

TechNet

2007. FEBRUÁR – MÁRCIUS

MAGAZIN MÉLYVÍZ, CSAK ÚSZÓKNAK!

Microsoft®

System Center

HÁZIREND ÉS JÓHISZEMŰSÉG

Az e-mail mint
kommunikációs
csatorna kritikus
fontosságúvá vált

AJAX – A WÉBFEJLESZTÉS ÚJ TÁVLATAI

Egyre több feladattal látjuk
el a webes alkalmazásokat

FOLYAMATOSAN ÁRAMLÓ VÍZBEN

Interjú Szalontay Zoltánnal

HOGYAN ALAKÍTSUNK KI DINAMIKUS INFORMATIKAI RENDSZEREKET:

**DSI – MŰKÖDÉSRE
TERVEZVE** ✓

**RENDSZEREK
ÉS GAZDAIK** ✓

MASS DEPLOYMENT ✓

**SCE – FÉGYVERT
A HŐSÖKNEK!** ✓

Microsoft TechNet

Ismerje meg a HOLONAP termékeit hamarosan induló tanfolyamainkon!

Exchange 2007
SharePoint 2007
SQL 2005 BI
Visual Studio 2005
Windows Vista/2003
Biztalk

A 2007-es évben több új Microsoft termék is megjelent a piacon, melyek megismeréséhez tanfolyamainkon és workshopjainkon most az elsők között szerezhet aktuális és hasznos, teljes körű rendszergazdai és fejlesztői információkat! Használja ki a kínálkozó alkalmat, és regisztráljon most biztosan induló képzéseinkre!

A teljes kínálatért és további részletekért, kérjük, keresse fel internetoldalunkat!

Néhány képzés ízelítőül:

- Exchange 2007 rendszergazdai újdonságok, áttérés (3938) *április 4-6.*
- Exchange 2007 Workshop (TechNet Lab) *március 27., 28., 29.*
- Windows Vista rendszergazdáknak (5115-5117) *április 23-27.*
- SharePoint 2007 újdonságok üzemeltetőknek *április 10-12.*
- Windows 2003 Security (2830/2823+PKI) *március 19-23., május 14-18.*
- SQL Server 2005 üzleti intelligencia (témák: BI, OLAP, ETL, Reporting Services, ProClarity, Business ScoreCard Manager) *március-április hónapban*
- Visual Studio 2005 fejlesztői képzéssorozat (Windows, web, nagyvállalati alkalmazásfejlesztés, architektúra- és szoftvertervezés) *márciustól májusig havonta egy-egy tanfolyam*
- BizTalk Server 2006 üzemeltetés és fejlesztés (2933/2934) *április 23-27.*

Rendeljen egyszerre több képzést!

10 tanfolyami nap esetén **10%**,
15 tanfolyami nap esetén **15%**,
15 tanfolyami nap felett **20%**

kedvezményt

biztosítunk a képzések listaárából!*

*Az akció valamennyi fenti témakörű tanfolyamra érvényes a szabad helyek erejéig. Az akció más akciókkal, kedvezményekkel nem vonható össze. További részleteket internetoldalunkon találhat. A képzésekre a jogszabályok szerint igénybe vehető a *szakképzési hozzájárulás*, és felhasználható az *SA oktatási utalvány*.

a mi tudásunk
az **ÖN** sikere



Telefon: 203-0304 / 4122-es mellék
www.szamalk.hu/tisza

A JÖVŐBE NÉZVE

Számtalan új lehetőség
az informatikusok kezébe.



Budai Péter

Microsoft Magyarország

Hamarosan egy teljes grafikus termékcsaláddal (Expression), otthoni szerverrel (Windows Home Server) is bővül a paletta. Mégis, talán a legérdekesebb, igazán korszakalkotó újdonságok a rendszergazdák világában bukkannak fel a következő fél-egy év során. Ma már számtalan eszköz könnyíti meg a rendszergazdák életét. Egyszerűsíthetnek és központosíthatnak címtárral, csoportházirenddel, skálázhatnak rendszereket kedvükre, automatizálhatnak feladatokat, igénybe vehetnek a rendszer állapotát figyelő szoftvereket is. Akár anélkül is felügyelhetnek rendszereket – egyszerre több cégnél is –, hogy fel kellene állniuk a saját karosszékükből.

A vállalatok számára egészen komoly folyamatok, ajánlások és bevált gyakorlatok érhetők el. Ugyanakkor egyre gyakrabban változnak meg az IT-vel szemben támasztott igények.

Általában öt-tíz évente érkezik el az idő, amikor a Microsoft áttekinti, milyen technológiák állnak rendelkezésre egy adott területen, platformon, mik a közös pontok a technológiákban, hogyan lehetne egyszerűsíteni, majd utána az új, rugalmasabb komponensekből teljesen újszerű képességeket fejleszteni. Természetesen megnézik, mik a legfontosabb igények a felhasználók részéről (itt jelen esetben az informatikusokról beszélünk), és mik azok a korábbi megoldások, amelyeket a legjobban szeretnek használni.

Adott tehát Redmondban néhány nagyon jó szoftvertervező (köztük *Anders Vinberg*, a DSI főtervezője), akik kaptak néhány évet arra, hogy friss szemmel, tervezőként tekintsék át a Microsoft IT-megoldásait. Egy feladatuk volt: találják ki a jövő dinamikus infrastruktúráját. Nekiestek. Volt alapanyag bőven, volt mit kombinálni. Absztraháltak, tervezgettek, ahogy egy nagy szoftverrendszer szokás, és kitaláltak valami igazán egyedit.

A végeredményül kapott koncepció nem egyszerű – nagyon összetett, és sok mindenre nyújt megoldást egyszerre. Ezért ebben a lapszámban igyekszünk ezt a területet az alapoktól kezdve áttekinteni, valamint megmutatni, hogy a System Center-szoftverek hogyan lesznek a segítségünkre néhány hónapon belül a gyakorlatban.

SZERKESZTŐSÉG
Főszerkesztő
 Sziebig Andrea – asziebig@vogelburda.hu
Szakmai lektor
 Budai Péter – ipbudai@microsoft.com
Vezető szerkesztő
 Varga János – jvarga@vogelburda.hu
Nyomdai előkészítés
 Budakeszi Bajárát Kft.
Korrektor
 Matula Zsolt
Lapterv és címlap
 Emotion Bt.

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

KIADÓ
 A Microsoft Magyarországi megbízásából kiadja
 a Vogel Burda Communications Kft.

A kiadásért felel
 Walitschek Csilla
cswalitschek@vogelburda.hu
 Tel.: 888-3450, fax: 888-3499

A TechNetben közölt cikkek fordítása, utánnomása, sokszorosítása és adatrendszerekben való tárolása kizárólag a kiadó engedélyével történhet. A megjelent cikkeket szabadalmi vagy más védettségre való tekintet nélkül használjuk fel.

Hirdetési igazgató:
 Farkas Viola – vfarkas@vogelburda.hu, tel.: 888-3459

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 – sszendrey@vogelburda.hu, tel.: 888-3455
 Fax: 888-3459

Hirdetési koordinátor:
 Szőke Erika – eszoke@vogelburda.hu
 Tel.: 888-3411, fax: 888-3459

Nemzetközi hirdetésfelvétel:
 Eric N. Wicha – ewicha@vogelburda.com

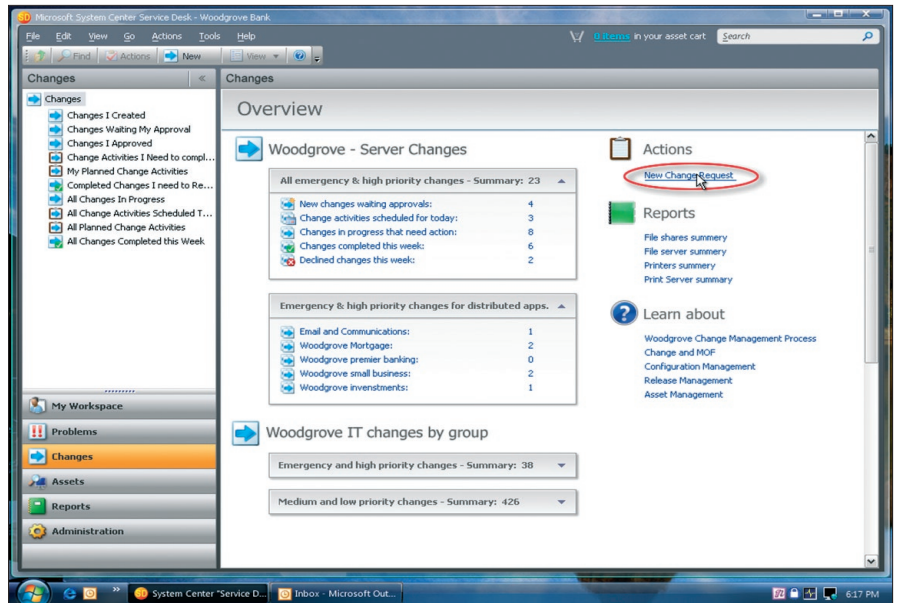
Vogel Burda Holding
 Poccistrasse 11, D-80336 München
 Tel.: +49 89 74642-326, fax: +49 89 74642-325
 A hirdetések körültekintő gondozását kötelességünknek érezzük, de tartalmukért felelősséget nem vállalunk.

Marketing:
 Gajdos Barna – bgajdos@vogelburda.hu, tel.: 888-3494

Terjesztés
 Terjesztett példányszám: 3000

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

Címlapon



DSI – működésre tervezve

(Budai Péter)

A Microsoft Dynamic Systems Initiative célja olyan dinamikus, rugalmas rendszerek létrehozása, amelyek kimondottan könnyen üzemeltethetők

6. oldal

Rendszerek és gazdáik

(Lepénye Tamás)

Az informatikai rendszerek elég gyakran élnek szimbiózisban üzemeltetőikkel. Együtt nőnek, együtt érnek, együtt öregszenek

11. oldal

Mass Deployment

(Gál Tamás)

Már a kifejezés fordítása is problémás egy kissé. Tömeges telepítés? Talán ez a legjobb. A hivatalos terminológia szerint a „Deploy” bevezetés, a „Deployment” pedig központi telepítést jelent...

15. oldal

System Center Essentials: fegyvert a hősöknek!

(Lepénye Tamás)

Az informatikát alkalmazó szervezeteket jól el lehet különíteni aszerint, hány végfelhasználói berendezést üzemeltetnek. A 25-500 végberendezést üzemeltető szervezetek a középvállalatok – informatikai Középfölde sok-sok IT-hőssel

20. oldal

MOF: a szolgáltatásorientált üzemeltetés alapjai

(Kurucz György)

Hogyan tekintünk folyamatorientált szemlélettel saját IT-üzemeltetésünkre, és hogyan váljunk jó informatikai szolgáltatóvá?

