumbprint                               Subject
----------                               -------
D8524F8EB0C749C15D8C4D76F26CEADAACD2D8FB CN=Miklos Fulop
D4D7B44C3B59F963CBF740CAD5EE98D0B66ABEE1 E=mfulop@microsoft.com, CN=Mik...
ADA5AA88866E3280F072D645297EBA75CEA5F2AF CN=Miklos Fulop, OU=UserAccoun...
```

Természetesen nem vagyunk kötve az alapértelmezett formázáshoz: a format-* kezdetű cmdleteket használhatjuk a kimenet testre szabásához. Az egyik legegyszerűbb formázó cmdlet a format-list. Ez a cmdlet a neki átadott objektum(ok) attribútumait soronként listázza ki (paraméterként azt is megadhatnánk, hogy melyeket):

```
PS C:\> get-service plugplay | format-list Name, DependentServices

Name            : PlugPlay
DependentServices : {RasAuto, RasMan, TapiSrv, SCardSvr...}
```

Ha nem adunk meg attribútumot, akkor a nem-üres attribútumokat fogja listázni (format-list * használata esetén minden attribútum megjelenik). Több objektum esetén a felsorolás újrakezdődik.

A format-table cmdlet táblázatos formába hozza az objektumokat, például:

```
PS C:\> get-process iex* | format-table ID, ProcessName, StartTime

  Id ProcessName StartTime
  -- ----------- ---------
 948 iexplore    2006. 05. 11. 9:24:15
2816 iexplore    2006. 05. 11. 8:59:08
3076 iexplore    2006. 05. 11. 11:59:21
3604 iexplore    2006. 05. 11. 11:05:34
```

Az attribútumok helyén nem csak a formátumfájlokban, de itt is lehetnek számított értékek:

```
PS C:\> get-process iex* | format-table ID, ProcessName,
@{expression={((get-date).Subtract($_.StartTime)).TotalSeconds};
width=30;label="RunTime (s)"}

  Id ProcessName RunTime (s)
  -- ----------- ----------
 948 iexplore    11831,4049265
2816 iexplore    13338,1094405
3076 iexplore    2524,80118
3604 iexplore    5752,4534012
```

Házi feladat

A PowerShell megismerése hosszú folyamat – még több hónapnyi együttélés után is tud meglepetéseket okozni. Addig is, míg a következő részben továbbléphetünk a PowerShell látványosabb területei felé, mindenkinek javasolható, hogy töltse le, telepítse fel és próbálja ki a shellt. A get-command és a get-help cmdletek bőséges olvasnivalót biztosítanak a következő néhány hétre. Kedvcsinálónak közöljük egy PowerShell-ben írt RSS-olvasó forráskódját.

```
PS C:\> ([xml](New-Object
Net.WebClient).DownloadString("http://blogs.msdn.com/powershell/
rss.aspx")).rss.channel.item | Format-Table Title, Link
```

Fülöp Miklós

IT-SECURITY TODAY

INFORMATIKAI BIZTONSÁGI HAVILAP NAPI ONLINE TÁJÉKOZTATÓJA

- informatikai döntéshozóknak, technológiai szakembereknek
- az elmúlt 24 óra legfontosabb hazai és külföldi informatikai biztonság és információbiztonság hírei
- ingyenes napi online hírlevél

Regisztráljon!

www.it-business.hu/hirlevel

KÉTSZER HÚSZ ÉRV I.

Az üzemeltetők egy része az ISA Server 2004 Standarddal kapcsolatban a tervezés, illetve a bevezetés fárasztó óráit, napjait éli, és sokan vannak, akik még nem tértek át az ISA 2000-ről, de szeretnének.

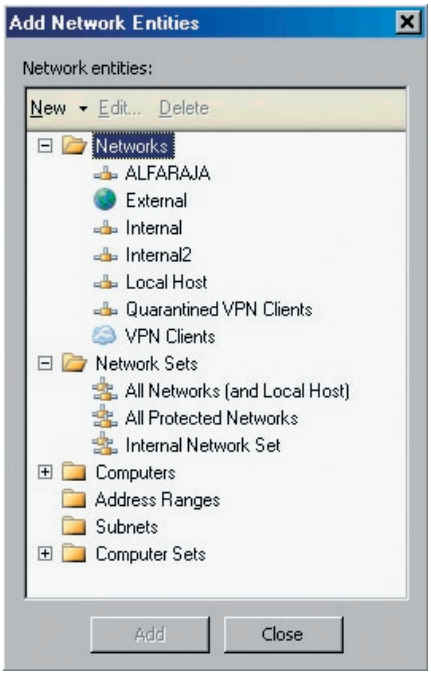
Kétrészes cikkünkben – összesen negyven pontban – az ISA Server 2004 Standard változatának összegyűjtött kulcsfontosságú jellemzőit, előnyös vonásait ismertetjük, kiegészítve a gyakorlatban felhalmozott tapasztalatokkal, valamint egy – szubjektív – szolgáltatási hiánylistával.

1. Több hálózat támogatása

Szemben az ISA 2000-zel, az ISA 2004 tetszőleges számú hálózat kezelését ajánlja fel. A „hálózat" szó értelmezésénél kicsit tekintsünk el a hagyományos definíciótól, abszolút nem fizikai hálózatról van szó (bár persze ez is lehetséges), hanem logikai alapon tervezhetjük meg a konfigurációt. Ennek fényes példája az előredefiniált „Local Host" hálózat, amely maga az ISA 2004 Server gép. Ez a megoldás jelentősen egyszerűsíti az életünket, gyakorlatilag teljesen ugyanolyan feltételekkel (tűzfalszabályok, web proxy, kivételek stb.) kezelhetjük ezt a „hálózatot", mint a belsőt vagy a külsőt. De mi az, hogy belső? Ha akár 1000 hálózatunk is lehet, akkor miért is nem lehet több belső, azaz minek egyetlen dedikált belső (internal)? A kérdés jogos: többé valóban nem kell foglalkoznunk például a LAT-tal – annyi logikai/fizikai alapú „belső" hálózatot kreálunk, amennyire csak szükség van.

Kényelmes dolog az is, hogy ezeket a hálózatokat tetszőlegesen, igényeink szerint rakosgathatjuk ilyen-olyan csoportokba (és itt is vannak „gyáriak"), ez a lehetőség például a tűzfalszabályok legyártásánál kifejezetten jól jön. Az ISA-konzolon a faszerkezetben a Configuration > Networks pont alatt a „Local Host" hálózat mellett előredefiniálva találhatunk még négy hálózatot:

- Internal: a telepítés alatt megadható azért egy belsőnek szánt tartomány, amely általában szükséges is;
- External: minden olyan hely, ami nincs megadva IP-tartománnyal, azaz a külső hálózat, tipikusan az internet;
- VPN Clients: az ISA-ra beérkező VPN-kliensek hálózata;
- Quarantined VPN Clients: működő VPN-karantén esetén, az első lépcsőfok ez a hálózat a VPN-kliensek számára.



Egy tűzfalszabály létrehozása közben válogatunk a hálózatok vagy a hálózatcsoportok közül

2. Hálózatszintű házirend

De miért jó a logikai szeparáláson kívül a több hálózat? Rengeteg okból. Ezek egyike az adott hálózatra testre szabható tűzfalszabályok alkalmazása. A legtöbb helyen nyilván szükséges egy DMZ (perimeter) hálózat a kívülről is elérhető web-, mail- stb. szerverek biztonságos publikálása céljából. Ez egy külön hálózat lesz az ISA-ban is, amelyet viszonylag egyszerűen képesek is leszünk létrehozni, majd aztán a többi hálózattól eltérő tűzfalszabályokkal (például publikálás, web-, ftp- stb. hozzáférés, hozzáférés belső hálózatból) üzemeltetni. Nem kell kínlódni különböző, az ISA 2000-ben megszokott ilyen-olyan irányú packet filterekkel, ugyanazokat a szabályteremtő mechanizmusokat használjuk, mint minden más hálózatnál, de a szabály hatókörére testre szabhatóvá vált.

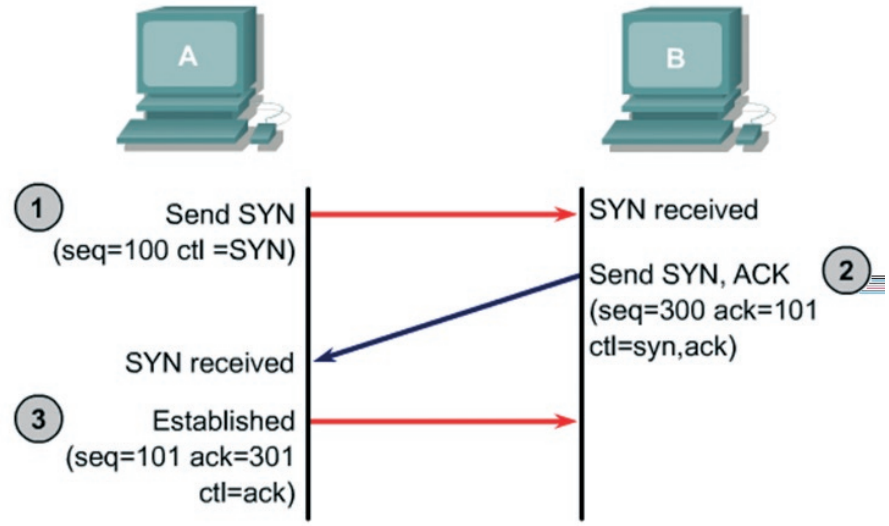
3. Hálózatok kapcsolata

A tömeges hálózatteremtési lehetőségből adódik az is, hogy ezeket a hálózatok közötti kapcsolatokat is szabályozni kell, az eddigi bedrótozottnál hatékonyabban. Az ISA 2004-ben bármely két hálózat között – a kapcsolat célirányosságától függően – „Route" illetve „NAT" típusú lehet a forgalom. Az utóbbit tipikusan a belső hálózat vagy a VPN-kliensek és a külső hálózat (internet) közötti kapcsolatban alkalmazzuk, mivel a címfordítás itt szükséges igény. A szimpla „Route" pedig például a több belső hálózat vagy például a VPN-kliensek és a belső hálózat közötti kapcsolat beállítása lehet. Fontos tudni, hogy ennek a lehetőségnek a beállítása még kevés ahhoz, hogy működjön a kapcsolat az adott

hálózatok között, ugyanis az engedélyező tűzfalszabályok nélkül ez is csak előjáték.

4. VPN-hálózatok ellenőrzése

A klasszikus TCP-forgalomban való alkalmazás mellett az ISA 2004 a VPN-kapcsolatokban is képes használni a csomagszűréshez a „Three-way handshake" („háromujjas kézfogás") módszerrel dolgozó stateful filteringet, megteremtendő a forgalmazásban részt vevő két oldal egymás iránti, kölcsönös bizalmát. Ez a lehetőség elsősorban abból adódik, hogy



A three-way handshake, azaz syn-syn-ack-ack

a VPN-kliensek külön hálózatot „kaptak", amely az eddigiek értelmében szintén jobban felügyelhető, és tetszés szerint tűzdelhetjük meg saját tűzfalszabályokkal is. Ám a stateful filtering nem jár ekkora szabadsággal, nem konfigurálhatjuk szabadon, mindig dolgozik.