24. oldal

Kézben tartott naplók

(Kelemen László)

Biztonsági audit a System Center Operations Manager 2007-ben

28. oldal

Infrastruktúra

Házirend és jóhiszeműség

(Petrényi József)

Akár tetszik, akár nem, mind a cégek közötti, mind a cégen belüli kapcsolattartásban az e-mail mint kommunikációs csatorna kritikus fontosságúvá vált. Ez nem csak azt jelenti, hogy rendszerhiba esetén a rendszergazdáknak úgy kell rohangászniuk, mint zseblámpafényben pókoknak a falon

32. oldal

Biztonság

Windows Vista – a biztonság jegyében

(Szabó Gábor)

Az ezredfordulóra egyértelművé vált, hogy az informatikai biztonságot fenyegető vírusok és különböző rosszindulatú kódok létezése nem csupán városi legenda, hanem valós tény

38. oldal

Alkalmazásplatform

AJAX – a webfejlesztés új távlatai

(Nagy Levente)

Szeretjük és egyre több feladattal látjuk el a webes alkalmazásokat: kényelmes, hogy más tartja karban a háttérrendszereket, és bárholnan elérhetjük a szolgáltatásokat. Azért persze a weben sem minden tökéletes

41. oldal

A Microsoft üzletiintelligencia-eszközei

(Kovács Zoltán)

A Microsoft üzletiintelligencia-eszközei az alkalmazások széles körét támogatják, az egyszerű jelentéskészítéstől a vállalati teljesítményértékelésen keresztül a komplex pénzügyi elemző, tervező rendszerek kialakításáig

44. oldal

Közösség

Folyamatosan áramló vízben

(Budai Péter)

„Én meg mindig megpróbáltam a konvertálható tudás irányába mozogni”

– interjú Szalontay Zoltánnal

49. oldal

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



Fontos, hogy minden komponens önmagában hordozza mindazt a tudást, ami saját működésével kapcsolatos, és ennek segítségével önműködően viselkedjen, valamint tudja, hogy mely további komponensekkel áll még kapcsolatban. Ezek a komponensek lehetnek akár emberek, adatok, szolgáltatások, számítógépek, szoftverek, hardverek is. Csupán építőkövek mindannyian az IT-rendszer szemszögéből.

Bármilyen meglepő is, ezek az objektum-orientált, illetve az elosztott rendszerek programozásának és tervezésének alapjai, sőt, ha még tovább megyünk, ugyanez a lényege a manapság agyonhasznált szolgáltatásorientált megközelítésnek is, amit SOA néven emlegetnek.

Az pedig talán már nem is szorul komolyabb magyarázatra, hogy a komplexitás csökkentése, illetve magának a problémának az eliminálása önmagában is költségcsökkentő tényező a rendszer egészét tekintve. Ez pedig lehetővé teszi újabb informatikai megoldások könnyebb kialakítását és bevezetését, tovább növelve a vállalat hatékonyságát.

Lássuk, hogyan alkalmazhatjuk az előbb ismertetett koncepciókat az informatikai infrastruktúra egészére – lényegesen érthetőbb példák kíséretében.

Tudás és modell alapú megközelítés

Ahhoz, hogy egy rendszert átlássunk és megértünk, tudásra van szükségünk. Ismerni kell a rendszer összetevőit, komponenseit. Ismernünk kell azok kapcsolatait. Tudnunk kell a rendszer meglévő hibáiról, illetve arról, hogy a korábbi problémákat hogyan hártottuk el. Persze ez egy komplex rendszer esetében rengeteg, egymással szorosan összefüggő információ ismeretét feltételezné, ami egy ember – vagy akár egy teljes team – számára is elképzelhetetlen feladatot jelentene. Nem biztos például, hogy fel tudjuk mérni, mivel fog járni egy egyszerűnek tűnő változtatás egy nagyobb rendszer egészére nézve.

Nézzük meg ugyanezt egy másik irányból is! Egy alkalmazásnál vagy szolgáltatásnál cél, hogy azt annak mélyreható ismerete nélkül is lehessen telepíteni és használni, csak úgy, mint egy egyszerű berendezést, például egy tv-t vagy digitális kamerát. Ehhez azonban szükség van egy olyan leírásra, amelyik bemutatja a telepítendő szoftverrendszer vagy üzleti folyamatot, és azt, hogy annak

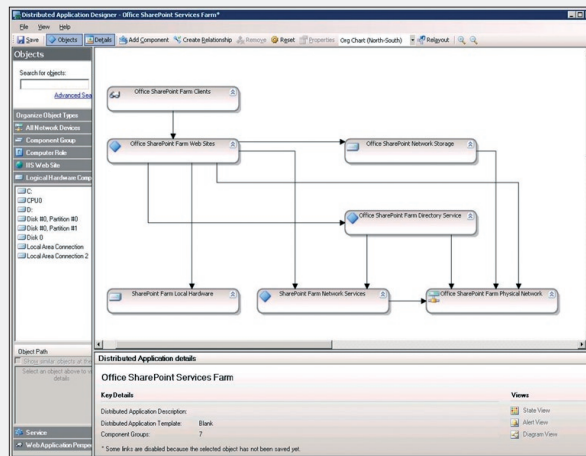
telepítéséhez és üzemeltetéséhez milyen technológiákra és lépésekre van szükség. A konfigurációs és architektúráis részletek igazán csak akkor lesznek érdekesek, amikor a rend-

inkább olyan, mint egy tervrajz az építés számára, azonban míg a tervrajz teljesen statikus, a rajta lévő elemek nem változnak – addig a rendszermodellnél cél, hogy dinamikusan jelenítse meg az éppen aktuális állapotot, és annak változásait folyamatosan nyomon lehessen követni. Mi is ez valójában?

A rendszerünk néhol egyszerűsített, de úgyszólván mindenben pontos megfelelő. Egy elosztott, mindig friss és dinamikus CMDB (Configuration Management Database).

Mire jó ez az egész?

A tudás és modell alapú gondolkodásmód alapvető paradigmaváltást jelent az informatikai rendszerek



A SharePoint komponenseinek összefüggései a System Center Operations Manager 2007-ben

szer nem megfelelően (lassan vagy hibásan) működik, illetve egyáltalán nem sikerül azt üzembe helyezni.

A modellek lényege, hogy egy adott rendszert több nézőpontból, az éppen szükséges adatok megjelenítésével tudnak ábrázolni, a számunkra tökéletesen felesleges részletek elrejtésével. A modell mindig a valóság egy meghatározott szelete, csak részinformáció, egy kis tudásmorzsa. Több modell viszont kapcsolatban is állhat egymással, és így együtt meghatározhatják a rendszer egészét. Egy modell általában nagyon egyszerűen átlátható, de a modellek összessége lehet tetszőlegesen komplex.

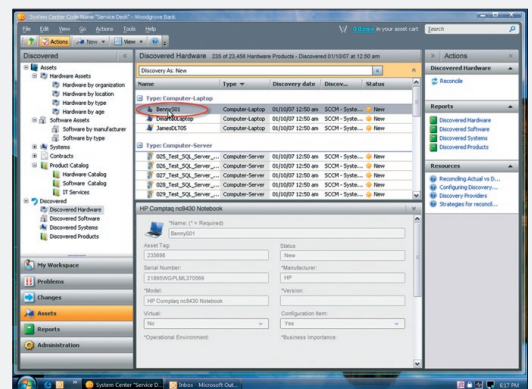
A DSI egyik kulcstechnológiája, az SDM (System Definition Model) pontosan ennek a megvalósítását teszi lehetővé. Az informatikai rendszer pontos és hihetetlenül precíz tervrajzát adja a kezünkbe, önálló és egymással összekapcsolódó modellek és komponensek formájában. A modellek pedig nem egy központi helyen vannak, hanem egymással laza kapcsolatban állva, elosztott módon található meg a rendszerben – gyakorlatilag minden komponens mindent tud saját magáról, minden más már csak a köztük fennálló kapcsolatokon múlik.

Az így kapott rendszermodell pedig leg-

esetében. Érdemes végiggondolni, hogy milyen hatása lehet a jelenleg elfogadott és megszokott informatikai folyamatokra nézve, illetve milyen új megoldásokat tesz elérhetővé.

Rendszermenedzsment

Mit szeretnénk elérni? Azt, hogy ezek a különálló komponensek képesek legyenek – amennyire csak elképzelhető – önállóak lenni. Képesek legyenek különösebb külső vagy manuális beavatkozás nélkül települni, letölteni magukat, konfigurálni magukat az



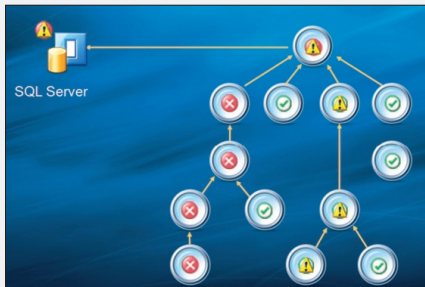
Hardverlelőár a System Center Service Deskben

aktuális igényeknek megfelelően, optimalizálni magukat a múltbeli tapasztalatok alapján, megvédeni önmagukat a támadások és a biztonsági fenyegetések ellen, menedzselni saját magukat, és ha mégis bekövetkezik va-

lami hiba, képesek legyenek elhárítani is azt, legyenek öngyógyítóak. Mindezek a képességek az SDM modellekbe kódolhatóak.

A rendszermenedzsmment lényege – különösen az automatizált rendszermenedzsmmenté –, hogy definiáljunk egy elvárt állapotot, folyamatosan figyeljük, hogy a rendszer valójában milyen állapotban van, majd közöljük egymáshoz a kettőt. Ha túl nagyok az elvárások, csökkentjük őket, vagy ha az elvárásoknak nem felel meg a rendszer, akkor változtassuk meg a rendszert úgy, hogy ez a probléma elháruljon.

A legegyszerűbb, amire itt gondolhatunk, egy adott rendszer vagy szolgáltatás rendelkezésre állása, amelyet akár SLA-k képében is definiálhatunk. Vizsgálhatjuk, hogy a szolgáltatás megfelelően fut-e, megfelel-e az SLA-nak, és ha valamiért nem, akkor egyrészt



Mi lehet a hiba oka? Általában a legmélyebben található hibás komponens a bűnös

naplózunk (hogy lássuk később, milyen volt valójában a rendelkezésre állás), másrészt vagy automatikusan megpróbálhatja a rendszer kijavítani magát, vagy szól egy megfelelő szakértelemmel rendelkező embernek, aki manuális munkával megoldja a problémát.

A modellekkel és a CMDB-ben nemcsak a komponensek állapotát tárolhatjuk el, hanem akár tudásbázisként is használhatjuk azt, hogy megnézhessük, milyen problémák fordultak elő korábban a rendszerben, és azokra mi volt a megoldás. Tárolhatjuk benne azokat a scripteket – vagy bevált módszerek dokumentációit –, melyeket napi szinten használunk a rendszer üzemeltetéséhez.

Ezeket a scripteket könnyen időzíthetjük, összeköthetjük eseményekkel, esetleg konkrét hibákkal, hogy automatikusan lefussanak, amint egy komponens állapota vagy egy adott tulajdonsága megváltozik. Így válik lehetővé öngyógyító rendszerek létrehozása. Ha nem automatizálunk, akkor is sokat segít

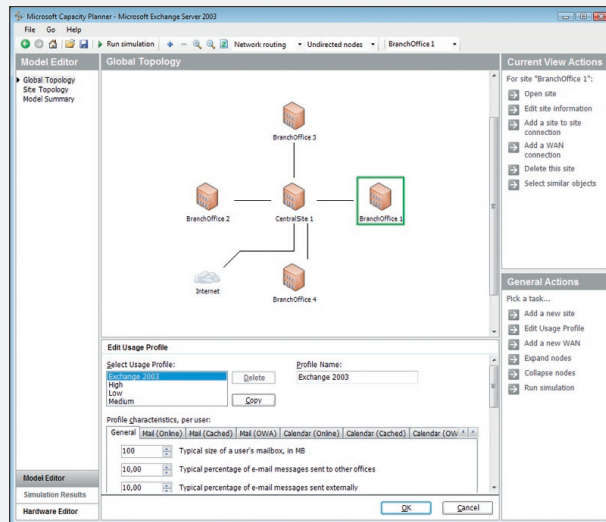
a tudásbázis, hiszen rögtön tudunk válogatni a korábban már sikerrel alkalmazott megoldások közül, és mi magunk dönthetjük el, melyikre van éppen szükségünk.

Az egyes komponensek monitorozásakor és állapotuk ellenőrzésekor is sokat segíthet a CMDB, hiszen az tartalmazza a komponensek közti kapcsolatokat. Amikor leáll egy szolgáltatás, rögtön sejtethető, hogy az valamely alkomponensének a hibájából állt le, vagy valamely konfigurációs beállítás nem megfelelő. A komponensek SDM modellekben rögzített kötöttségeinek hálója, automatikusan kideríthető, hogy mik lehetnek a legvalószínűbb okok, amelyek a szolgáltatás leállítását idézték elő. Mindezt akár vizuálisan is ábrázolhatjuk. Így ahelyett, hogy a tudásbázist kellene böngészni, vagy magunknak kellene rájönnünk a hiba okára, nagy eséllyel rögtön megtaláljuk, mi okozza a hibát. Ráadásul nemcsak mi jövünk rá, hanem a rendszer maga is, így akár a beavatkozásunk nélkül, automatikusan is el tudja azt hárítani.

Előzzük meg a bajt!

Mindenesetre a legjobb megoldás a rendelkezésre állás biztosítására a teljes megelőzés. Ezt úgy érhetjük el, hogy egyszerűen meg sem

vagyunk annak pontos következményeivel. Természetesen ez a megoldás a hardverhibák esetén nem sokat segít, de az emberi mulasztások vagy akár az automatizált scriptek által okozott hibák többségének véget vethet. Mi a megoldás lényege? Az, hogy a változtatás-



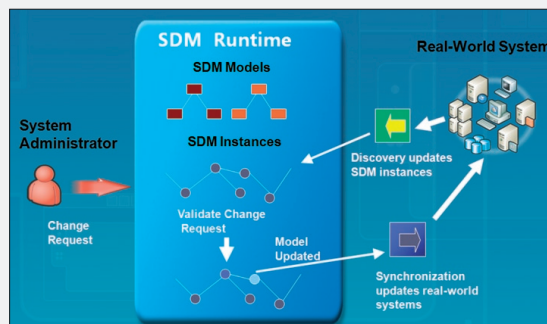
Kapacitás- és rendszertervezés a System Center Capacity Planner 2006-tal

kat egy tesztkörnyezetben, de nem is akármilyenben, hanem mindössze egy modellen végesszük el!

A modellek kötöttségeit és lehetőségeit értékelve hamar kiderül, hogy életképes lesz-e az általunk készített változat (ez a folyamat a validáció), és ha elégedettek vagyunk az eredménnyel, akkor a végleges, elkészített modell alapján juttatjuk érvényre a szükséges változtatásokat az éles rendszeren is (ezt nevezzük szinkronizációnak). Ilyen módon választ kaphatunk a „mi lenne, ha?” kez-

tű kérdéseinkre anélkül, hogy tesztkörnyezetet kellene építenünk, vagy veszélyeztetnünk az éles, működő rendszerünket; illetve azok a változások, amelyek a modellek szerint biztosan hibát okoznának, nem futhatnak le megerősítés nélkül.

Könnyen észrevehetjük, hogy ez a modellen végzett változtatás sok minden másra is jó lehet. Tervezhetünk például hipotetikus rendszert is – akár már meglévő építőkövek felhasználásával –, ugyanis egyáltalán nem kötelező a CMDB-eket használni kiindulásként. Ezen az elképzelt rendszeren végezhetünk teljesít-



Változtatás előtt validálunk, utána szinkronizálunk az éles rendszerre – ez lesz a „Longhorn” Server környékén

engedjük olyan változtatások véghezvitelét, amelyek veszélyeztethetik a rendszer működését, vagy ha mégis, akkor előre tisztában

lásával –, ugyanis egyáltalán nem kötelező a CMDB-eket használni kiindulásként. Ezen az elképzelt rendszeren végezhetünk teljesít-

ménytervezést is, így már a rendszer tervezése során fel tudjuk mérni, hogy milyen számítógépeket és szervereket kell vennünk, illetve az általunk megálmodott infrastruktúra működőképes lesz-e, képes lesz-e megfelelni például az SLA-knak, továbbá más, pontosan definiált igényeknek.

Folyamatok integrálása

A különféle folyamatok akkor működnek igazán megbízhatóan és hatékonyan együtt, ha képesek egymással megosztani az információt. Ennek ideális eszköze például egy adatbázis, mondjuk, maga a CMDB. A fejlesztési és üzemeltetési módszertanok (például MSF, MOF, ITIL) jól illeszkednek a DSI koncepciójába: a rendszer- és szoftverfejlesztés folyamata a rendszeradminisztrációval és az üzemeltetéssel a modellek révén könnyen összekapcsolhatóvá válik. A felhasználói visszajelzéseket is rögzítheti a rendszer, valamint naplózhatjuk a felmerülő hibákat, a teljesítménymutatók értékeit, a biztonsági eseményeket és így tovább.

Ezek az információk azonnal eljuthatnak (kezelhető formában) a felhasználótól az üzemeltetőkhöz, vagy akár a rendszerek fejlesztőihez is, amiből akár kimutatásokat is készíthetünk, és ezeket később változtatási kérelmekké finomíthatjuk. Összességében a CMDB segítségével a rendszerek változáskezelése, az üzemeltetés, a támogatás és az optimalizálás is egyszerűbbé, folyamat- és adatközpontúvá válhat.

Virtualizáció és átterhelés

Részben a DSI témakörébe tartozik a virtualizáció is, ami gyakorlatilag abban segít, hogy rendszerünk összetevőit minél inkább elszigeteljük egymástól, és lehetővé váljon ezeknek az építőköveknak a tetszés szerinti mozgatása, cseréje, frissítése.

Az operációs rendszer virtualizációja már mindenki számára elérhető, például a most megjelent Virtual PC 2007 vagy a Virtual Server 2005 R2 használatával. Segítségével a hardver és az operációs rendszer közötti kötelekeket sikerült elvágni, így most már egy operációs rendszer tetszés szerint másolható, áthelyezhető egy másik gépre is akár.

Ha körülnézünk, milyen megoldások érhetőek el ma, találkozzhatunk még jó néhány érdekes virtualizációs elképzeléssel. Létezik már alkalmazásszintű virtualizáció is (pél-

A termékcsalád tagjai, és várható elérhetőségük

Microsoft® System Center

System Center Operations Manager 2007 (2007 első félév). A MOM új verziója, rendszerfelügyeleti eszköz – ez a vezérlőfülke, ahol mindig látszik az informatikai rendszer aktuális állapota. Segítségével a Microsoft bármely szerver-szoftvere és operációs rendszere, valamint rengeteg más gyártó szoftvere és hardvereszköze is felügyelhető.

System Center Configuration Manager 2007 (2007 második félév). Az SMS új verziója. Többek között frissítések kezelésére, távoli és tömeges telepítésre, valamint a CMDB összeállítására és karbantartására használható (hardver- és szoftverleltár).

System Center Essentials 2007 (2007 első félév). A középvállalatok és kisebb cégek informatikájának központi felügyeletét megvalósító eszköz, kombinálva az SCOM, az SCCM és a WSUS képességeinek számukra releváns részeit.

System Center Reporting Manager (már elérhető). Jelentéseket készíthetünk vele az informatikai rendszer állapotról és működéséről.

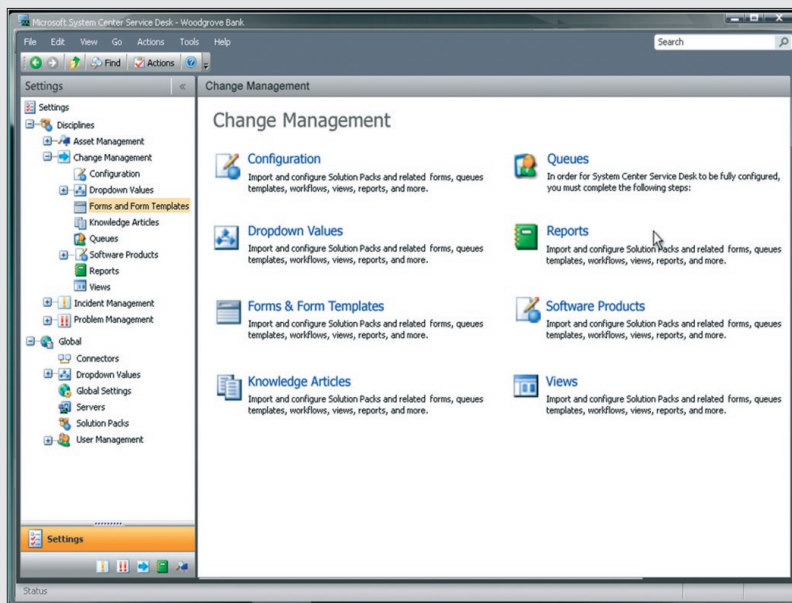
System Center „Service Desk” (2008 első félév). Az üzemeltetés központja, a MOF folyamatrendszerét köti össze a System Center eszközeivel – leginkább a MOF támogatási és változáskezelési negyedének tevékenységeit segíti.

System Center Capacity Planner (már elérhető). Kapacitástervező eszköz, hipotetikus rendszerek tervezésére és terhelésének modellezésére használható.

System Center Virtual Machine Manager (2007 második félév). Virtuális gépparkok központosított kezelésére alkalmas.

System Center Data Protection Manager (már elérhető). Automatizált adatmentés és -visszaállítás támogatására használható.

A „Longhorn” Server megjelenésének idején (ez 2007 végére várható) a DSI alatechnológiai elkezdenek beépülni az operációs rendszerekbe is, így például az új Server Manager felület és azon belül a Role Management Tool is SDM-mo-delleket használ a színtalpak mögött.



A System Center Service Desk összefogja a rendszermenedzsment-folyamatokat

A System Center termékcsalád az itt bemutatott problémák és ötletek megoldására született, és már számtalan tagja elérhető vagy hamarosan elérhető lesz. A System Center valójában a Microsoft rendszermenedzsment-termékeit és -technológiáit fogja össze, hogy segítse az informatikai rendszerek tervezését, felépítését és üzemeltetését.