5. A Site-to-Site VPN-hálózatok ellenőrzése

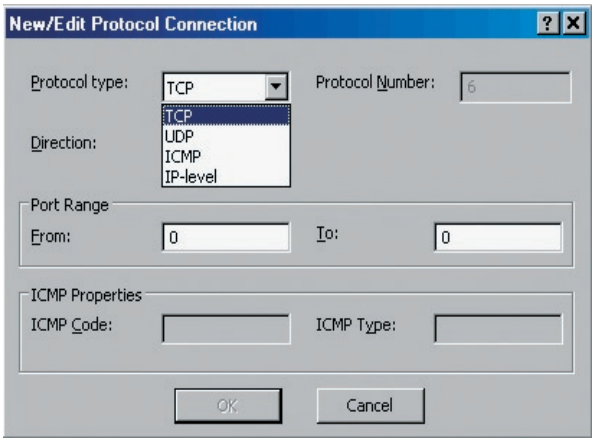
Az ISA 2000-ben a Site-to-Site VPN-hálózatok esetén nem volt lehetőségünk a kontrollra, nem volt semmilyen szűrési mód vagy opcionális tűzfalszabály-alkalmazás. Az ISA 2004-ben ez szerencsére változott, egyrészt a stateful filtering itt is működik, másrészt felhasználó-, illetve csoportszintű szűrésre is van lehetőség.

6. SNAT-támogatás a VPN-klienseknek

Szintén teljesen hiányzott az ISA 2004 megjelenéséig az a lehetőség, hogy a ISA VPN-kiszolgálóhoz csatlakozott VPN-ügyfelek működő tűzfalkliens nélkül is internet-hozzáféréshez jussanak. Ez a lehetőség immár adott az SNAT-kliensek számára is (a SecureNAT a legkevésbé macerás ISA-kliens, elég neki az alapértelmezett átjáró IP-címe, nem kell telepíteni, konfigurálni semmi egyebet), így nem kell bajlódni a tűzfalkliens telepítésével.

7. VPN-karantén

Az ISA 2004 kibővíti a Windows Server 2003 RRAS VPN-karanténszolgáltatását, illetve a Windows 2000 kiszolgálókon is lehetővé teszi ennek a technikának az alkalmazását. A VPN-kliensek alapértelmezésben nem kapnak hozzáférést a belső hálózathoz, hanem a speciális VPN-kliens (amelyet az üzemeltető állít elő a Windows részeként feltelepíthető Connection Manager Administration Kittel), illetve az ISA-ra telepített VPN-karanténszolgáltatás kommunikál egymással először. Ennek eredményeképpen csak bizonyos feltételek (bekapcsolt tűzfal, friss vírusirtó-adatbázis, biztonsági frissítések megléte stb.) teljesítése után léphet át a sztenderd VPN-klienshálózatba a távoli gép. Ellenkező esetben a kapcsolat automatikusan megszakad, és ez így lesz mindaddig, amíg nem teljesülnek az üzemeltető által meghatározott feltételek.



A lista alján az „IP-level" sor lesz az érdekes

8. PPTP-szerverpublikálás

Hála a kibővített protokolltámogatásnak, immár nemcsak L2TP/IPSec NAT-T VPN-szervereket lehetséges publikálni a belső hálózatból, hanem például az egyszerűen létrehozható, minimális igénnyel fellépő, ám azért elégségesen biztonságos PPTP-protokollt használó VPN-kiszolgálókat is. Ráadásul a kapcsolat biztonságossá tételéhez az ISA 2004 rendelkezik egy integrált PPTP-alkalmazásszűrővel is.

9. Az IPSec-tunnel használata a Site-to-Site VPN-nél

Az ISA 2004-ben megjelent a harmadik protokoll a hálózatok biztonságos összekötésére, és ez az IPSec (önmagában). Azért rendkívül fontos ez, mert egy sor hardveres router (a SOHO-kategóriából) is támogatja ezt a VPN-technikát, vagyis egy telephelyes hálózatban (ha nem akarunk vagy nem tudunk, illetve nem fontos a telephelyenként 1-1 ISA-kiszolgálót is bevetni) a biztonságos forgalom biztosítása végett viszonylag egyszerűen ki lehet építeni ezekből az eszközökből és a központi ISA-szerverből a háttér-infrastruktúrát.

10. Kiterjesztett protokoll-támogatás

Az ISA 2000 (egyébként nem kevés elemet tartalmazó) előredefiniált protokollkészlete kibővült az IP-szintű protokollok támogatásával. Így válik lehetővé a TCP-, az UDP- és az ICMP-protokollok mellett például az említett PPTP-kiszolgálópublikálás (IP 47), illetve a ping és tracert használata a kliensoldali alkalmazásokból, vagy akár az IPSec-forgalom engedélyezése.

11. A komplex protokollok használata

A streaming media és az egyéb audio/video-forgalmat eredményező alkalmazások arra kényszerítik a tűzfalszoftverek készítőit, hogy komplex, többszörös elsődleges és másodlagos protokolltámogatást is beépítsenek a termékeikbe. Az ISA 2000-nél ezeknek az igényeknek megfelelve bonyolult szkriptekkel kellett megtámogatni, illetve kibővíteni a kimenő forgalom elsődleges protokollszabályait. Az ISA 2004-nel viszont nincs erre szükség, az új protokollvarázslóval felvehetünk több elsődleges, illetve másodlagos protokollt is. (Meg kell jegyezni, hogy a házon belüliek mellett a konkurens streaming media-szerverek alkalmazásszűrői is szép számmal képviselve vannak az ISA 2004-ben.)

12. Testreszabható protokolldefiníciók

Amikor az ISA 2004-ben kreálunk egy tűzfalszabályt, lehetőségünk van arra, hogy bármely protokoll tulajdonságai között (a panel jobb alsó sarkában keressük) határokat szabjunk – vagy ellenkezőleg: egyáltalán ne limitáljuk – a használható forrás-, illetve célportok tekintetében. Ez a lehetőség értelemszerűen megtalálható a publikálószabályoknál is, kibővítve a tűzfal és a publikálószerver vonatkozó portjainak megszorításával együtt.

13. ISA-felhasználói csoportok

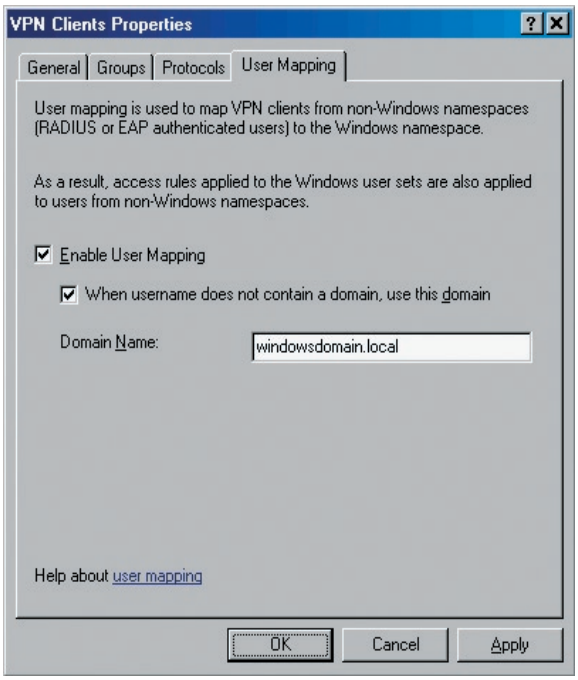
ISA 2000 esetén, ha különbséget szeretnénk tenni felhasználók szerint például az internetelérés fokozataiban, azaz hitelesítéshez kötjük a web proxy használatát, akkor a felhasználói fiókokat csak a lokális felhasználói adatbázisból vagy a tartományi címtárból vehetjük – közvetlenül. Ami egyúttal azt is jelentette, hogy ha teljesen logikusan, csoportokat szerettünk volna létrehozni e fiókok hozzáférési mértékének megfelelően, akkor ezeket a forrásokat többnyire rendszergazdai jogosultsággal kellett elérnünk, és muszáj volt például közvetlenül a címtárban matatnunk. Ennek akár vége is lehet, mert az ISA 2004-ben közvetlenül is létrehozhatunk csoportokat, majd azokba belehelyezhetjük a különböző névterekből (például az AD-ból) betallózott felhasználókat, csoportokat. Nagyobb szervezetek esetén ez azért is fontos, mert ennek megfelelően el lehet különíteni egymástól az ISA Admins és a Domain Admins csoportokat (a helyi rendszergazdai csoportban viszont továbbra is bent kell lennie az ISA-t telepítő, illetve üzemeltető felhasználói fióknak).

További információk

http://www.tjszki.hu/gtamas/publikaciok/
http://www.rsasecurity.com/node.asp?id=1157

14. A tűzfalkliens jogosultságának továbbítása

Már a korábbi ISA-nál is működött az a lehetőség, hogy a tűzfalkliensek gyorsítótárra vonatkozó kéréseit a HTTP Redirector elküldte a web proxy szervizének, így a tűzfalkliensek is megkaphatták a gyorsítótár tartalmát. A gond abból adódott, hogy a felhasználói jogosultságok egyúttal elvesztek ebben a folyamatban, és ha a web proxynak muszáj volt azonosítania, akkor a kérés gyakorlatilag negligálódott. Az ISA 2004-ben viszont elképesztően jó irányt vettek a web proxy szolgáltatások, illetve a függőségi viszonyok! Nincs többé külön szerviz a web proxyhoz (olyan alkalmazásszűrő lett belőle, amelynek csak előnyei vannak a korábbi implementációhoz képest), nincs többé HTTP Redirector, van viszont intelligens http-filter, ami egy az egyben képes átadni minden adatot például a tűzfalkliens és a gyorsítótár közötti forgalomban is (az SNAT-kliensek hasonló kéréseivel is ez a helyzet, csak ott nem beszélhetünk jogosultságokról és hitelesítésről). A web proxy szolgáltatást viszont már nem szükséges bevonni ebbe a körbe.



Mindent összekötünk mindennel

15. RADIUS-névtér a hitelesítésnél

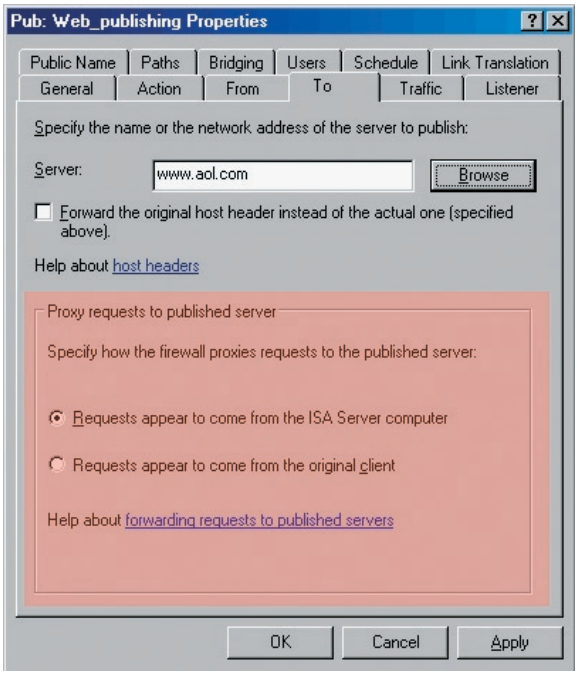
Mint említettük, kibővült a jogosultságok, hitelesítési lehetőségek eszköztára is. Ez azt jelenti, hogy egyáltalán nem szükséges az Active Directory közvetlen használata, azaz egyáltalán nem kötelező beléptetni a tartományba az ISA-kiszolgálót, akkor sem, ha a címtárból szeretnénk felhasználói fiókokat, csoportokat használni.

A RADIUS-névtér elsődleges használata persze azt eredményezi, hogy például Unix-platformról érkező hitelesítési kéréseket is képes feldolgozni az ISA 2004 web proxyja, azaz a RADIUS-on keresztül érkező felhasználók kiszolgálója is lehet egy ISA Server 2004. Sőt, például VPN-kliensek esetén képes az ISA Server 2004 a felhasználói nevek automatikus hozzárendelésére, azaz a „user mapping”-re.

Ez az opciót azért találták ki, hogy az értelemszerűen nem egy tartományból érkező, windowsos hitelesítésre képtelen felhasználói fiókot megfeleltessük egy tartományi felhasználóként. Így ha egy azonos nevet kreálunk a címtárban, akkor gyakorlatilag össze is kötöttük (de csak az ISA-n érvényesülő) jogosultsági szempontból a két névteret. Ha ezt megtesszük, akkor a RADIUS-on már túljutott (hitelesített) felhasználót az ISA 2004 tűzfalszervize az adott tűzfalszabálynak megfelelően feljogosítja a web proxy használatára, ugyanúgy, mintha a Windows-névtérből érkezne.

Visszatérve az ISA 2004 tartományba léptetésének szükségtelenségére, a megoldáshoz szintén a RADIUS-t, azaz a Windows RADIUS-át, az IAS-t (Internet Authentication Servert, egy teljesen RFC-kompatibilis, Windows Server 2000/2003 alá egyaránt feltelepíthető komponenst) kell használnunk. Egyszerűsítve a leírást, ekkor az ISA 2004 RADIUS-kliensként viselkedik, az IAS lesz a kiszolgálója, és az IAS lesz egyúttal a kapocs a címtár és az ISA kö-

zött. Ha az ISA web proxyjának szüksége lesz hitelesítési információra, akkor végigjárva ezt az utat, megkaphatja a címtárból. E megoldás feltétlen előnye, hogy teljesen elválasztjuk az ISA-kiszolgálónkat a tartománytól, azaz az alapesetben meglehetősen paranoid tűzfalgazdák is nyugodtabban alszanak.



A jelenlegi állapot szerint nem sok minden derül ki a webszerver-logból

16. A „Basic" hitelesítés delegálása

A publikált webszervereknél (nemcsak a sima IIS-mappáknál, hanem Exchange OWA, FBA, RPC over HTTP stb. esetén is.) az ISA 2004 átveszi a jegyvizsgáló kalauz szerepkörét, azaz még a belső webszerver előtt megvizsgálja a hitelesítési információkat, és el is bírálja ezeket. E kedves gesztus révén kevésbé terheljük a belső webszervert, ráadásul a nem passzoló kérést nem engedjük be a belső hálózatba, már a kapunál lebukik. Azonban logikusan gondolhatnánk azt is, hogy akkor még egyszer meg kell adnunk a minimálisan szükséges felhasználónév–jelszó párost az ISA-n túljutva, a webszerver kérésére. Szerencsére nem, az ISA szépen továbbadja ezt az információt a webszervernek, vagyis nem lesz duplikált hitelesítés. Ez egy szép kerek történet, ami hiányzik még belőle: a megvalósításhoz fel kell keresni az adott publikálószabályunkat (egyesével), és ki kell pipálnunk a „Forward Basic authentication credentials (Basic Authentication)" négyzetet a „Users" panelen.

17. Valós IP-információk a webszerver-logban

Akár jelentéktelen dolognak is tekinthetnénk ezt az opciót, de azért gondoljunk bele: jobban örülnénk, ha a belső webszerverünk naplói az ISA-kiszolgáló belső IP-címét tartalmaznák állandóan, az igazi „érdeklődők" IP-címei helyett?

Egy kissé nehéz lenne ebben az esetben például hibátlan statisztikát készíteni, mivel az ISA IP-je mindent vinne, hiszen a webszerver ilyenkor nincs közvetlen kapcsolatban a nagyvilággal, csak az ISA-kiszolgálóval.

18. Az RSA SecurID-hitelesítés

Eljutottunk a harmadik névtérhez is, amelyet az ISA 2004 képes kezelni, ez pedig az RSA cég komoly lehetőségekkel felvértezett megoldása. A SecurID-hitelesítés kétfaktoros hitelesítés, azaz szükséges hozzá egy hardveres kulcs (például egy pendrive-ba építve vagy egy külön csak erre használható eszköz, vagy esetleg egy smartcard), amely egy 60 másodpercenként változó, csupán egyszer használatos számkombinációt generál a kijelzőjére, és amelyet egy, a felhasználó által ismert PIN kóddal párosítva egy „passcode"-ot kaphatunk.

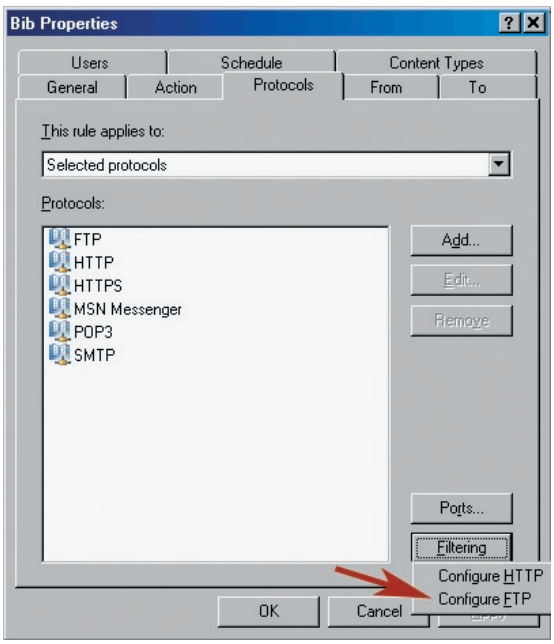
A hitelesítéskor ezt a kódot elküldve a szerveroldali alkalmazás (jelen esetben az ISA) képes az adott felhasználót egyedileg azonosítani, és mindezt a szokásoshoz képest nagyobb bizonyossággal, mivel a PIN kód (mint jelszó) mellett egy másik kútfőből származó adatra is szükség van a művelethez, amely ráadásul állandóan változik (és amelyet a felhasználó nem is irkálhat ki a monitorra, asztalra, tenyerébe stb.). Ennek a megoldásnak a támogatása egyébként már az ISA 2000 Feature Packban is megvolt, de most végleg beépítették a web proxy hitelesítési lehetőségeit kiegészítve.

19. Delegálásvarázsló

Mint már tudjuk, az ISA telepítéséhez és teljes körű üzemeltetéséhez minimum helyi rendszergazdai jogosultság kell, de a hozzáféréshez nem feltétlenül. Három szerepkör is létezik, az egyik a korlátlan úr (ISA Full Administrator), a másik (gyengébb) az ISA Server Extended Monitoring, amelyhez a monitorozással kapcsolatos beállítások kezelése és az ellenőrző folyamatok teljes körű megtekintési joga tartozik, míg a harmadik szerep az ISA Server Basic Monitoring. Ez a legkevésbé erős szerepkör; használója csak betekintést nyerhet az ISA naplóiba, ellenőrizheti a hálózati forgalmat, de nem konfigurálhat semmit.

20. FTP policy

Sok kezdő ISA-rendszergazda életét megkeserítő lehetőségről van szó, ezt az opciót ugyanis elég nehéz megtalálni, viszont lehetetlenné teheti a feltöltést, akkor is, ha egyébként minden jog és megengedő szabály a rendelkezésünkre áll. Két helyen szabályozhatjuk az FTP-forgalmat, egyrészt az Add-ins > Application Filters listában a teljes ISA-ra nézve kikapcsolhatjuk a szűrést, de azoknál a szabályoknál is



Protocols > Filtering > Configure FTP > Read-Only

van (alapértelmezésben!) egy feltöltést blokkoló pipa, ahol szerepel az FTP-protokoll.

Gál Tamás

Microsoft Virtual Server I.

Sokan és sokféleképpen szeretnék bebizonyítani, megmutatni, hogy az egykor PC-igarágnak nevezett valami „felnőtt” korába lépett.

Születésnapi rendezvénye volt nemrég az Apple-nek, az AMD-nek, az Intelnek, a PC-nek, a Windowsnak, a Microsoftnak és megannyi más, fontos ICT-szereplőnek és -márkának. A Wintel-platform érettségét leginkább a kiszolgálókban megjelenő virtualizációs képesség mutatja.

A virtualizácó – bár már évek óta jobbnál jobb termékek bizonyítják a létjogosultságát – a magyar informatikusok számára még mindig valami különös, távoli, egzotikus technológia, amely lehet ugyan szép, de valójában érdektelen. Akik így gondolkodnak, tévednek. A virtualizáció – ezen belül pedig az elkövetkező cikkek fő témája, a szerverparticionálás – az a technológia, amely alaposan revidiálja mindazt a tudást, de főleg gyakorlatot, amelyet a kiszolgálórendszerek tervezéséhez, létrehozásához, üzemeltetéséhez megszereztünk.

Jóllehet eddig is telepítettünk szervereket, PC-ket, de ezután ezt már másképp fogjuk tenni. Ha mentettünk már lemezeket, azt újra kell tanulnunk, ha pedig valaki még sohasem méretezett vagy monitorozott kiszolgálókat, de üzemelteti őket, akkor jobb, ha mielőbb megtanulja. Rövidesen elvárnak tőlünk katasztrófatűrést, amit a korábbi költségek töredékéért megvalósíthatunk; naprakész tudással, okos tervezéssel sokkal jobb rendelkezésre állást leszünk képesek kicsiholni a ránk bízott architektúrából, mint azt valaha gondoltuk volna – anélkül, hogy ezért külön fizetnünk kellene.

A virtualizáció minitörténete a Microsoft megjelenéséig

A virtualizáció olyan technológiai elv, amelyet sokféleképpen építhetünk a rendszereinkbe, és meglehetősen régóta alkalmazzuk őket, elég csak a RAID tömbökre gondolnunk. A kiszolgálók virtualizálása is legalább harminc évre tekint vissza, az elv és az első implementációk a mainframe-rendszerekben jelentek meg. A PC-k és a Wintel-világban azonban csak a kilencvenes évek végén tűnt fel az első olyan termék (Vmware Workstation), amely csírájában már hordozta a jelenünket. Az előadótermeket, konferenciákat (beleértve a Microsoftéit is) hirtelen elárasztotta a virtualizáció, s csupán hardver kérdése volt, hogy mekkora demókörnyezetet lehetett felvarázsolni egyetlen gépre.

Az évezred első évében jelent meg a kiszolgálókra szánt szoftververzió, és ekkor tűntek fel az alternatív virtualizációs megoldások, többek között a Connectixé, amely korábban Macintosh rendszerekre írt PC-emuláló szoftvert. 2003-ra már körvonalazódott, hogy a technológia alapvető változásokat indukálhat a kiszolgálók üzemeltetésében, így a Microsoft számára is fontos lett, hogy szereplővé váljon ezen a területen. Mint már korábban annyiszor, a Microsoft ezúttal sem a semmiből kezdte saját termékének fejlesztését, inkább felvásárolta a Connectixet.

A bekebelezés után pár hónappal, 2003 októberében megjelent a (már korábban a Connectix által elkezdett) Virtual PC 2004, 2004 júliusában pedig a vállalati kiszolgálókba szánt Microsoft Virtual Server 2005. Ez utóbbiból 2005 novemberében adták ki az R2 verziót – amelyet a következőkben alaposan szemügyre veszünk. Ez év áprilisától a termék ingyenessé, így bárki számára elérhetővé vált. Ha tehát valaki – akár e cikk olvasása után – kedvet kap, hogy megismerkedjen a jövő IT-rendszereinek egy alappillérével, azt bátran megteheti. S hogy ez az ismerkedés ne legyen parttalan, végigvezetjük az olvasót a technológia alapjaitól a szoftver kezelésén át a kiegészítő eszközökig, nem felejtve el a kapcsolódó megoldásokat sem.

A szerver-virtualizáció architektúrája

A Virtual Server esetén nem a működési elv a legizgalmasabb, sokkal inkább az elv segítségével megvalósított funkciók, mégis, csak az alap-architektúra megértésén át vezet út a funkciókhoz.