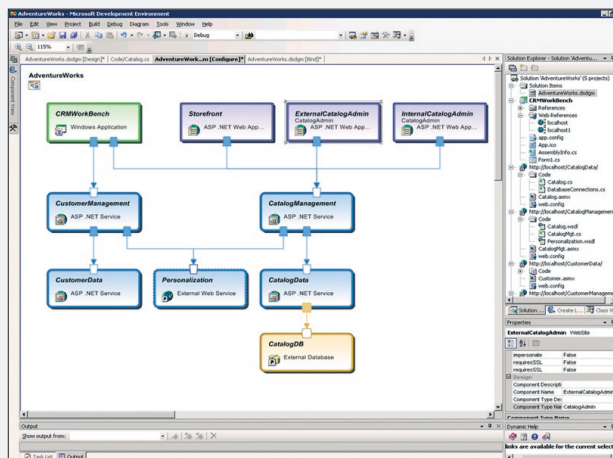
dául Microsoft SoftGrid), ez lehetővé teszi az alkalmazások futtatását úgy, hogy azok valójában nincsenek is telepítve az operációs rendszerre. Sőt, a futó szoftver azt hiszi magáról, hogy csak ő egyedül van telepítve az adott operációs rendszerre! Ezzel a megoldással sokkal jobban elkülöníthetők az operációs rendszertől a futtatandó alkalmazások és szoftverek, és az is megoldható vele, hogy akár egy gépen, egy időben párhuzamosan több verziójú Word (például XP, 2003, 2007) futhasson.

Találkozhatunk hardver, illetve tárolórendszer-virtualizációval is, ide sorolható például a hagyományos UTP kábelekkel is működő, clusterek összekötésére is alkalmas iSCSI, de még hosszasan sorolhatnánk a megoldásokat. Az mindenesetre közös mindegyikben, hogy az informatikus ezeknek az eszközöknek az alkalmazásával sokkal rugalmasabb, átláthatóbb rendszereket lesz képes kiépíteni, akár a korábbi megoldásoknál olcsóbban is.

Az igazi áttörést azonban ezek kombinálása jelenti majd. Tegyük fel, hogy összeköjtjük a virtualizáció adta lehetőségeket és a modellekben, illetve a CMDB-ben fellelhető tudást. Néhány példa, mik a felmerülő lehetőségek:

- A meglévő szolgáltatásainkat és operációs rendszereinket egy központi felületről oszthatjuk le a rendelkezésre álló hardverekre, ezek automatikusan települnek, és megfelelően beállítódnak (a modellek adatai alapján). Ezek a szolgáltatások természetesen az igényeknek megfelelően később még mozgathatók a gépek között.
- A rendszereket ért terhelés megváltozása esetén bármikor adhatunk több hardvert szolgáltatásainknak. Ez lehet az adott gépen belül is, további processzormagok vagy memória allokálásával (scale up), de

a fűrtözést támogató szoftverek esetében hamar, akár automatizáltan is üzembe állíthatunk egy újabb virtuális kiszolgálót egy másik fizikai hardveren (scale out).



Az első oldalon látott „rendszermodell” egy kicsit másképp – Visual Studio 2005-ben

Ez már majdnem egy igazi grid-megoldás, ahol egy összességében homogén géppark megadott szolgáltatásokat lát el. A végfelhasználó számára pedig teljesen mindegy, hogy a háttérben ez hogyan, hány gépen fut valójában. Mi pedig könnyen cserélhetjük a géppark részegységeit, anélkül, hogy ezt bárki észrevenné.

Heterogén rendszerek, iparági szabványok

Jóllehet a DSI alapját képező technológiák többségét a Microsoft találta ki, és fejlesztette ki azok első verzióit is, azonban azok mára már iparágazatra elfogadott szabványokká nőttek ki magukat. Az elosztott rendszerek felügyeletével és ezek szabványos megoldásaival foglalkozó testület, a DMTF (Distributed Management Task Force) például SML (System Modeling Language) néven szabványosította az SDM 3-as változatát.

Az SDM mindig is XML alapokon működött ugyan, azonban az SDM hármas verziója már kizárólag W3C szabványokra épül. Ez gya-

korlatilag azt jelenti, hogy a DSI modell alapú megközelítését nemcsak a Microsoft, hanem valamennyi gyártó képes lesz kihasználni saját rendszermenedzsment-megoldásában.

A heterogén rendszerek összekötése azonban a szabványos modelleken kívül a különféle platformok és menedzsment-szoftverek közötti kommunikáción is múlik. Erre szolgál a szintén W3C szabványokon alapuló WS-Management protokoll is, ami lehetővé teszi, hogy akár az IBM, a Microsoft, a Sun, a Dell, az AMD, az Intel vagy más gyártók megoldásai is képesek legyenek egymással kommunikálni.

Az sem mellékes, hogy már kezdenek felbukkanni azok a hardvereszközök (például hálózati printerek), amelyek beépítve képesek a WS-Management és a WS-Discovery alkalmazására, és így nagyon könnyen menedzselhetők, és automatikusan megmutathatják magukat a hálózat egésze számára.

Sok érdekes újdonság érkezik tehát a rendszermenedzsment területén! Mindenesetre megijedni nem kell, attól még igencsak messze vagyunk, hogy a számítógépek vagy a szoftverek öntudatra ébredjenek, és átvegyék az uralmat a világ felett. A DSI nem



A System Center egyik alapköve a virtualizáció

más, mint egy egységes koncepció, amely a Microsoft rendszermenedzsment-szoftvereinek fejlődését mutatja meg a következő évtizedre nézve. A System Center pedig az az eszközkészlet, amely lehetővé teszi számunkra, hogy egyszerűbbé tegyük az IT-rendszerekkel kapcsolatos teendőinket.

Budai Péter

(i-pbudai@microsoft.com) Microsoft Magyarország

További információk

www.microsoft.com/dsi

RENDSZEREK ÉS GAZDÁIK

Az informatikai rendszerek elég gyakran élnek szimbiózisban üzemeltetőikkel. Együtt nőnek, együtt érnek, együtt öregszenek.

Olyannyira összetartoznak, hogy szinte el sem lehet képzelni Ablak vállalatot Józsi – Zsiráf állami intézményt pedig Pista nélkül.

A vállalatok dolgai jól működnek, amíg Józsi és Pista életében be nem következik valami jelentős változás: nyugdíjba mennek, elüti őket a villamos, vagy elégedetlenek lesznek a fizetésükkel, és munkahelyet váltanak. Hirtelen megszűnik az együttélés – és ez azonnal meglátszik a szolgáltatás minőségén. A frissen felvett munkaerő alig érti a rendszer felépítését, újabb és újabb összefüggések derülnek ki, akár még egy év múltán is előbukkanhatnak hekkkelések, ilyen-olyan trükkkel megoldott feladatok.

Tudás a fejekben

A probléma jól ismert, tövig lerágott csont: Józsi és Pista a fejében elviszi (néha a sírba) a tudást, az élő tudást a rendszerről. Mi ez a tudás? Mindenekelőtt a rendszer leltára: mi van a hálózaton, kik használják. Azután a fejükben vannak a kapcsolatok: ha kiakad a DNS szolgáltatás, akkor leáll a levelezés; ha nem érkezik meg a vállalati jelentés, akkor a riportok sorban állnak a vállalatirányítási rendszerben; ha pedig nem jön időben egy sms, leállt a task manager, amely az sms-t időzítve küldte volna.

Van még másfajta tudás is Józsinál és Pistánál.

Ők ott voltak az egyes rendszerek, komponensek bevezetésekor. Tudják, hogy az a Visio-ábra miért tartalmaz eggyel több szerveret („végül nem jutott rá pénz”), vagy hogy miért vannak egészen más IP-címek a dokumentációhoz képest („nem maradt idő a tervek módosítására”). Nekik még elmondták szóban azt a néhány fortélyt, amit a tervezéskor bevetettek, meg „azt a három dolgot”, amit naponta ellenőrizni kell.

A végfelhasználók ugyancsak a mi rendszergazdáink tudását gyarapították. Tudnivaló, hogy Lajos paranoiás, és ha telefonál is, nem kell komolyan venni. Ha viszont Sanyi „szól le”, akkor áll a számlázás, vagy valami tényleg lassú. Pontosan érzékelhető, hogy reggelenként a terminálszerverek már nehezebben bírják az iramot (és rohamot), legközelebb majd azokat kell bővíteni, egyébként is már négyéves eszközök...

Végezetül Józsi és Pista az évek során bőséges tapasztalatot szerzett a hibák elhárítása területén, legyenek azok akár teljesen ismeretlenek. Először az eseménynaplót kell átböngészni: ott lesz a hibaüzenet és annak kódja. Ezt a kódot meg kell adni az eventid.net-en, hátha azonnal jön a megoldás. Ha így nem járt sikerrel a kolléga, akkor jöhet az internet áttűrése kereséssel, s lám, egyszer csak kibuggyan a megfelelő tudásbáziscikk. Most már csak el kell olvasni, le kell tölteni a hotfixet, telepíteni, szervert újraindítani és hopplá, kész vagyunk. Mindössze 5-6 óra munka.

Mielőtt elhagynánk a valóság alapot nem nélkülöző, mindazonáltal kitalált példánkat, és elméleti fejtegetésbe kezdenénk, érdemes elgondolkodni, miért is van mindez így.

Tudás (nem)áramlás

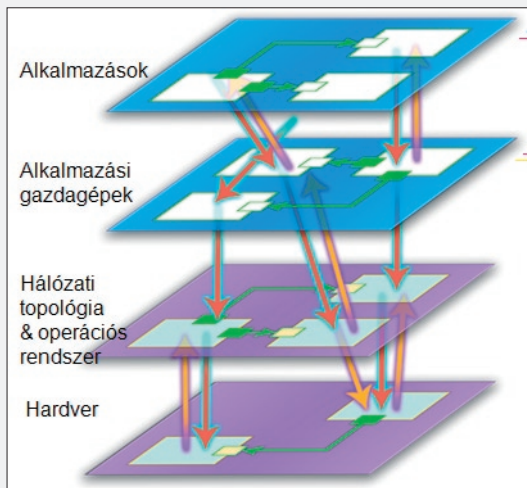
Az informatikai rendszerről sok mindenkinek van elképzelése (más szóval: tudása). Kezdjük a szoftverfejlesztőkkel: felismernek bizonyos problémákat, meghallgatják az ügyfeleiket, aztán készítenek „valamit”, amiről azt gondolják, jó, s ezt úgy, ahogy (úgy, ahogy tudják) dokumentálják, hogy aztán átadhasák a szoftvert azoknak, akik majd bevezetik. Nevezük ennek a második csoportnak a tagjait rendszertervezőknek.

A tervezők a „hozott anyagból” és a felmért igényekből kialakítanak egy elosztott architektúrát kapcsolatokkal, beállításokkal. Követik a szoftverfejlesztők ajánlásait meg a maguk tapasztalatait (a „legjobb gyakorlat” az aktuális elnevezés), és végül átadják a „kész” rendszert az üzemeltetőknek – Józsinak és Pistának. Az üzemeltetők a duplán hozott (torzított és hiányos) anyagból aztán megpróbálják üzemeltetni a rendszert, visszacsatolva a felhasználók panaszait és javaslatait.

A fenti folyamat, bár egyenes vonalú, egyenesletes mozgásnak tűnik, egyáltalán nem az. A folyamat résztvevői ugyanis nem értenek egymás világához, gyakran egymás „nyelvét” sem beszéljük. A szoftverfejlesztő sohasem mérete-

zett rendszert, a tervező pedig többnyire egyáltalán nem üzemeltetett, és ezek a tapasztalathiányok meg is látszanak a munkáikon.

Hányszor szentségelünk azon, hogy egy-egy alkalmazáshoz százával kell tűzfalportokat kinyitni? Nos, az a fejlesztő sem felelt soha biztonsággért, aki ilyen szoftvert adott ki a kezéből. És hányszor kell utólag fűrtözni valamit, pedig akár előre lehetett volna látni az igénye-



1. ábra. A különféle modellek és kapcsolataik adják ki a teljes rendszert

ket: a tervező is hibázhat bőven. Olyan régóta mennek így a dolgok a mi szakmánkban, és mindez olyan törvényszerűnek tűnik...

Fogd (a tudást), és fuss!

A hosszan, sok-sok (nem véletlenül) felsorolt példával a Microsoft Research kutatói is szembesültek, s megpróbálták a lehetetlent: megalkotni egy olyan nyelvet, amelyet megért a szoftverfejlesztő, a rendszertervező, az üzemeltető, sőt – talán ez a legfontosabb – a gép is. Az első eredmény neve SDM volt, ez a System Definition Model rövidítése. Az SDM egy olyan XML alapú, modellezésre alkalmas nyelv (metamodel), amellyel komplex, elosztott informatikai rendszereket lehet leírni. Miért éppen modellezés?

Egy rendszer akkor menedzselhető, ha annak minden aspektusa ismert. Az elvárt állapotokat meg kell határozni, az aktuális rendszerállapotot pontosan „érzékelni” kell, a kettőt össze kell hasonlítani, hogy az eltérés igényel-e beavatkozást. Ezenfelül olyan eljárásokra is szükség van, amely az aktuális állapotot bizonyos üzemeltetési paraméterek között tartja. Mindezt modellek segítségével valósíthatjuk meg.

Ez eddig a spanyolviasz – az igazi ötlet az, hogy az SDM-et használjuk a szoftver teljes életciklusában – a fejlesztéstől az üzemeltetésig. Hopp! Íme a javasolt megoldás az egymás nyelvét nem beszélő szakemberek számára. Ha a szoftverfejlesztő SDM-mel írja le az általa elkészített szoftvert, azt a rendszertervező képes lesz megérteni; hasonlóképpen a tervező végtermékét SDM-mel leírva az üzemeltető átláthatja a terveket – a visszacsatolás pedig szintén könnyebbé válik.

Az ötlet egyszerű, de olyan egyszerű, hogy tucatjával álltak mellé szoftverfejlesztő cégek (BEA, BMC, Cisco, Dell, EMC, HP, IBM, Intel és a Sun), így aztán az eredeti SDM harmadik verziója a „System Modeling Language” (SML) nevet kapta a keresztségben, vagyis mondhatjuk, hogy az SML az SDM utódja lesz majd, ha elkezdik alkalmazni.

Hogyan működik az SDM?

Mint minden modellező megoldás, az SDM is egy csomó, egymással kapcsolatban álló objektum. Az objektum a rendszer egy elemét reprezentálja, de ez lehet egyfajta karakterisztika, elvárt konfiguráció vagy állapot. Az objektumokat összekötő vonalak a karakterisztikák kapcsolatát hivatottak leírni.

Ha mindezt ábrázolni szeretnénk, akkor dobozokat és összekötő vonalakat lehetne rajzolni. A dobozok jelenthetnek rendszert, de alrendszert és komponenseket is. A vonalak a kapcsolatokat ábrázolják. Egy kapcsolat négyféle lehet.

A **tartalmazás (composition)**. Ilyen kapcsolat például az, ha az egyik SDM egy számítógépet ír le (valamilyen tulajdonságokkal rendelkező szervergép), míg a másik egy számítógépen futtatható szolgáltatást, például egy SQL Server 2005-öt. Ilyenkor az SQL Server 2005-öt „tartalmazza”, jelen esetben hostolja az adott számítógép, és ez a viszony tükröződik a modelljeik között is. Az SQL Server szintén „tartalmazhat” más alkotmense-

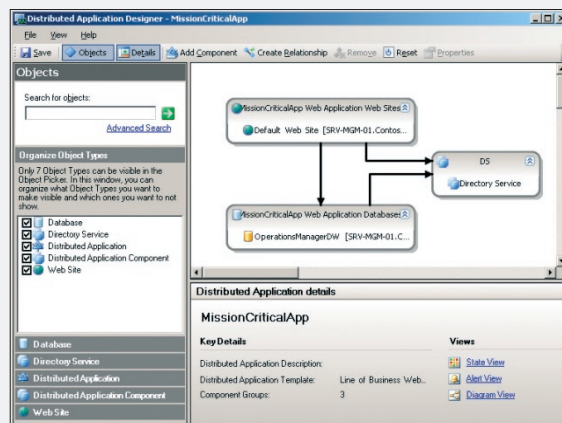
ket is, és így tovább, lemehetünk tetszőleges mélységig.

A **származtatás (derivation)**. Ennek a kapcsolatnak az általánosítás a lényege. A szülőmodell alapul véve lemásoljuk azt, majd szigorítunk rajta valamilyen megkötés hozzáadásával (restriction), és/vagy kiterjesztjük az eredeti modellt további tulajdonságokkal (extension).

Például van egy SDM-modell, amelyik a switchek általános képességeit és lehetőségeit tartalmazza, majd készítünk ez alapján egy másikat, amelyik egy konkrét Cisco switch képességeit mutatja meg.

A **kötöttség (constraint)**. Két komponens között fennállhatnak olyan kötöttségek, amelyek meghatározzák, hogy milyen beállítások esetén képesek együttműködni egymással. Az SQL Server példájánál maradvá: nem tehetünk fel SQL Server 2005-öt egy olyan számítógépre, amelyen például Windows 98 operációs rendszer fut.

A **folyam (flow)**. Az eddigieknél jóval egyszerűbb kapcsolat, gyakorlatilag valamilyen (adat)áramlást vagy kommunikációt ábrázol két komponens között. Például hálózati forgalom fizikai szinten a kábeleken át vagy magasabb szinten lévő protokollon át végzett kommunikáció (például SOAP).



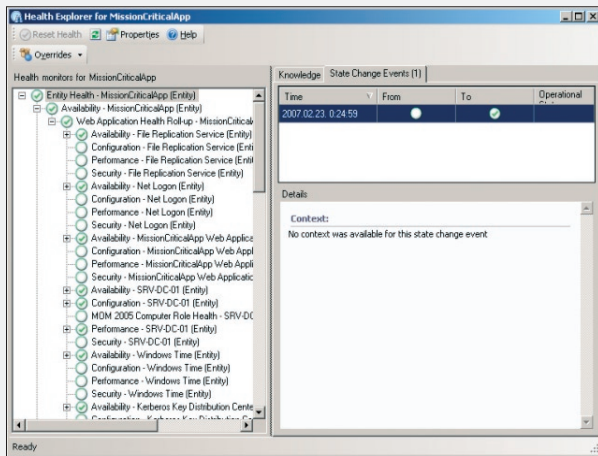
2. ábra. Egy üzletileg kritikus alkalmazás függőségeinek definiálása

Egyértelműen belátható, hogy az objektumok és kapcsolataik tetszés szerinti mélységben egymásba ágyazhatók, mintha fraktálokat szemlélünk.

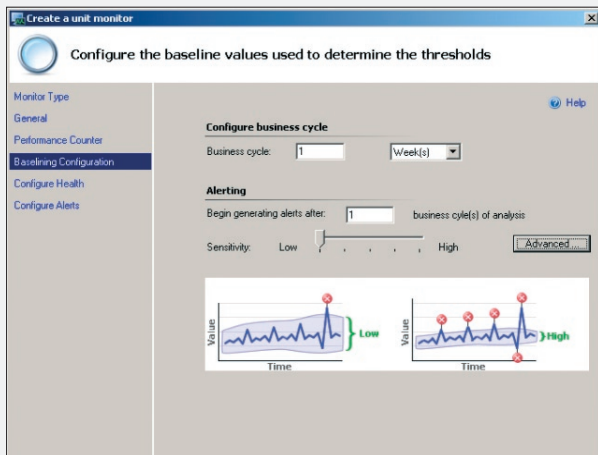
A jövő menedzsmentje

Milyen következményekkel jár, ha egy szoftvert az SDM szem előtt tartásával készítetnek? Egy ilyen szofver képes leírni önmagát, a sa-

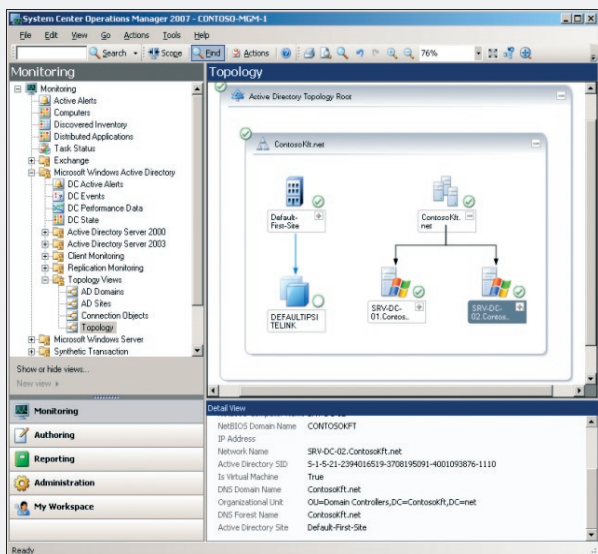
ját igényeit jelezni más (SDM-et értő) rendszereknek, de akár azt is, hogy ezek az igények, elvárások, körttségek teljesülnek-e.



3. ábra. Az egészségi állapottal kapcsolatos lehetőségek



4. ábra. Rugalmasan beállítható küszöbértékek



5. ábra. Egy egyszerűbb elosztott rendszer felügyelete

Ennél azonban tovább is mehetünk. Ha egy rendszer képes önmagát leírni, és „ismert állapotban van”, akkor talán az lenne a legmegfelelőbb, ha nem is nyúlnánk hozzá kézzel. Elvégezhetjük a módosítást a modellen, s ha minden szempontból konzisztens a kérésünk, maga az SDM-szolgáltatás végzi el.

Ezt nevezzük modell alapú menedzsmentnek, hiszen mi valójában nem a valós rendszert, hanem a modellt manipuláljuk. És hol van ilyen SDM-szolgáltatás? Bingó! A Longhorn világában.

Az SDM jelene

Akinek most elment a kedve az egészségtől, hogy valami nagyon távoli, valami nagyon ködös, megfoghatatlan, szoftverben sohasem manifesztálódott dologról értekezünk, az megnyugodhat: nem. A Microsoft három évvel ezelőtt tette közzé a maga vízióját a jövő rendszereiről, ezt Dynamic System Initiative-nak hívják (erről előző cikkünk szól), s ennek az egyik pillére az SDM nyújtotta modell alapú szoftverkészítés és üzemeltetés. Az induláskor három SDM-„hullámot”, vagy generációt vázoltak fel. Az első generációhoz a Visual Studio 2005 Team System tartozik, itt a tervezés időszakában lehet ellenőrizni az elképzeléseket. Azzal, hogy az SDM először itt jelent meg lehetővé vált, hogy egykor majd minden szoftver „üzemeltetésre kész” lehessen.

A második generációhoz a most megjelenő menedzsmenttermékek, valamint a „Longhorn” Server tartozik. A System Center

Operation Manager 2007 elosztott alkalmazások modellezésére és a maga egészségmodelljéhez használja az SDM-et, a System Center Configuration Manager 2007-ben – leánykori nevén SMSv4 – pedig az elvárt konfiguráció (desired configuration) funkcionalitása SDM alapú.