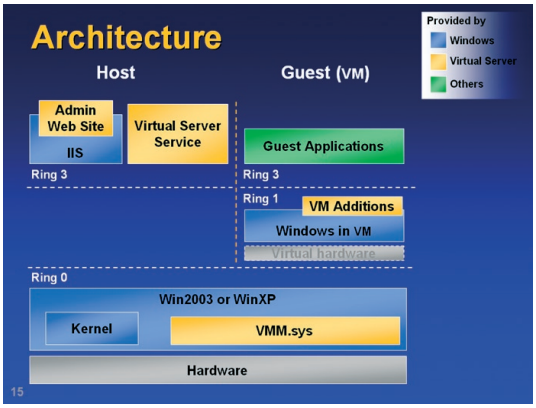
A gazda- és a vendégrendszer viszonya

Ahhoz, hogy egyetlen, fizikailag is létező szervert több partícióra osszunk a Microsoft Virtual Server segítségével, a hardver mellett szükségünk van egy „hagyományos” operációs rendszerre, amelyet ezúttal gazdarendszernek (host OS) nevezünk, mivel ez képezi – a Virtual Server 2005 mellett – a vendégrendszerek alapját.

Miután létrejött a gazdarendszer és a Virtual Server 2005 szimbiózisa, készen állunk, hogy virtuális gépeket hozzunk létre és indítsunk el. Ezek a virtuális gépek a Virtual

Server által létrehozott (emulált) hardverkörnyezetet és a rajtuk futó operációs rendszert jelentik.

A közös (és valódi) hardverre először az alaprendszert kell telepíteni, amelynek kernele a processzor által védett üzemmódban, ring 0-ban fut. A gazdarendszer éppúgy futtathat alkalmazásokat, mint a vendégrendszer, ezek a szoftverek a korlátozottabb lehetőségeket jelentő ring 3 üzemmódot használják. A Virtual Server telepítésekor a szoftver egyes komponensei kernel-üzemmódban (ring 0), mások user-üzemmódban (ring 3) működnek. Az ábra jobb oldala, vagyis a virtuális gépek architektúrája több mint érdekes. Milyen processzormódban fusson a vendég-operációsrendszer rendszermagja? Ring 0-ban nem futhat, mert akkor a VMM nem tudná ellátni az izolációs feladatait, és ő maga sem lenne védett a virtuális gépekkel szemben. Ring 3-ban futhatna, ekkor viszont jelentős a teljesítménycsökkenés, ráadásul el kellene különíteni a virtuális gép kernelét az alkalmazásaitól. A legkevesebb teljesítménycsökkenés úgy valósítható meg, ha a vendég-rendszermag (az amúgy alig használt) ring 1-ben fut, ahogy az ábrán is látjuk. A VMM feladata, hogy ezt a tényt elrejtse a vendégrendszer elől. Végül a vendégrendszer alkalmazásai az általuk amúgy is megszokott ring 3-as szintet foglalhatják el.



A rendszer technikai megvalósítása

Nagyon fontos hangsúlyozni, hogy a létrejött virtuális rendszerek „kívülről" teljesen úgy viselkednek, mint a valóságosak, sőt kijelenthető: pusztán a szolgáltatások igénybevételével nem állapítható meg, hogy egy adott kiszolgáló valóságos vagy épp virtuális.

A Virtual Server 2005 rendszerkomponensei

A virtualizáció szíve, pontosabban motorja a már említett kernelmódú VMM.SYS (Virtual Machine Monitor) eszközmeghajtó. Ez a komponens felelős a vendégrendszerek izolálásáért – egymástól és a gazdarendszertől –, kontrollálja, hogy az egyes virtuális gépek miként férhetnek hozzá a fizikai erőforrásokhoz, továbbá megvalósítja a virtuális gépek által látott hardver szoftveres emulációját.

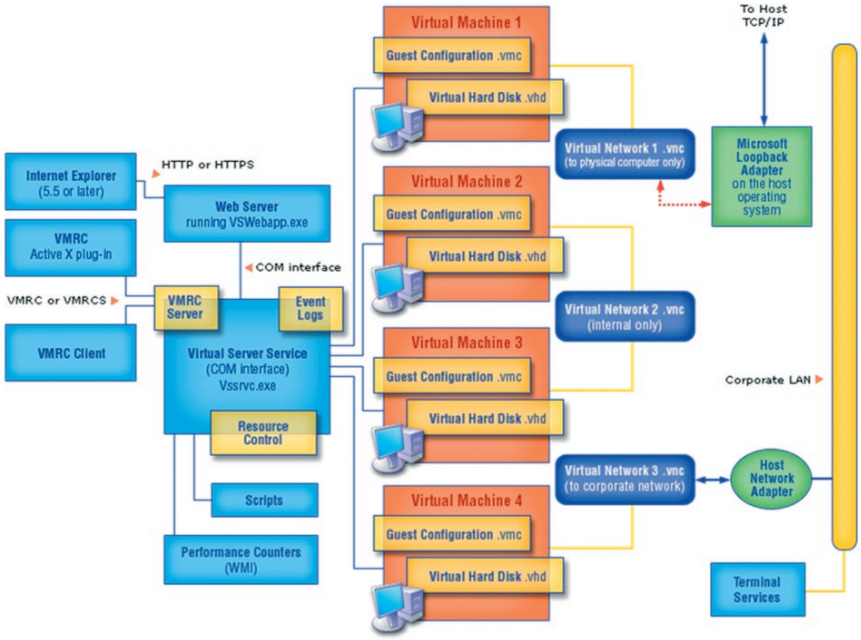
A VMM mellett a másik fontos komponens a Virtual Server Service. E szolgáltatás segítségével lehet létrehozni, elindítani, leállítani, tehát kezelni a virtuális gépeket, ez biztosítja számukra a 32 bites címteret is. A Virtual Server Service része a VMRC (Virtual Machine Remote Control) szerver. Ha analógiát szeretnénk keresni, akkor a VMRC – a kliens-komponenssel együtt – leginkább egy távmenedzsment-kártya szolgáltatásait biztosítja: elérhetjük vele a virtuális gép konzolját függetlenül attól, hogy esetleg az adott gép olyan alhálózatban üzemel, amelynek elérése ilyen módon nem lenne lehetséges. (Gondoljunk csak a DMZ-ben vagy egyéb speciálisan izolált módon működő gépekre.) A konzol elérése a VMRC-kliens alkalmazása mellett webes felületről ActiveX segítségével is lehetséges.

A Microsoft-szolgáltatásoknál megszokott módon beépítették a szabványos eseménykezelő (EventLog) és teljesítményszámláló (WMI Performance counter) modulokat is. A Virtual Server kezelőfelületét (Administration Website) webböngészőn keresztül egy Internet Information Server felhasználásával érhetjük el. Alapértelmezetten a kezelőfelület települ, de megvalósítható az IIS elhagyása, egészen pontosan központosítása is, növelve ezzel a biztonságot és csökkentve a gazda-operációsrendszer erőforrásigényét.

A Virtual Server Service mellett meg kell említenünk a Virtual Server Helper Service-t is, amely lehetővé teszi, hogy egy virtuális gép egy adott felhasználó kontextusában fusson. A felhasználói kontextus megadása csupán opcionális, ha nem akarjuk, akkor nem kell megadni. (Látni fogjuk, ez lesz a ritkább eset.) Ilyenkor a Virtual Server annak a felhasználónak a kontextusát használja, amelyik az adott virtuális gépet elindította.

Ha automatikusan indítani szeretnénk a virtuális gépet a Virtual Server indulásával együtt, vagy scripteket is szeretnénk használni, akkor mindenképp meg kell adni egy felhasználói nevet és jelszót. Éles környezetben mind a kettő szükséges funkció, s ez egyben a Helper Service létjogosultságát is mutatja.

Nem elhanyagolható szereplők a Virtual Server összetevői között a virtuális gépek reprezentációi sem. Egy virtuális gép kikapcsolt



A Virtual Server 2005 rendszerkomponensei

állapotban a .VMC kiterjesztésű fájlban tárolja a saját hardverére vonatkozó információkat, illetve egy .VHD állományban (vagy állományokban) a lemezeinek a tartalmát. A fenti állományokhoz tartozhat még egy memóriaállapot-mentést tartalmazó .VSV állomány, illetve bizonyos esetekben „Undo" lemezállomány is .VUD végződéssel.

A Virtual Server összetevőinek felsorolását a virtuális hálózattal zárjuk. Egyelőre minden részletet mellőzve annyit érdemes tudni, hogy háromféle hálózattípust használhatunk: közvetlenül egy valódi hálózatra csatlakozót, belső (kizárólag virtuálisan létező) hálózatot és a gazdagépet elérő hálózatot. A Virtual Server szolgáltatása egy úgynevezett Virtuális DHCP-kiszolgáló, amely a virtuális hálózatra csatlakozó gépeket látja el IP-címmel, megtakarítva egy önálló (virtuális) kiszolgáló felállítását.

Az emulált hardver

Ismerjük már a virtuális gép létrehozásának elvét, és láthatjuk a gép fizikai reprezentációit is, itt az ideje az emulált hardver megismerésének. Fontos megérteni: a virtuális gép mindig egy a Virtual Serverbe beégetett, nagyon szűk körű, emulált elemlistából épül fel, vagyis semmi, de semmi köze ahhoz a hardverhez, amelyen a (tényleges) gazdagép fut. A beégetettség azt jelenti, hogy azt a Microsoft határozta meg, és külső eszközökkel nem bővíthető, a szűk kör pedig azt, hogy egy bizonyos hardverkategóriából (például monitorvezérlőből) csak egyetlen eszköztípus létezik (S3 Trio64). Nézzük át futólag az elemlistát!

Adódik a kérdés, hogy miért éppen ezeket az eszközöket emulálták. Nos, mivel minden eszköz megvalósítása szoftverek útján történik, egészséges kompromisszumot kellett kötni a funkcionalitás és a sebesség között. Szofisztikáltabb hardverelemek esetén – bár javulhat a funkcionalitás – a szoftveres megvalósítás esetleg összességében több (teljesítmény)veszteséget okozhatott volna. Ezenfelül a Virtual Server tervezésekor fontos szempont volt, hogy jól ismert, bejáratott, minden operációs rendszer által támogatott lista jöjjön létre, mert így a virtuális hardver nem okozhat meglepetést. Az emulált eszközök többnyire azt tudják, amit a valóságos eszközök tudnának, de azért van pozitív és negatív eltérés is.

A floppy- és a CD/DVD-eszközöknél használhatunk ISO image-eket, ez a valós eszközöknél nem jellemző. A hálózati kártya névlegesen 100 Mbit/s áteresztőképességű ugyan, valójában azonban akkora sávszélességet használ, amekkorát csak tud, s ezt a tényleges fizikai média mellett a processzor sebessége határozza meg. Ha azonos gazdagépben két virtuális rendszer hálózati kártyával kommunikál, akkor a sebesség a memórialapok másolásának sebességével történik(!), vagyis itt a rendszerbusz kapacitása a meghatározó. A virtuális lemezek rugalmassága és (a hagyományos diszkekhez képest érzékelhető) funkciógazdagsága külön kiemelendő.

A fenti táblázatból azonnal látszik, hogy néhány eszköz bizony szűkös képességekkel rendelkezik a mai valóságos versenytársakhoz képest. Az S3 Trio64 nem lesz sohasem 3D-kártya, a memóriája sem elégséges, tehát olyan alkalmazások nem virtualizálhatók, amelyek ezt igénylik. Még fájóbb pont lehet, hogy nincs sem hang-, sem USB-támogatás. A hangkártya megtalálható a Virtual PC 2004 eszközlistájában, igaz, ott is egy ISA SoundBlaster eszközről van szó. Az USB-nél viszont már a teljes Microsoft-termékskála egységes: használhatjuk ugyan a gazdagép USB billentyűzetét és egerét, de pendrive-ot vagy USB alapú smartcard-olvasót nem installálhatunk. Szintén hiányzik a felsorolásból a faxkártya, vagyis a fax-alkalmazások sem virtuális gépekbe valók. Végezetül nincs lehetőségünk (hangsúlyozandó: a vendégrendszerben!) emulált host-bus adapterek használatára, így közvetlenül nem érhetőek el olyan eszközök, amelyeket Fibre Channel alapú SAN-ra kötöttünk, itt elsősorban a szalagos könyvtárakra kell gondolni. (Meg kell említeni, hogy a hálózati kártyák segítségével megvalósítható iSCSI hálózatokat támogatja a Virtual Server. Ez alternatívája lehet az FC SAN-megoldásoknak.)

Alaplap	Intel 440BX chipkészlet, PIIX4 komponensekkel (CMOS, rendszeróra, VRAM, memóriavezérlő, ISA és PCI busz stb.)
Floppy	1,44 MB lemez
Portok	COM, LPT
Egér, billentyűzet	Standard PS/2, de hozzárendelhető a fizikai gép PS/2-eszközéhez
Hálózati kártya	DEC 21140 10/100 TX Ethernet-adapter (néha Intel 21140-nek látszik)
Processzor	Ami a gazdagépben van, de legfeljebb 1 darab
Memória	A fizikai gép memóriája, de legfeljebb 3,6 gigabájt
Video	S3 Trio64 4 MB VRAM, Vesa 2.0, DirectX
IDE/ATAPI	Max. 4 darab IDE-eszköz (merevlemez, CD/DVD vagy ISO image), legfeljebb 127 MB/IDE csatornával
SCSI	Adaptec 7870. Legfeljebb négy adapter, egyenként legfeljebb 7 merevlemezzel, amelyek max. 2 terabájt nagyságúak lehetnek
Hang	Nincs emulált verzió
USB	Nincs emulált verzió

Mindazonáltal nem szabad szomorkodni az emulált eszközök szűkösségén: a Wintel-világban a virtualizáció koránt sincs még érett szakaszában, s az elkövetkező években számíthatunk arra, hogy mind a kapacitások, mind a funkcionalitás tekintetében gazdagabb eszközkészlethez jutunk majd. A táblázatot alaposan tanulmányozva, beruházásai, illetve technológiai változtatásai előtt mindenki a korlátok figyelembevételével hozhatja meg a maga „Go!" vagy „Don't go!" döntését. Több processzort igényel egy alkalmazásunk? Elégtelen a 3,6 gigabájt memória? Két terabájtnál nagyobb állományokat is kezelünk? USB-támogatást igénylünk? Speciális hardverkártyát használunk? Ezekben az esetekben (még) nem a Virtual Serverrel kell megoldanunk a feladatot. Ha viszont a felhasználóink száma, a várható processzor- és memóraigény belefér a Virtual Server adta keretekbe, továbbá nem hiányzik a virtuális hardverből semmi, akkor bátran virtualizáljunk.

Az emulált hardver minden eleméhez a Microsoft által aláírt eszközmeghajtó jár, így telepítés után egy „ismert állapotú" rendszer jön létre, s ennek a kifejezésnek később még nagy jelentősége lesz. A Microsoft törekvése, hogy minden termékét alkalmassá tegye arra, hogy a Virtual Server vendéggépen is működőképes, ezáltal támogatható legyen. (Jelenleg csak a Speech Server, a Sharepoint Server és az ISA Server nem támogatott virtuális környezetben.) A támogatás egyébként azt jelenti: a Microsoft nem várja el azt, hogy az ügyfél a hibát nem virtualizált környezetben reprodukálja, a valós és virtuális gépet azonosnak tekinti. Más virtualizációs termékek esetén ez az elvárás létezik, habár a Microsoft kiemelt ügyfelek esetén „üzletileg ésszerű erőfeszítést tesz" a felmerült problémák megoldására.

Lepenye Tamás

TechNet

Mélyvíz, csak úszóknak!

Megrendelőszelvény

☐ Igen, előfizetek a TechNet Magazin következő 6 számára: 7599 Ft (bruttó).

Technet0606

Az előfizető (vállalat) neve: .....

Az előfizető (vállalat) címe: .....

Ha más címre kéri a lap kézbesítését: .....Telefonszám:.....

Az előfizetés kezdete (hónap):.....

E-mail cím: .....

Aláírás (cégszerű):..... Számlát kérek: ☐ Csekket kérek: ☐

Kérjük, hogy a megrendelőszelvényt küldje a 06 (1) 888-3499-es faxszámra, vagy a Vogel Burda Communications Kft. címére (1426 Budapest, Pf. 300/139)! Az előfizetést a nap 24 órájában megrendelheti weboldalunkon a www.itmediabolt.hu, illetve e-mailben a terjesztes@vogelburda.hu címen. Várjuk megrendelését a 06 (1) 888-3421, 22 telefonszámokon is.

Hozzájárulok, hogy a Vogel Burda Communications Kft. adataimat marketingakcióihoz, promócióihoz felhasználja. Kiadónk az Ön személyes adatait az 1995. évi CXIX. adatvédelmi törvény szerint kezeli. Adatairól kiadónknál, a következő címen érdeklődhet: Vogel Burda Communications Kft. (1077 Budapest, Kéthly Anna tér 1.). Amennyiben nem járul hozzá, kérjük itt jelezze: ☐

ÚJ FUNKCIÓK, KEVESEBB HIBA

Nem kellett sokat várnunk az SQL Server 2005 első javítócsomagjára, nem egészen fél évvel a termék megjelenése után már meg is érkezett az SP1.

A Microsoft SQL Server 2005 Service Pack 1 csomag számos új funkciót, valamint teljesítményjavító módosítást és hibajavítást tartalmaz. Cikkünkben elsősorban az új funkciókra koncentrálunk, ugyanakkor természetesen szót ejtünk néhány hibajavításról, továbbá kitérünk a teljesítményjavító újdonságokra is.

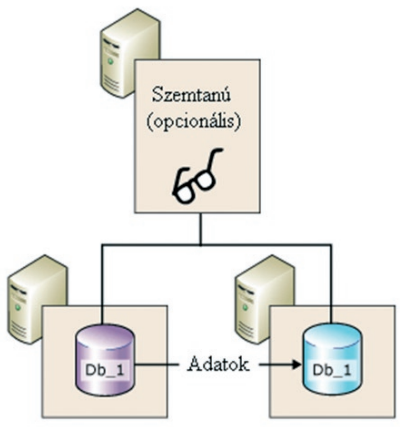
Új funkciók

Az SP1 új szolgáltatásai közül kiemelkedik az adatbázis-tükrözés támogatása és az SAP NetWeaver Business Intelligence adatkapcsolati interfész (.NET Data Provider), illetve a hozzá tartozó MDX lekérdezésszerkesztő.

Az SP1-gyel párhuzamosan az SQL Server Express változatához is fontos frissítések jelentek meg: a Reporting Services integrálása az SQL Expressbe, valamint a Management Studio Express. E funkciókon kívül még jó néhány újdonságról találhatunk információt a http://support.microsoft.com/kb/916940 címen.

Adatbázis-tükrözés – az SP1-ben már hivatalosan támogatott

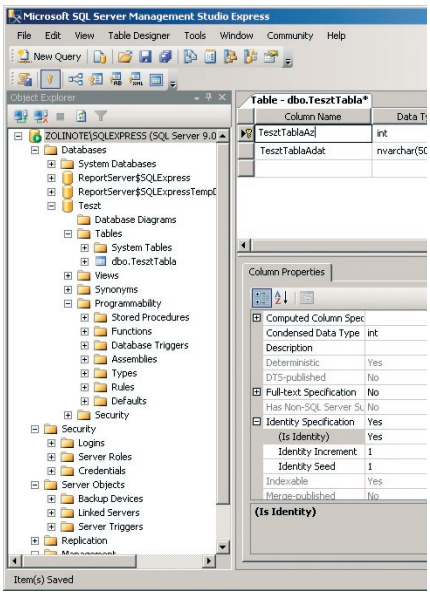
Az adatbázis-tükrözés (Database Mirroring) viszonylag olcsó és egyszerűen konfigurálható megoldás a magas rendelkezésre állás támogatására. Lényege, hogy egy adatbázist (az elsődleges adatbázist) egy másik szerverre tükrözünk, azaz előállítunk az adatbázisunkról egy másolatot (egy tükköradatbázist), és ezt folyamatosan szinkronban tartjuk az eredeti adatbázissal, majd figyeltetjük (egy erre a célra kijelölt szerverrel, a szemtanúval), hogy az elsődleges adatbázis rendelkezésre áll-e.



Adatbázis-tükrözés szemtanúval

Amennyiben nem érhető el az elsődleges adatbázis, a szemtanú automatikusan kezdeményezi a tükköradatbázis kinevezését elsődleges adatbázissá. A folyamat nagyon gyors, akár néhány másodpercen belül megtörténhet az átállás, ellentétben a fürtözési megoldások több percen át tartó átköltözési idejével.

Az adatbázis-tükrözést szemtanú nélkül is kiépíthetjük, ebben az esetben viszont le kell mondanunk az automatikus átállás lehetőségéről, azaz hiba esetén manuálisan kell végrehajtanunk az átállást.



Management Studio Express

Az adatbázis-tükrözéshez kliensoldali támogatás is tartozik, a .NET- és natív SQL-ügyfelek kapcsolati beállításai között megadhatjuk a tükörszerver (failover partner) nevét. Az elsődleges szerverrel való kapcsolat lezárását vagy elvesztését követően az újrakapcsolódás során az ügyfélalkalmazás az általunk megadott tükörszerverre kapcsolódik, amennyiben nem érhető el az elsődleges szerver. Ez sajnos nem teljesen automatikus, azaz az ügyfélalkalmazásnak detektálnia kell a kapcsolat megszakadását, majd újra kell kapcsolódnia. A fejlesztőknek oda kell figyelniük arra is, hogy a tükköradatbázis helye is megváltozhat,

ezért az adatbázisszerver nevéhez hasonlóan ezt sem érdemes „beégetni” az alkalmazásba.

Az adatbázis-tükrözést nemcsak a magas rendelkezésre állás támogatására, hanem a teljesítmény növelésére is használhatjuk, mivel a tükköradatbázisról csak olvasható pillanatfelvételt készíthetünk, így annak adatait elérhetővé tehetjük a lekérdező, jelentéskészítő alkalmazások számára.

Az SP1 talán legfontosabb újdonsága az adatbázis-tükrözés támogatott változatának megjelenése. A magas rendelkezésre állást támogató adatbázis-tükrözés az utolsó pillanatokban került ki a tavaly novemberben megjelent termék támogatott funkciói közül, a Microsoft indoklása szerint stabilitási problémák miatt. A fejlesztők és a technológiát tesztelni szándékozó felhasználók azonban bekapcsolhatták azt az 1400-as nyomkövetési opcióval, ám üzemszerű működésbe állítását a Microsoft mindeddig nem javasolta.

Az SP1 feltelepítése után az adatbázis-tükrözés megvalósításához már nem kell az 1400-as nyomkövetési opciót bekapcsolni (az opció hatástalan az SP1-ben), a tükrözést egyszerűen konfigurálhatjuk a Management Studióból. A tükrözés telepítése után egy új monitorfunkció is rendelkezésünkre áll, amelyet az adatbázisokra kattintva a „Tasks” → „Launch Database Mirroring” menüpontban érhetünk el.