A harmadik hullám már nem SDM, hanem SML alapú lesz, s remélhetőleg a teljes rendszer modellezését lehetővé teszi.

SDM a gyakorlatban

Az alábbiakban rigorózan haladjunk végig a cikk elején felsorolt példákon, és nézzük meg, hogy az SDM alapokkal felvértezett System Center Operation Manager 2007 milyen megoldásokkal igyekszik Józsi és Pista tudását megőrizni, gondolva a nyugdíjazás, villamoselés és szakítás eseteire.

A rendszer leltára. Az Operation Manager 2007 képes felfedezni a körülötte működő informatikai környezetet, hardver- és szoftverelemeket. Háromfajta objektumot különböztet meg: az ügnyökkel felügyelt, az ügnyök nélkül felügyelt és az SNMP protokoll segítségével felügyelt eszközöket. Ez utóbbi és a szabadon használható konnektor-keretrendszer segítségével bármilyen eszköz felügyeletére alkalmas.

Az már csak hab a tortán, hogy teljes egészében ismeri a WS-Management szabványt, amelynek segítségével bármely, a szabvány szintje beszélő eszközt közvetlenül is, konnektorok nélkül képes vezérelni.

Vannak kapcsolatok. Az SCOM 2007 az SDM technológia segítségével lehetővé teszi a rendszergazdák számára, hogy tetszés szerinti elosztott alkalmazás architektúrát definiáljanak. Mi egy egyszerű webalkalmazást hoztunk létre (5. ábra), amely egy adatbázissal és a címtárszolgáltatással áll kapcsolatban.

A példa azonban összetettebb, mint első pillanatra látszik: a címtárszolgáltatás maga is egy összetett (mellesleg a rendszer által automatikusan generált) szolgáltatás. Ez jól mutatja a modellezés erejét: tetszőleges mélységű és összetettségű rendszert definiálhatunk, jelezve a kapcsolatokat. Abban a pillanatban, amikor elmentettük az elosztott alkalmazást, már indul is a rendelkezésre állásának mérése. Az eddig összetett valamiből egyetlen „objektum” lesz, amelynek egészségmodellje a belső, elosztott architektúra alapján áll össze.

Meglódulhat a fantázia: itt a lehetőség a saját összetett szolgáltatások definiálására, és azok összegzett rendelkezésre állásának mérésére

A riportok sorban állnak. Az SCOM 2007-ben, akárcsak a korábbi verzióban, riasztást lehet definiálni bizonyos teljesítménymutatókra, illetve azokra az esetekre, amikor a mutatók értékei eltérnek a normálistól. A korábbi megoldással szemben most azonban az eltérés nem merev érték, hanem rugalmas. Megtanítható, hogy egy adott üzleti ciklusban a hővégi zárás kivétel, és ott nem gond, ha például a processzorkihasználtság a szokásosnál – és a normál küszöbértékekénél – magasabb.

Az a Visio-ábra! Az SDM-funkcionalitás nemcsak az elosztott alkalmazások létrehozásakor, hanem topológiák feltérképezésekor is nagyon hasznos. Szemben azonban a statikus Visio-ábrákkal, itt élő – a valóságos állapotot ábrázoló – képekkel van dolgunk, amelyek tetszés szerint bővíthetők, a mélyükre lehet ásni stb. Az SDM tehát a rend-

szerünk élő, naprakész rendszer-dokumentációja, a frissítéséről pedig maga a szoftver gondoskodik, nem nekünk kell elvégeznünk.

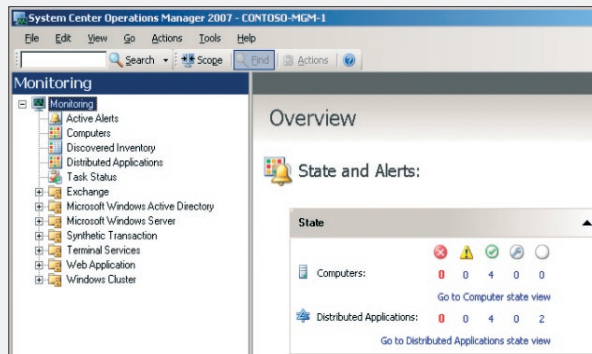
Azt a három dolgot... Igen könnyű ellenőrizni, mert az SCOM áttekintő ábrákkal emeli ki a legfontosabb információkat.

mentcsomagokban tudásbázisokat tartalmaz. Ha egy riasztás érkezik a konzolra, akkor a riasztáshoz tartozó cikkek azonnal megjelennek, minimalizálva a hibaelhárításra fordított időt. Sőt! Arra is van lehetőség, hogy a riasztásokhoz saját „vállalati” cikkeket írjunk, kiegészítve a meglévő tudástárat.

Meglehet, nem érintettük minden vonatkozásban a „tudás megőrzésének” témáját a rendszeremnedzsmenttel kapcsolatban, de az áttekintés talán mégis elég lesz ahhoz, hogy újragondoljuk az üzemeltetési módszertanainkat: vajon tényleg Józsi és Pista változó minőségű, sokszor megbízhatatlan, s csupán látszólag állandó tudására támaszkodunk, vagy megpróbáljuk összegyűjteni, rendszerezni és tárolni ezt a tudást ott, ahol a legnagyobb

sükség van rá: magában az IT-környezetben. Ez pedig a rendszergazdának is jó, hiszen végre tud a napi tűzoltásnál fontosabb feladatokra is koncentrálni.

Lepénye Tamás
(tamasi@microsoft.com) Microsoft Magyarország



6. ábra. Folyamatosan nyomon követhetjük rendszereink állapotát

Ezenfelül lehetőség van saját oldal összeállítására, ha valaki egy nagy szervezetben csak bizonyos rendszerek felügyeletét látja el.

A hibák elhárításának területén. Nem kell már feltétlenül órákon át az internetet keresgélni. Az Operation Manager a menedzs-

IT-BUSINESS TODAY

- felsővezetőknek, döntéshozóknak
- az elmúlt 24 óra legfontosabb magyar és nemzetközi ICT híre
- ingyenes napi hírlevél

Regisztráljon!

www.it-business.hu/hirlevel

MASS DEPLOYMENT

Már a kifejezés fordítása is problémás egy kissé. Telepítés? Nem, annál több. Tervezés és telepítés? Nem, ennél inkább kevesebb. Bevezetés? Esetleg, de a magyarban ez egy rendkívül széles jelentésű szó. Tömeges telepítés? Talán ez a legjobb.

Hívhatjuk persze akárhogy, a rendszergazdák, üzemeltetők tudják, miről van szó, és valószínűleg azzal is tisztában vannak, hogy egy olyan kulcsfontosságú területet érintünk, amelynek érvényessége az egészen kisméretű hálózatoktól kezdve a több földrész felölelő nagyvállalati rendszerekig is terjedhet. Ebben a témakörben rettenetes méretű eszközzel, megoldási módszerrel, leírással, elsajátítandó dokumentummal találkozunk szembe az, aki belevág, ergo először is próbáljunk meg rendet tenni a fejünkben, és behatárolni, hogy a különböző célok elérése érdekében mely eszközökkel lehetséges, illetve érdemes dolgozni.

Másrészről a Vistával rengeteg újdonság köszöntött be számos területen, és természetesen nemcsak a látható felszínen, hanem a mélyben is. A telepítés – és persze a tömeges telepítés –

rendszerünk tervezésének, létrehozásának lépései előtt röviden bemutatunk.

BDD 2007

Az új (idén január közepétől letölthető: <http://www.microsoft.com/technet/desktop-deployment/bdd/2007/default.mspx>) BDD-csomag rendkívül komplex és integrált, de mégis egészen jól kiismerhető és kezelhető. Csomagról beszélünk, mivel a BDD egy megoldásötvető eszköz, amely integrál egy halom komponenst, és szépen „aládolgozik” a tervezési módszereinknek.

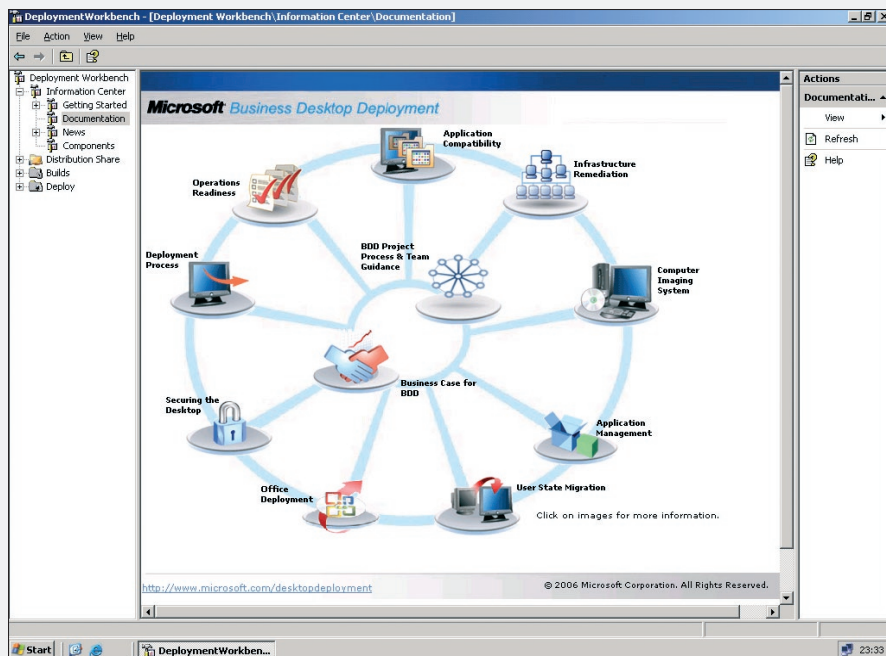
Nagyon úgy látszik, hogy feltett szándék volt belezúfolni a BDD 2007 körülbelül 30 megabájtos telepítőjébe, amit csak lehet, mert például a mostanában szokásos áttekintő oldalon kívül szinte az összes lehetséges doksit elérhetjük könnyedén – szintén az MMC-n belül. A faszerkezet passzoló pontjában egy hatalmas képet láthatunk, ami elsőre megrázképtető, mert nemcsak látványos, hanem hasznos is, az egyes elemekre kattintva a BDD használatát segítő tekintélyes háttéranyag tartalomjegyzéke lapul.

Építsünk telepítési rendszert!

Megvan a kulcseszközünk, nézzük tehát sorban, milyen feladataink lesznek egy komplett telepítési rendszer munkába állítása kapcsán. Elméleti szinten legalább négy nagy részre osztjuk fel a feladatokat: tervezésre, fejlesztésre, teszteszre és kivitelezésre.

Tervezés

Ebben a körben a jelenlegi helyzet felmérése az első teendő, azaz el kell döntenünk, hogy



A BDD konzol dokumentumtára, az eligazodást segítő képes tartalomjegyzékkel

sohasem tartozott a látványos területek közé, ettől függetlenül itt is gyökeres változások történtek: nagyon úgy néz ki, még sohasem volt ilyen könnyű dolgunk, hogy egy olyan rendszert tervezzünk, amelynek segítségével a lehető legegyszerűbben tudjuk majd a Vistát, illetve például az Office 2007-et telepíteni, minimális beavatkozással, központilag, akár több száz gépre is. Ehhez láthatóan a kulcs a Business Desktop Deployment (BDD) 2007 lesz, amelyet a telepítési

a rendelkezésre álló telepítési típusok közül (új telepítés, frissítés, csere) melyekre lesz szükség. Az szinte biztos, hogy többre is, ergo valószínűleg kombinálnunk kell majd ezeket a módszereket. Minden típus más és más jellemzőkkel bír, nézzük ezeket sorban.