SQL Server Express – egy ütős ingyenes adatkezelő

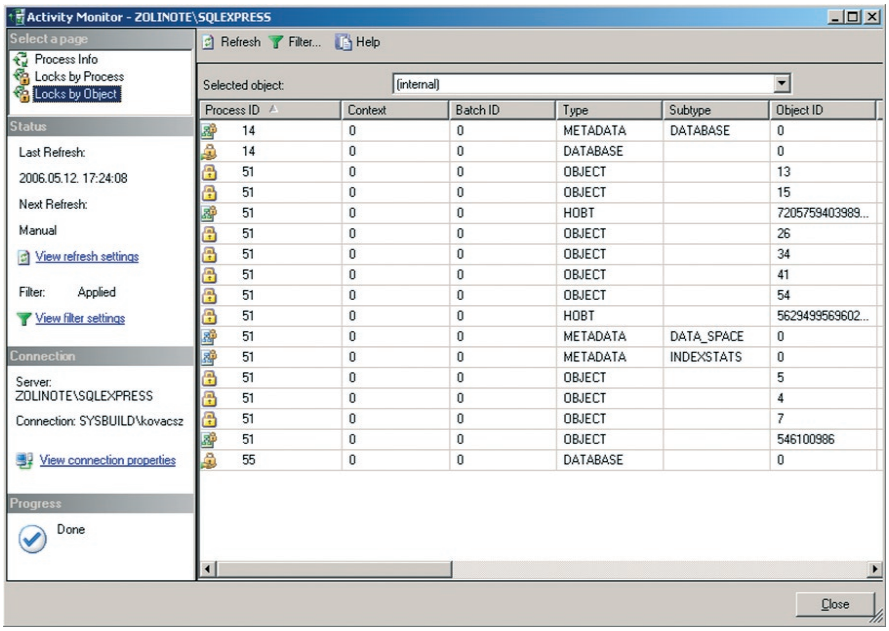
Az SP1-hez kapcsolódó másik nagy újdonság az SQL Server 2005 Express Edition with Advanced Services, illetve a Management Studio Express megjelenése.

Az SQL Express Advanced kiadása tartalmazza a Management Studio Expresst, a Reporting Servicest és a teljes szöveges keresést, így az Express változatban számos olyan funkcióhoz jutunk ingyen hozzá, amelyekért eddig bizony – ha nem is túl mélyen, de – a pénztárcánkba kellett nyúlnunk.

Figyelembe véve, hogy az Express-szel akár 4 gigabájtos adatbázisokat is építhetünk, korlátlan számú kapcsolatot létesíthetünk (az MSDE-be épített teljesítménycsökkentő korlátozás nélkül), és kihasználhatjuk a .NET CLR-támogatás nyújtotta előnyöket is – nyugodtan kijelenthetjük, hogy a Microsoft végre egy olyan ingyenes eszközt bocsátott a fejlesztők rendelkezésére, amely ideálisan használható önálló vagy kisebb hálózaton működő Windows-alkalmazások, valamint webes alkalmazások adatbázis-kiszolgálójaként.

Vessünk most néhány pillantást az SQL Express újdonságaira!

A Management Studio Express egy minden igényt kielégítő adminisztrációs felületet biztosít az SQL Express-példányok felügyeletére: a felület szinte teljesen megegyezik a nagyobb testvérekbe épített Management Studióéval, a nem támogatott funkciók kivételével ugyanazok a menüpontok, konfigurációs eszközök érhetők el. Adatbázisokat hozhatunk létre, kezelhetjük az objektumokat, lekérdezéseket szerkeszthetünk és elemezhetünk, figyelhetjük a szerveren futó folyamatokat, zárolási információkat, megrendeléseket hozhatunk létre publikált adatbázisokból, és még számtalan további feladatot elvégezhetünk.



Zárolási információk megjelenítése a Management Studio Expressben

Néhány szó a korlátokról: a Management Studio Express-szel csak SQL Server-példányokat kezelhetünk, Analysis Services, Reporting Services, Notification Services és SSIS konfigurálására nem használhatjuk; csak SQL-projekteket hozhatunk létre, és ezek kezelése is nehézkes kissé, mivel hiányzik a Solution Explorer; nincs Tuning Advisor és Profiler, így a komolyabb teljesítményhangolást inkább egy Developer Edition segítségével végezhetjük el.

A Business Intelligence Development Studiót az SQL Server 2005 Express Edition Toolkit letöltése után telepíthetjük fel. A Toolkit egyébként majdnem mindent tartalmaz ahhoz, hogy SQL Expressünket felügyeljük: benne van az adatbázis-elérési összetevőket tartalmazó „Connectivity Components” csomag, a Management Studio Express, a BI Development Studio és az SQL Express SDK (az utóbbitól ne várjunk túl sokat, néhány header-fájlon, libraryn és assemblyn kívül más nincs benne, a példákat és a dokumentációt külön kell letöltenünk).

A BI Develeopment Studióval SQL Server-, Analysis Services-, OLEDB-, OBDC-, XML-, Report Model- és SAP NetWeaver BI-adatforrásokból készíthetünk jelentéseket. A jelentésszerkesztő megegyezik a nagyobb testvérek által használt szerkesztővel, tartalmazza például az Analysis Services- vagy NetWeaver BI-adatbázisok lekérdezéshez használható MDX lekérdezésszerkesztőt (bár az ezzel készített lekérdezések a Report Server Express változatán nem futnak), támogatja a dinamikusan paraméterezett és interaktív jelentések készítését.

Az SQL Express-szel együtt települő Report Server jól használható, azonban a Standard és Enterprise változatokhoz képest erősen lebutított verzió. Ennek ellenére kiválóan alkalmas online jelentéskészítő megoldások, webes és Windows-alkalmazások kiszolgálására: a jelentéseket könyvtárakba csoportosíthatjuk; Windows- vagy Active Directory-cso-

portok és -szerepkörök segítségével szabályozhatjuk a hozzáférést; az elkészült riportokat .PDF és Excel-formában exportálhatjuk; a felhasználóknak engedélyezhetjük saját jelentések feltöltését a szerverre; a csatolt jelentések segítségével pedig egy jelentésből több példányt is létrehozhatunk különböző paraméterek vagy adatforrások megadásával. Sajnos néhány olyan fontos funkció, mint például a jelentések megrendelése és a pillanatfelvételek készítése kimaradt a támogatott tulajdonságok közül, de ne legyünk telhetetlenek, ami megmaradt, az is bőven elég.

Mindenképpen fontos megemlíteni, hogy az SQL Server 2005 Express nem minden szempontból váltja még ki a korábbi MSDE-t, hiszen az SQL Server 2005 Express igazából egy ingyenes, de leginkább szerveroldalon használható megoldás. Ha lokális, az adatbázisszerverrel szinkronban lévő adattárolást és cache-elést szeretnénk megvalósítani a kliensoldalon (például a kliensalkalmazás offline működésének megvalósításához), akkor még nem az SQL Server 2005 Express az ideális megoldás számunkra, mivel az sokkal inkább egy teljes értékű SQL Server, amit kliensre telepíteni talán pazarlás lenne az erőforrások tekintetében. Erre megoldást a nyár végén első bétaállapotba kerülő SQL Server Everywhere fog nyújtani, ami kifejezetten a kliensek, illetve a kisebb alkalmazások adattárolási és feldolgozási igényeit elégíti ki. Ennek a szoftvernek a végleges változata 2006 végére várható.

SAP NetWeaver BI-támogatás – SAP BI-adatok közvetlen elérése

A Microsoft az SAP NetWeaver BI-támogatás bevezetésével nagyon fontos lépést tett az SAP és a Microsoft üzletiintelligencia-eszközeinek együttes alkalmazása, integrációja felé.

A NetWeaver BI adataihoz való hozzáférést egy .NET-es adatelérési komponens (Microsoft .NET Data Provider 1.0 for SAP NetWeaver Business Intelligence) és az ezen a provideren keresztül működő vizuális lekérdezésszerkesztő biztosítja. A provider az SAP BW 3.5-ös verziójához készült, de használható a BW 3.0B, BW 3.1 és BW 7.0 változatokkal is.

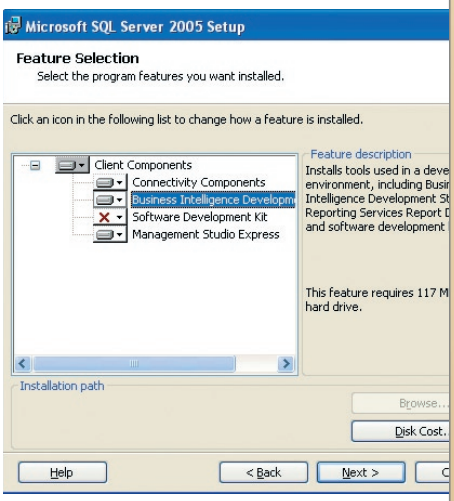
A két platform integrációját egyszerűsíti, hogy a SAP BW támogatja az XML for Analysis (XML/A) szabványt, és a rendszer felépítése nagyon hasonlít az Analysis Services felépítésére. Az XML/A direkt hozzáférést biztosít a BW QueryCube, InfoCube és MultiProvider objektumaihoz.

A lekérdezésszerkesztővel paraméterezett lekérdezéseket is készíthetünk a QueryCube objektumokon, és a paraméterek értéklistáit is feltölthetjük, a .NET-es adat-provideren keresztül pedig hozzáférhetünk a cellatulajdonságokhoz is.

A megfelelő teljesítményt a .NET-es provider és az SAP BW közötti kommunikációban alkalmazott GZIP tömörítés garantálja.

Néhány kényelmi és egyéb újdonság

- Az SP1-gyel egymás mellett működtethető a replikáció és az adatbázis-tükrözés, azaz a tükrözött adatbázisok replikációban is részt vehetnek.
- Az adatbázis-diagramok használhatók SQL Server 2000 kompatibilitási módú adatbázisokon is.
- A Database Mail működik 64 bites operációs rendszereken is.
- Statikus képeket, logókat adhatunk hozzá a Report Builderrel készített jelentésekhez.

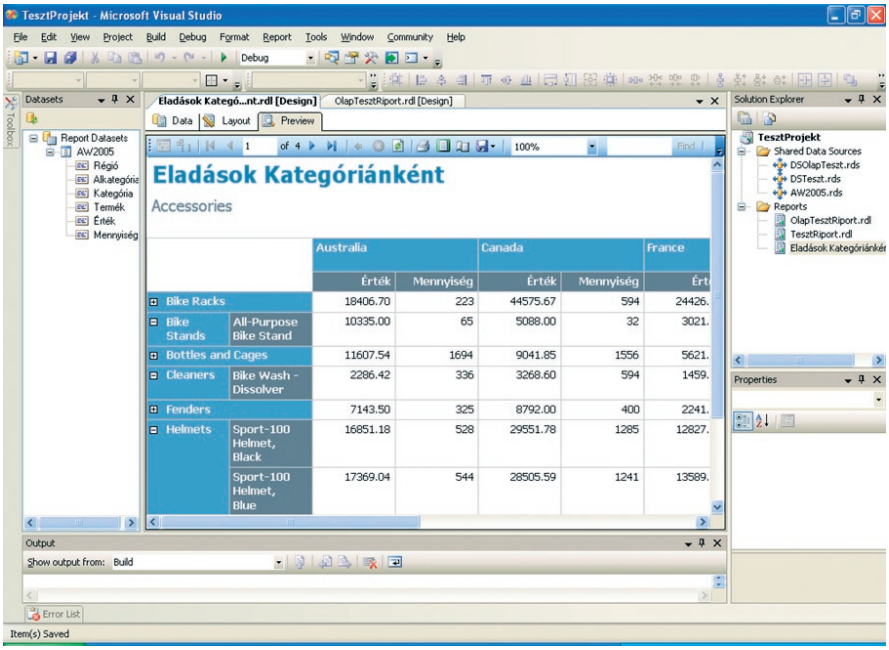


Az SQL Express Toolkit telepítése

- Gyorsabbak lettek a lebegőpontos műveletek, a komplex XQuery-lekérdezések, hatékonyabb lett az XML-adatok módosítása és gyorsabbak lettek a perspektívákra épített MDX-lekérdezések is.