Az új telepítés a legegyszerűbb metódus, mert teljesen új gépet használunk, azaz gyakorlatilag nincs mit migrálni, nincsenek felhasználói adatok, profilok, és valószínűleg az

adatokat a régi gépen lementjük, az új gép új operációs rendszerét és teljes környezetét beállítjuk, majd a két gép között egy importálást végzünk.

A tervezés következő lépése a telepítőkészletek terjesztési módszerének kiválasztása, amely elsősorban az informatikai infrastruktúránktól és a rendelkezésre álló eszközeinktől függ. A BDD 2007 használata esetén két fő variáció lehetséges, az úgynevezett

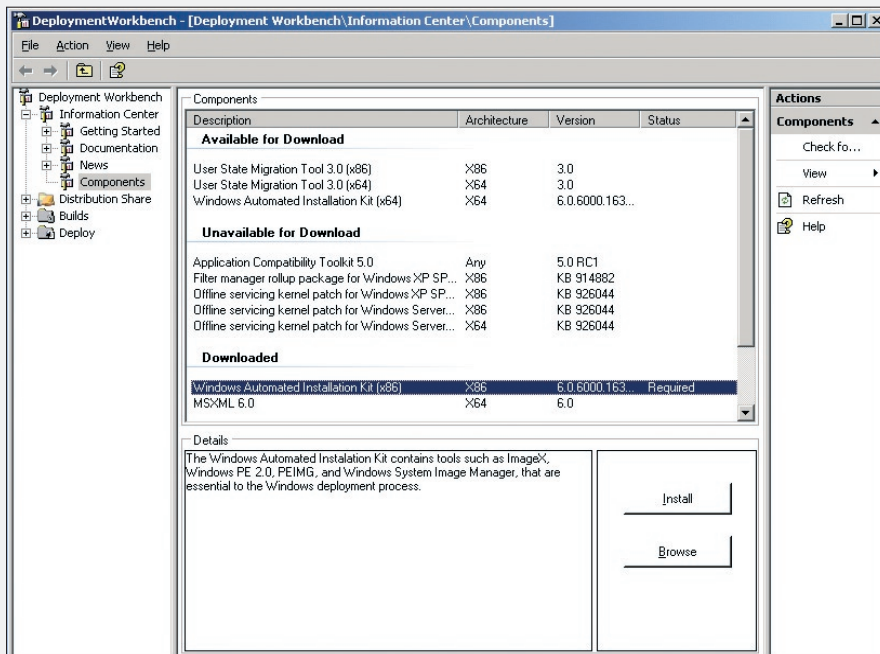
azt is, hogy az előzetes konfigurálással kevesebb dolgunk lesz, mivel minden telepítéskor manuálisan adjuk majd meg a paramétereiket. De amit ezzel nyerünk, azt elveszítjük a másik oldalon, mivel több száz gép esetén ez nyilván nem járható út. Ez az a tulajdonság, ami miatt valóban csak kisebb szervezeteknél célszerű ez a módszer.

A másik módszer, a ZTI a nagyobb rendszerekhez készült. Mindenképpen szükséges hozzá az SMS 2003, az SMS 2003 SP2 és az SMS 2003 OSD Feature Pack (ez utóbbi az operációs rendszerek telepítésének eszköze az SMS-ben, OSD – Operating Systems Deployment). Emellett Windows 2003 kiadóknak és címtárak is szükség van. Ebben az esetben a telepítőkészletek disztribúciós pontja az SMS alá van rendelve, a kliensek telepítése pedig szintén a WDS-ből vagy közvetlenül az SMS-ből kezdeményezhető. Az előzetes, a BDD-ben végzett konfiguráció bonyolultabb, de a telepítési procedúra mindig teljesen automatikus, semmilyen további, menet közbeni beavatkozást nem igényel, tehát kifejezetten ideális az igazán tömeges telepítésre.

A következőkben fel kell mérnünk, hogy mi mindenre van szükségünk a BDD 2007-hez, illetve az LTI/ZTI módszerekhez, és ezekről a szoftveres komponensekről előzetesen gondoskodnunk is kell. Az utóbbi két technika szükségleteit már kivesztük, a BDD 2007 igényeiről viszont még nem esett szó. A terjesztési módszerektől függetlenül a következő komponensekre szükség lesz:

- User State Migration Toolkit 3.0;
- Application Compatibility Toolkit 5.0;
- Windows Automated Installation Kit;
- Microsoft Core XML Services (MSXML) 6.0;
- Microsoft Management Console 3.0;
- WSH 5.6. (csak XP és W2K/W2K3 esetén);
- Microsoft .NET Framework 2.0.

Semmiképp ne ijedjünk meg ettől a listától, hiszen egy részük a telepítéskor automatikusan felkerül, emellett a legszebb ebben a szakaszban az, hogy a többi alkotóelem a kezelőfelület (BDD Workbench) indítása után rögvést letölthető és telepíthető – az MMC-n belül! Sőt, a frissítésükre ugyanígy, ugyanígy van biztosítva a lehetőség. Még arra is odafigyeltek, hogy ha bármilyen okból megszakad egy letöltés (a WAIK például több



A Deployment Workbench komponensek menüpontja

alkalmazásokkal és a meghajtóprogramokkal sem lesz gond.

A gyakorlatban a frissítés a legproblematisabb eset, mert a jelenleg is működő operációs rendszer helybeli frissítését jelenti egy újra, a meglévő profilokkal, adatokkal és lehetőleg minél több, az új operációs rendszer alatt is működő régi alkalmazással. Valamint ez az egyetlen eset a felsoroltak közül, amikor egy esetleges fájlrendszer-cserére vagy -módosításra is fel kell készülnünk. Ráadásul a gép is marad ugyanaz, tehát a gépfüggő paraméterek (hardverek, driverek) problémáival is számolnunk kell.

A tisztítás speciális módszer, amelynek során egy működő környezet összes, a jövőben is szükséges adatát lementjük, majd a régi operációs rendszer törlése után egy újat telepítünk. Tehát gyakorlatilag migrálunk, de a gép marad, és tiszta lappal indul.

Csere. Ez az igazi migráció! A szükséges

Lite Touch Installation (LTI), illetve a Zero Touch Installation (ZTI). A két lehetőség egy helyen említéséből talán rögvést sejtethet az is, hogy a BDD-ből nincs többé Standard, illetve Enterprise változat – összehegesztették őket. Ez azzal az előnnyel is jár, hogy bármely terjesztési módszert is választjuk, a Deployment Workbench-ben végezzük majd el a telepítőkészletekkel kapcsolatos összes teendőt.

Az LTI minimális infrastruktúrát igényel, az ajánlás szerint maximum 25 PC-vel számolva. Ebben az esetben az operációs rendszereket egy hálózati megosztásból (disztribúciós pontból) vagy egy eltávolítható médiáról (CD, DVD, pendrive, USB, HDD stb.) telepítjük. A telepítés művelete indítható automatikusan (többek között a Windows Deployment Services-zel) vagy manuálisan, például a WinPE-vel indítva a gépet. Ha ezt a módszert választjuk, akkor tudnunk kell

száz megabájt), akkor legközelebb nem újraindul, hanem folytatódik. Más szempontból is intelligens, szépen felismeri a rendszerbe már korábban telepített, a BDD-hez passzoló eszközöket, illetve a például manuálisan – a BDD MMC-n kívül – felkerülteket is.

A tervezési szakasz következő lépése egyformán érvényes az előbb említett két módszerre, ugyanis mielőtt elkezdjük majd a konkrét telepítéseket, szükség lesz egy, a környezettől függő műveleti sorrendre és esetleg további testre szabásra. Ezt egy eléggé összetett fájlban (CustomSettings.ini) fogjuk tárolni, amelyhez viszont szükség lesz a telepítendő gépek számos adatára (a gépek MAC-címe, UUID-ja, esetleges sorozatszám, az alapértelmezett átjáró címe és egyebek). Ezekkel tehát rendelkezniünk kell előre, de segítségképpen a szükséges konkrét paraméterek listáját, illetve részletes mintákat e fájl elépítéséről mind megtaláljuk a BDD 2207-ben, a dokumentumok között a Deployment Configuration Guide.doc-ban.

Fontos dolog a tervezés utolsó lépéseként előre eltervezni azt, hogy hogyan fogjuk ellenőrizni a telepítések végrehajtását. Ehhez jelenleg a MOM 2005 a kulcs, azaz a Reporting Services-zel van lehetőség jelentések készítésére, mivel mind az SMS-hez, mind a BDD 2007-hez rendelkezésre áll egy Management Pack.

Fejlesztés

A telepítési rendszer építésének ez a szakasza már gyakorlati elemeket is tartalmaz, nem is keveset. Első körben telepíteniük kell a BDD 2007-et, amely bármilyen modern operációs rendszerre feltelepíthető (nyilván Vista-ra is), de valószínűleg egy kiszolgálóra érdemes igazán, arra, amelyikre például a telepítési rendszer többi elemét is fel fogjuk pakolni.

A BDD 2007 tartalmazza az LTI/ZTI szkripteket, konfigurációs fájlokat, az oprendszer és WinPE imagek elkészítéséhez szükséges összes varázslót, és többek között a már említett USMT 3.0-at, a profilok és egyéb felhasználói adatok mentéséhez és visszatöltéséhez. Egyszerűen minden eszközt és forrást, ami – bármelyik terjesztési típushoz – csak kellhet.

Akarmelyik terjesztési módszert választjuk, szükségünk lesz a telepítőkészletek tárolására, azaz az első lépésként létre kell hoznunk egy disztribúciós pontot.

Ebből legalább négyfélélt kreálhatunk a BDD Workbench-csel.

1. Lab/Single-Server deployment: az adott gépen a telepítés során létrejött Distribution mappát osztjuk meg, és ide kerül a csomag. Frissítés esetén ide csatlakozunk be például egy XP GUI-ról a megfelelő .vbs futtatásával, vagy a WinPE is innen táplálkozik – teljesen automatikusan.

2. Separate Deployment Share: egy másik mappa megosztása és feltöltése a cél, akár helyben, akár egy másik gépen. Ez nyilván akkor szükséges, ha a BDD nem az adott, az image-eket tároló kiszolgálón van.

3. Removable media (DVD .iso, USB-lemez vagy pendrive): értelemszerűen az említett hordozókra készült csomag.

4. SMS2003 OSD: egy olyan tároló kialakítása, amelybe az összes olyan fájl belekerül, ami szükséges ahhoz, hogy az SMS speciá-

san. Ezekről a BDD-doksi mappájának Zero Touch Installation Guide.doc állományából kaphatunk részletes információt.

Van már telepítőkészlet-tárolónk, de nincs még olyan eszközünk, amellyel a telepítés kezdőfolyamata automatikusan elindítható például az új gépek esetén. Szükség lesz tehát

What's New in ConfigMgr OSD?