Összefoglalásul elmondható, hogy a Service Pack 1-gyel az SQL Server 2005 sokkal gazdagabb, kényelmesebb, gyorsabb és megbízhatóbb lett. Aki eddig vonakodott feltelepíteni az új verziót, vagy elindítani az áttérési projektet, mondván, hogy jobb megvárni az SP1-et, az ne habozzon tovább: az SQL Server 2005 az SP1-gyel már minden tekintetben jobb, mint az elődök.

Kovács Zoltán



Jelentéskészítés a BI Development Studióval

- Többszálú SQLCLR-programokat is debug-olhatunk.
- Az SSIS-ben nem kell átkapcsolni „contol flow” nézetre, ha le akarunk futtatni egy adatfolyam feladatot (Dataflow Task): ezt közvetlenül megtehetjük az adatfolyamon egy jobbegér-kattintással és az „Execute Task” menüpont kiválasztásával.

IT-BUSINESS PRODUCTS

INFOKOMMUNIKÁCIÓS TERMÉKEK ÜZLETI DÖNTÉSHOZÓKNAK

- informatikai döntéshozóknak és technológiai szakembereknek
- az elmúlt 168 óra legfontosabb hazai és külföldi, ICT-piaccal kapcsolatos termékbejelentések, hardvereszközök és termékújdonságok
- heti ingyenes elektronikus hírlevél

Regisztráljon!

www.it-business.hu/hirlevel

MEGÚJULTAK A TANFOLYAMOK ÉS A MINŐSÍTÉSEK

A Microsoft – elsősorban az új termékek (SQL Server 2005, Visual Studio 2005, BizTalk Server 2006) és az ezekhez kapcsolódó új technológiák megjelenése miatt – új alapokra helyezte és kibővítette a korábbi minősítési és vizsgarendszerét.

Mind a 2005-ös, mind pedig a 2006-os év meglehetősen termékenynek bizonyult a Microsoft-szoftverek szemszögéből. Tavaly jelent meg a forradalmi változásokat hozó SQL Server 2005, a Visual Studio 2005, és mindezt támogatja a szerverplatform irányából az idén megjelent Windows Server 2003 R2 és a BizTalk Server 2006. Az idei évre várható továbbá a Windows Vista, szerveroldalon pedig a „Longhorn" Server és az Exchange Server 2007 megjelenése.

Az új termékek azon felül, hogy a korábbi verziókhoz képest új funkciókkal bővültek, alapvető, a szoftverek legmélyét is érintő változásokon estek át. Ennek következtében egy-egy terület teljes körű, mindenre kiterjedő ismerete már a többéves tapasztalattal és gyakorlattal rendelkező Microsoft-rendszermérnököknek, -fejlesztőmérnököknek, vagy akár az oktatással foglalkozó kollégáknak is gondot okozhat. A Microsoft ezért korábbi minősítési, vizsga- és tanfolyami rendszerét átalakította és kibővítette.

Mi volt, mi lesz? Tanfolyami modell és struktúra

A korábbi Microsoft-képzések alapvetően három csoportot alkotnak. Az oktató által vezetett hagyományos képzések egyenlő arányban tartalmaztak előadásokat, feladatokat és gyakorlatokat. A workshopok gyakorlatorientált képzések, kevesebb előadással és sok laborral, amelyek a témában korábbi előismeretekkel rendelkezőknek hasznos. A specifikus, kisebb témák megismerésére fél-, illetve egynapos előadásokat (Clinic) kínált a Microsoft.

Az eddigi képzések felépítése alapjában változatlan marad, az új termékekhez kapcsolódóan azonban már megkezdődött az anyagok, tematikák reformálása.

Mit is jelent ez?

Az új tanfolyami modell célja, hogy az egyes képzések még pozicionáltabbak legyenek, vagyis az egyes célcsoportoknak megfelelő igényeket, ismeretanyagot, szakmai területet még jobban lefedjék, másrészt az eddiginél még magasabb szintű és specifikált ismeretet adjanak, és ennek segítségével a már haladó, de egyes területen hiányos ismerettel rendelkező szakemberek is teljes körű tudást kaphatnak.

A képzések felépítése szorosan kapcsolódik (vagy legalábbis igyekszik kapcsolódni) az új minősítési rendszerhez és vizsgákhoz is.

Szintek és pozicionálásuk

A modell három fő szintre épül, ezek: a technológiai szint, a professzionális szint, valamint a tervezői szint.

A technológiai szintű képzés az alapja a modellnek. A technológiai tanfolyamok olyan szakemberek számára javasolhatók, akik egy adott témához kapcsolódóan alapos és átfogó technológiai ismeretekkel szeretnének rendelkezni, és feladatuk lesz az ezeknek az ismereteknek a felhasználásával adott problémák megoldása, feladatok végrehajtása. A technológiai szint egyben az alapja a professzionális képzéseknek is, de a professzionális tanfolyamokhoz sok esetben többéves, a technológiai tudásra épülő gyakorlati időre és tapasztalatra is szükség van.

A professzionális szinten elsősorban már tapasztalt, az adott témában járatos szakemberek részére szánt, magas szintű, különböző, specifikált témákkal foglalkozó kurzusok kapnak helyet. Az ebbe a csoportba szánt tanfolyamok a technológiai szintű tudásra és

a többéves gyakorlati időre, tapasztalatra építenek. A professzionális szint két részből tevődik össze, az IT-szakemberek (MCITP) és a fejlesztő szakemberek (MCPD) képzéséből.

A professzionális tanfolyamok elsősorban gyakorlat- és problémaorientáltak, vagyis nem foglalkoznak az általánosnak nevezhető területekkel, kérdésekkel, hanem speciális témákra vannak kihegyezve, és azt több szempontból is elemzik. Előtérbe kerül a vita, a közös, csoportos konzultáció, a különböző problémák felvetése és elemzése, megoldások optimalizálása adott problémához. Egyes képzéseknél IT- és fejlesztői projektvezetési/irányítási témák is fontos részei az anyagnak.

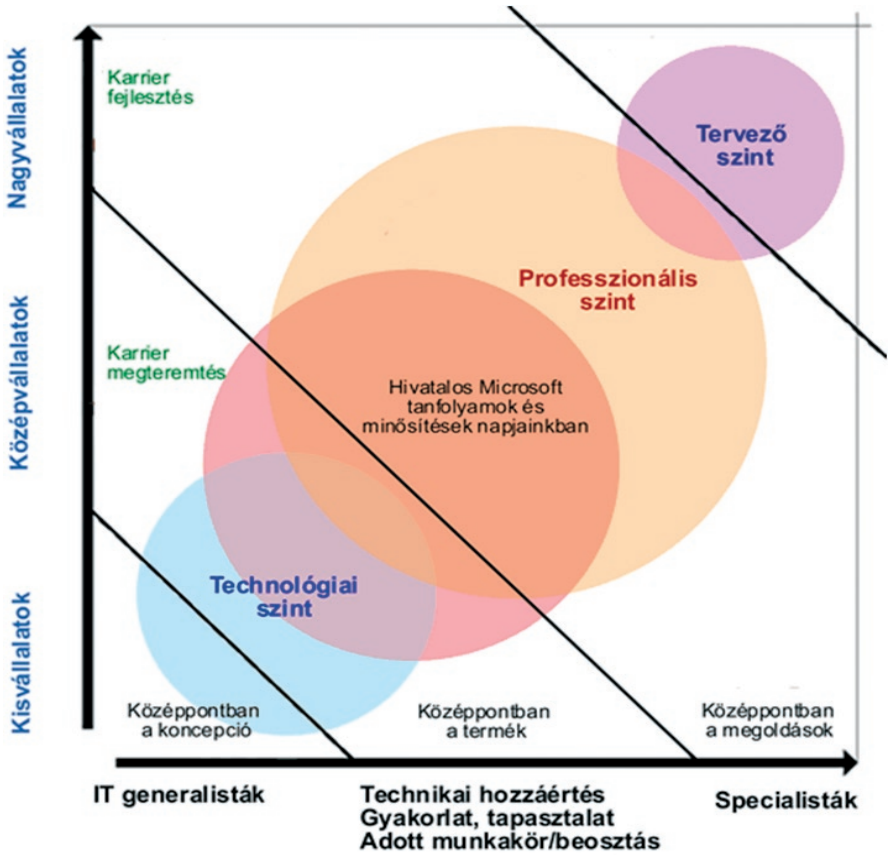
A tervezői (Architect) a Microsoft legmagasabb szintje a modellben. Jelenleg még kidolgozás alatt áll, mivel összességében kevés olyan szakember van, akik számára ilyen irányú ismereteket lehetne közvetíteni. Ezek a képzések olyan szakemberek érdeklődésére tarthatnak számot, akik legalább 10 éves IT- és legalább 3 éves projektvezetési tapasztalattal és referenciákkal rendelkeznek az IT vagy a fejlesztés terén.

Szintek és célcsoportok

A pozicionálás mellett a tanfolyami anyagok és tematikák összeállítása is változik, így például a kezdőbb szintű tanfolyamoknál az e-learning alapú képzések, illetve anyagok kerülnek előtérbe, míg a haladó képzéseknél nagyobb hangsúlyt helyeznek a gyakorlat- és problémaorientált oktatásra, konzultációra, adott valós életbeli problémák megoldására, esettanulmányokra.

A Microsoft Press hivatalos vizsgafelkészítő anyagai és kiadványai is ebbe az új modellbe integrálódnak.

A Microsoft első körben a Visual Studio 2005, az SQL Server 2005, továbbá a BizTalk Server 2006 témaköreiben hozta létre tanfolyamait az új koncepciónak megfelelően. Hasonló képzések várhatók majd a Windows Vista és az újabb szerveroldali termékekhez kapcsolódóan is.



További információk

www.szamalk.hu/tisza
www.microsoft.com/learning

Az oktatási program folyamatos fejlesztés alatt áll – csakúgy, mint azok a – még készülő – szoftverek, amelyek majd a legújabb tanfolyamokon kerülnek sorra. Ez egyben azt is eredményezi, hogy még vannak kisebb lyukak az egyes képzések egymásra épülését és a szükséges előismeretek megszerzését illetően. Az oktatóközpontok hivatalos képzésekből összeállított egyedi, saját készítésű tanfolyamokkal igyekeznek kitölteni ezt a hézagot.

Minősítések és vizsgák

Az új modellnek megfelelően a Microsoft új minősítési és vizsgarendszert dolgozott ki, vagyis az egyes tanfolyamokhoz társított hivatalos vizsgák is változnak. Az új minősítési rendszerben – a képzésekhez hasonlóan – technológiai, professzionális és tervezői szintű minősítéseket lehet szerezni IT- (jelenleg SQL Server 2005 és BizTalk), illetve fejlesztői (Visual Studio 2005) témákban.

A korábbi technikai minősítések, mint például a rendszeradminisztrátori (MCSA), rendszermérnöki (MCSE), fejlesztőmérnöki (MCSD) stb. továbbra is különállóan megmaradnak és élnek a modell professzionális szintjéhez kapcsolva.

A Microsoft a korábbi Microsoft SQL Server 2000 adatbázis-adminisztrátori (MCDBA) és Microsoft-fejlesztőmérnöki (MCSD) minősítéssel rendelkező szakemberek részére frissítő vizsgákat is kínál, ezek letételét és a technológiai szint elérését követően megszerezhetők az új kapcsolódó címek.

Az azonban biztos, hogy a most megszerezhető képesítésekről sokkal könnyebben lehet majd áttérni az új rendszerre, mint ha nulláról próbálna meg valaki előrejutni az új tanfolyamok és vizsgák ranglétráján.

Emellett persze az is tisztán látható, hogy az új képesítések sokkal pontosabb képet adnak arról az szakemberről, aki birtokolja azokat; ez mind a munkáltatóknak, mind az informatikusoknak előnyös: ugyanis az adott képesítés értéke és elismertsége jelentősen emelkedni fog. A korábbi rendszerről az újra történő áttéréshez pedig egyszerűbb, rövidebb tanfolyamok állnak rendelkezésre, és egyben kevesebb vizsga is szükséges hozzá – de már ezek is garantálják, hogy az azokon sikerrel vizsgázó informatikus az adott területet tökéletesen ismeri, és a gyakorlatban is képes megállni a helyét.

Simon Ferenc

A TechNet program

A Microsoft Magyarország már hosszú évek óta kiemelten foglalkozik az informatikai szakemberekkel – folyamatosan igyekszik eseményeket, szakmai tartalmat, támogatást biztosítani minden érdeklődőnek, nem csupán a vállalatoknál dolgozó szakembereknek.

Az biztosan sokak számára nyilvánvaló, hogy az általános asztali szoftverek célközönsége az átlagfelhasználó, abba viszont már sokan nem gondolnak bele, hogy az informatikai szakemberek valójában a szervertermékek végfelhasználói. A szerverszoftverek pedig az esetek többségében azért születnek, hogy az informatikusok kezébe több lehetőséget adjanak. Ahhoz, hogy hatékonyabban tudják kiszolgálni a rendszer tényleges végfelhasználóit. A teljes TechNet program lényege, hogy hogyan tudunk egyre több, friss tudást átadni a szakembereknek, akik így saját munkájukat jobban, eredményesebben tudják végezni.

Ebben a rovatban egyfelől azt igyekszünk körüljárni, hogy az aktuális szám megjelenését megelőző két hónapban milyen újdonságok történtek a TechNet háza táján, másrészt pedig szeretnénk, ha kialakulna mielőbb egy kétirányú kommunikáció, és a szakemberek visszajelzésekkel, véleményekkel támogatnák munkánkat.

Miből építkezünk?

A TechNet szemináriumok már hosszú évek óta nagy népszerűségnek örvendenek, itt igyekszünk a lehető legmélyebben bemutatni az új technológiákat. Nagy örömünkre szolgált, hogy első TechNetünkön két MVP (Most Valuable Professional), *Fóti Marcell* és *Gál Tamás* adott elő az R2 generációról, és a visszajelzések alapján ez a résztvevőknek is kifejezetten tetszett. Hasonló megmozdulásra még lesz példa a második félévben is. Emellett lezajlott még két TechNetünk, egy a menedzsmentszoftverekről, a másik pedig a Windows Vistáról szólt, és rendeztünk egy üzemeltetői konferenciát is, ahol a mindennapi informatikai kihívásokra kerestünk megoldást. Magazinunk megjelenésével egy időben zajlik majd le az Office 2007-et bemutató előadás, majd azt követi a félév utolsó eseménye, *Rafal Lukawiecki* vendégszereplésével. Az aktuális események listája elérhető a www.microsoft.hu/events oldalon.

Idén májusban indítottuk el a TechNet Portált (www.microsoft.hu/technet), ami gyakorlatilag egy kombinált hírportál–blogportál, ahol mindennap a Microsoft munkatársai és MVP-k írnak a legfrissebb újdonságokról, tapasztalataikról. Itt lesznek elérhetők a következő hónapokban azok a témaközpontok is, amelyek könnyebbé teszik az adott terület minél teljesebb megismerését.

Ugyancsak nemrég indultak a magyar nyelvű online előadásaink, vagyis a webcastok, amelyeket szintén kiemelkedő szakemberek tartanak minden alkalommal. Ezek mind élőben, mind felvételről megtekinthetők, s a legkülönbözőbb témákról szólnak – legyen az az ISA Server 2004, a BizTalk Server 2006, az SQL Server 2005 vagy maga az alapinfrastruktúra és az akörüli teendők. A webcastok a www.microsoft.hu/webcast oldalon tanulmányozhatók, szinte biztos, hogy mindenki talál magának valót.

Mindemellett a szakemberek rendelkezésére áll a TechNetKlub.hu, ahol szakterületekre bontott levelezőlistákon lehet egymás segítségét kérni. Itt a Microsoft munkatársai és más szakemberek dolgoznak azon, hogy minden kérdésre legkésőbb 24 órán belül megérkezzen a válasz. A TechNetKlub.hu éppen jelentős átdolgozás előtt áll – természetesen be fogunk számolni a fejleményekről.

A Magazin

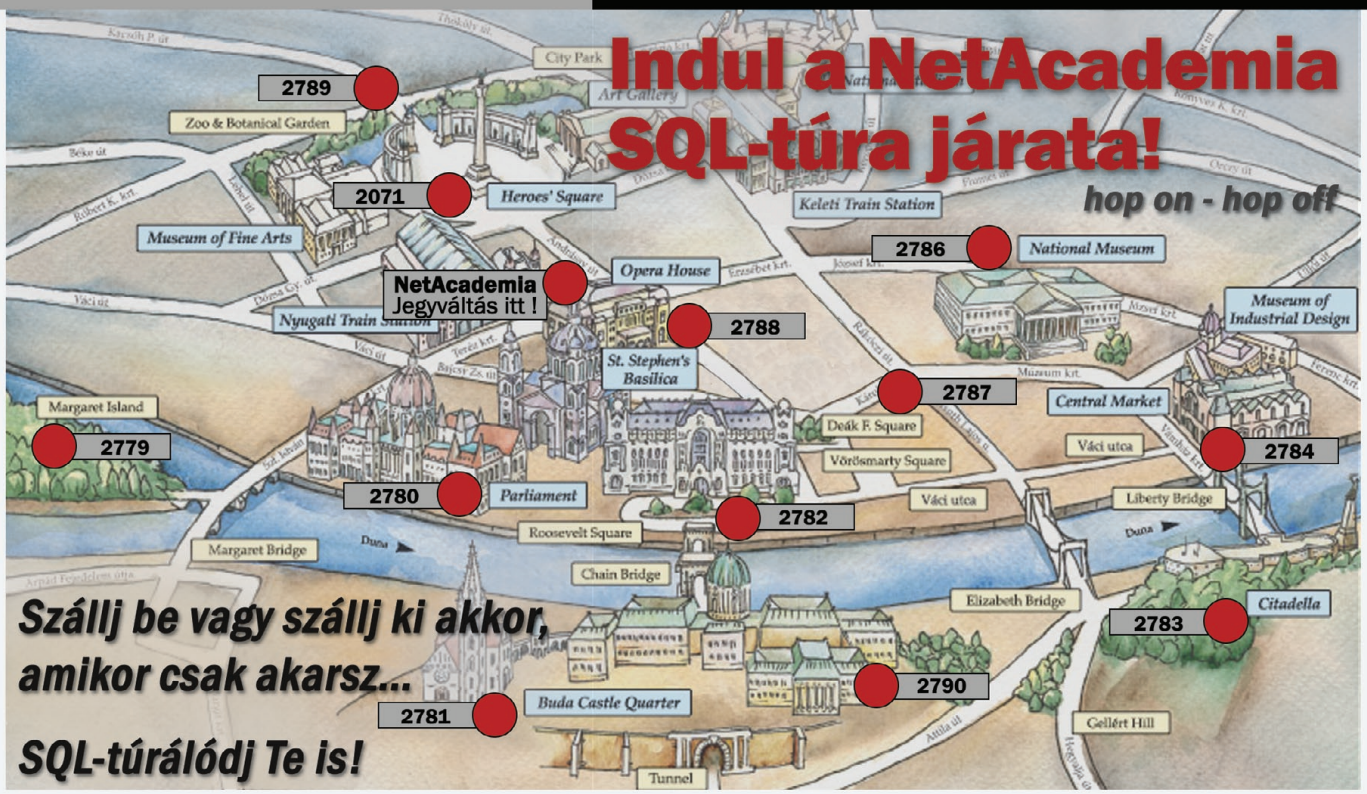
A TechNet Magazin korántsem ma jött a világra. A Magazint eredeti formájában Fóti Marcell és a NetAcademia stábja szerkesztette és jelentette meg, majd azt felkarolta a Microsoft. Most – a formai megújulás mellett – az a célunk, hogy egy olyan szakmai lapot adjunk minden olvasónknak, amiből valóban naprakész és használható információkhoz lehet jutni.

A közösség

Minden bizonnyal az elmúlt időszak legnagyobb eredménye, hogy végre elindult az igazi pörgés, egyre több a lelkesedés. Számtalan MVP, oktató, külsős szakember segít nekünk abban, hogy minél több témában tudjunk egyre több szakembert (tovább)képezni, segíteni őket mindennapi munkájuk során. Ami most elindult, az még csak a kezdet. A kezdeti lelkesedés ugyanakkor láthatóan egyre többekre ragad át, és pillanatok alatt el tudunk készülni olyan nagyszabású projektekkel is, mint például a most megújult Magazin vagy éppen a Portál és a webcastok – márpedig egyik sem jár kevés munkával.

A TechNet programok azonban eddig szinte csak a vállalatoknál dolgozó szakembereknek szóltak. A Portál, a webcastok és a Magazin megjelenésével mindez megváltozott. Bízunk abban, hogy mindenki nyugodt szívvel fogja ajánlani a TechNetet, ha informatikában elhelyezkedni vágyó emberrel találkozik, vagy olyasvalakivel, aki lépést akar tartani a rohamosan fejlődő technológiákkal. És még csak most jön a Windows Vista, az Office 2007 és a „Longhorn” Server... Lesz mit tanulni!

Budai Péter



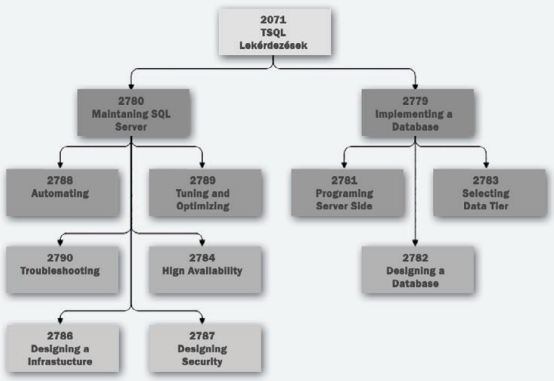
Tíz tanfolyam elvégzése eddig anyagi és időbeli lehetetlenség volt! A városnéző túrabuszokhoz hasonlóan egy-egy SQL nevezetségnél bármikor fel- és le lehet szállni a járatról.

Az SQL-túra mind időben, mind anyagilag előre kalkulálható, mivel egy egyszerű szabályt követünk: **A SQL-túrán az oktatás egységesen 20 eFt/nap*.**

A résztvevőknek tetszőleges SQL-túraútvonal választható, a részvételi feltétel csupán annyi, hogy a túra egynél több tanfolyamból álljon.

Az SQL-túra indulási időpontja:	2006. szeptember 10. hétfő
Az SQL-túra tanfolyamok időpontjai:	www.netacademia.net/SQLtura.aspx
Kedvezményes jelentkezési határidő:	2006. augusztus 31.
Oktatók:	Fóti Marcell MVP-SEC, MCSE-SEC, MCDBA, MCT, MZ/X Tóth László MCSD, MCDBA, MCT
Részvételi díj:	20 eFt/oktatási nap

(a fent nevezett tanfolyamár az MOC tananyagot és az étkezést nem tartalmazza)*



Jelentkezzen most, mert szeptemberben telt ház lesz nálunk!

netACADEMIA
A LEGJOBBAKAT TANÍTJUK.

Microsoft®
Neked lehetőség. Nekünk kihívás.™