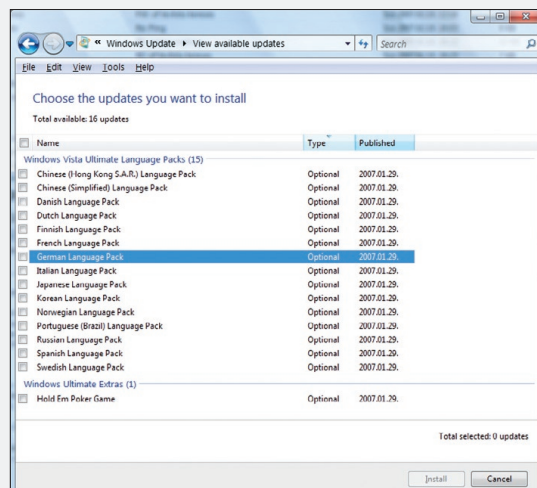
Scenario	SMS 2003 OSD FP	ConfigMgr OSD
End-to-end deployment	Yes	Yes
Fully automated	Yes	Yes
Wipe-and-load upgrade	Yes	Yes
Bare metal deployment w/PXE	Loose integration w/RIS	Built-in integration w/WDS
Side-by-side	BDD scripts	Yes, w/built-in SMP
Fully offline deployment	No	Yes
Integrated Vista upgrade planning	No	Yes
Full server deployment	No	Yes
Security	Good	Much stronger
Flexibility/customizability	Good	Excellent
Vista/LH compatibility	Good	Excellent
Device driver management	No	Yes

Microsoft
System Center
Configuration Manager 2007

A System Center Configuration Manager 2007 is sok új képességgel bővült

a Windows Deployment Serverre, azaz a RIS utódjára. Ezt megtaláljuk a WAIK- vagy az OPK-csomagban, de a Windows Server 2003 SP2-ben, illetve természetesen a Longhorn Serverben is elérhető lesz, választható komponensként. Jelenleg kétfajta módon konfigurálhatjuk: a GUI-s varázslóval, illetve a WDSUTIL.exe parancssori eszközzel.

Két fő területért felel konkrétan a WDS: miután a PXE kliens csatlakozott hozzá, el kell indítani a kliensgépen a WinPE-t vagy közvetlenül a Vista telepítőjét. Ez az állítás elsősorban az LTI módszernél igaz, illetve a ZTI esetén csak olyan szcenáriókban, amikor az SMS-sel nem lehetséges felügyelni az adott klienst. A WDS előkészítése is összetett folyamat, először meg kell majd határozni a WDS „üzemmódját” (Legacy, Mixed, illetve Native), amelyből az első teljes RIS-kompatibilitást nyújt, a második a vegyes mód, a harmadik pedig a WDS összes új lehetőségét megengedi. Ez utóbbi nem is használható a ZTI esetén, mert az SMS OSD nem kompatibilis vele. Ezután meg kell „mutatnunk” a WDS-nek a telepítőkészleteket és az indítókészleteket (a WinPE image-eket), azaz be kell majd másolni ezeket a WDS szerverre. Nem árt, ha tudjuk, hogy mivel a WDS-nek van teljesen RIS-kompatibilis üzemmódja is, ezért nemcsak az új (Vista – wim), hanem a

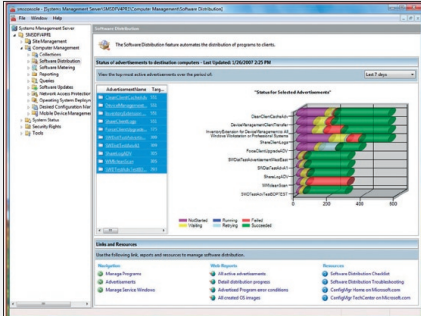


Egyszerűen telepíthető Vista nyelvi csomagok a WU listában

lis oprendszer-telepítő komponense képes legyen majd értelmezni és használni a lemezképet. Ezt a típust értelemszerűen csak a ZTI-nél használhatjuk, sőt, ennél a módszernél csak ezt. Meg kell említenünk, hogy a ZTI esetén (az SMS OSD miatt) további speciális állományokat is telepíteniük kell – manuáli-

régi (risetup és riprep) image-ek is használhatók vele.

Ezután már csak a WDS-sel kapcsolatos utolsó művelet maradt hátra, azaz az ismert azonosítóval (GUID/UUID) rendelkező gépek számítógépfiókjának elkészítése az



Softverdisztribúció System Center Configuration Manager 2007-tel

Active Directoryban. Ebben a műveletben semmilyen változás nincs, minden maradt a régiiben.

És még mi maradt ebben a fázisban? Például egy igen lényeges művelet, konkrétan annak eldöntése és kivitelezése, hogy mely felhasználói fiókokat milyen jogosultságokkal kell felvértetni, hogy az egész telepítési folyamat sikeres legyen. Többek között szó van a disztribúciós pontok, a megosztott mappák, a speciális alkalmazások vagy egyéb szerverek (SQL, Exchange) eléréséről. A jogosultságok beállítása némiképp eltér a két fő módszerünk esetén. Az LTI-nél egyszerűen a már említett CustomSettings.ini-ben konfigurálhatjuk a megfelelő fiókot (UserID, UserDomain, UserPassword), a ZTI-nél szintén, de itt az SMS 2003 Advance Client Network Access Account fiókot is használhatjuk. Az egyéb szerverekhez történő csatlakozás, illetve hitelesítés módja a szokásos „Connect to UNC action”.

A fejlesztési szakasz utolsó előtti lépése talán a leglátványosabb. Ekkor történhet meg ugyanis az eredeti operációs rendszer, illetve a WinPE telepítőkészletek importálása, összerakása és konfigurálása, az esetleges további alkalmazások és meghajtóprogramok „hozzáragasztása” a végleges image-hez. Ezeket a feladatokat részben a BDD Deployment Workbench-ben, részben manuálisan végezhetjük el, illetve a ZTI esetén ekkor kell használnunk az SMS OSD képességeit is.

Végül nem maradt más, mint hogy elvé-

gezzük a maradék munkát, azaz elkészíteni a műveleti sorrendet, és a tervezési szakaszban összegyűjtött helyi adatokkal elvégezni a testre szabást, a már említett CustomSettings.ini fájlban.

Tesztelés

Elvileg ez egy rövid, ámde velős szakasz is lehet, amelyben a leendő problémák kiderítése a cél – tesztkörnyezetben. A számunkra ideális terjesztési módszert, illetve ezen belül a 4 fő telepítési típus közül a megfelelőket próbáljuk ki ekkor, ellenőrizve a folyamat lépéseit, dokumentálva a problémákat, majd még az éles működés előtt kijavítva a fejlesztés vagy éppen a tervezés hibáit.

Kivitelezés

Nehéz dolgunk most már nem lesz, bár a telepítések még csak ezután jönnek. Igazából ez már csak – a telepítési típustól és környezettől függően – a WDS vagy az SMS indí-

talán XP-t telepítettünk már vállalati módszerekkel, viszont mostantól a Vistával szeretnénk folytatni, akkor nem árt figyelembe venni a következő tényeket, illetve (általában előnyös) változásokat.

1. A Vista telepítőkészlete jóval nagyobb méretű. Korábban bármelyik operációs rendszer telepítőkészlete bőven ráfért egy CD-re és a telepítés után is maximum 1-2 gigabájt helyet igényelt a partíción. A Vista (és a „Longhorn” Server is) már DVD-n érkezik (az install.wim kb. 2,2 gigabájt), és minimum 5 gigabájt helyre van szüksége a kitömörítés után. Így aztán megfontolásra érdemes a terjesztés módja, mondjuk egy 10 megabites vagy egy nem switchelt hálózaton mindenképp. A CD mint hordozó is nagyjából kiesik, ezenkívül egyelőre a pendrive-okból sem a 4/8 gigabájtos a tipikus, de ha van, jól jöhet, mert viszonylag könnyen bootolhatóvá tudjuk tenni, ráadásul kicsi és gyors. Arra is rá kell jönnünk a Vista alatt, hogy

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>bcdedit

Windows Boot Manager
-----
identifier          {bootmgr}
device              partition=C:
description         Windows Boot Manager
locale              en-US
inherit             {globalsettings}
default             {current}
displayorder        {current}
tooldisplayorder    {memdiag}
timeout             5

Windows Boot Loader
-----
identifier          {current}
device              partition=C:
devicepath           \Windows\system32\winload.exe
description         Microsoft Windows Vista
locale              en-US
inherit             {bootloadersettings}
osdevice            partition=C:
systemroot          \Windows
resumeobject        {8fa7990d-7d2d-11db-beee-ea80167c040b}
nx                  OptIn

C:\Windows\system32>
```

Az új boot manager, a bcdedit.exe

tásából vagy a WinPE valamilyen médiáról indítása után a manuális varázsló kattintgatásából áll. Ha jól terveztünk, fejlesztettünk, illetve teszteltünk, sok gond nem lehet.

Régen és most

A komplett telepítési rendszer kiépítésének procedurája után térjünk át egy másik témára, mégpedig az eddigi és a Vistával kezdődő korszak különbségeire – természetesen a telepítés témaköréhez kapcsolódóan. Ha szám-

nincs I386 mappa, és nem is vette át a szerepét semmi, minden, ami kellhet a jövőbeni telepítésekhez, a Windows mappán belül van (és nemcsak a SYSTEM32-ben).

2. Moduláris felépítés. Egy ideje már a modularitás is bevett jelszó a Microsoftnál, ennek ékes bizonyítéka a Vista és az Office 2007 felépítése, de ezt láthatjuk majd az IIS7-ben is. Ez a változás jelentősen érinti a telepítés területét is, hiszen emiatt vagyunk képesek a korábban említett WSIM-mel olyan

hatékonyan válogatni a komponensek közül. Sőt, a biztonsági frissítések, a nyelvi csomagok, a szervizcsomagok szintén egyszerűen hozzáadható elemekké váltak. Ezeket például a Package Manager (PKGmgr) segédprogrammal tudjuk integrálni a Vista esetén, offline és online módon is, amiből az első a nagyobb durranás, hiszen még a telepítés előtt felszerelhetjük az (eredeti!) készletet az aktuális javításokkal, tehát az esetleg rizikós működés kiküszöbölhető. A különböző meghajtóprogramokkal ugyanez a helyzet, azaz szintén offline hozzáadhatóak.

3. Ami már nem kell többé. Ilyenek a következők:

- RIS – teljes csere a WDS-sel (a W2K3 miatt azért még támogatott), a RIPREP és a RISEXP viszont nem működik együtt a Vistával;
- Setup Manager (Notepad) – a WSIM mindenben jobb, szebb, kényelmesebb és okosabb;
- WINNT.EXE és WINNT32.EXE:SETUP.EXE van csak;
- SYSCONFIG: csere, helyette van OCSETUP és az előbb említett PKGmgr;
- DOS boot floppy: használjunk Windows PE-t!

4. Text módú telepítés? Ha eléggé idős vagyunk, akkor tudjuk, hogy a lassan történelemmé váló Windows NT-től kezdve ugyanazt a szöveges telepítőt használjuk. Persze a telepítő egy része már színes-szagos, és ebben vannak is különbségek az oprendszerek között, de igazából minden telepítés ugyanúgy kezdődik. Az indítás után text módban a rendszerfájlok kicsomagolása az első lépés, majd ezek telepítése, a registry-kulcsok létrehozása, illetve a biztonsági beállítások alkalmazása következik. Ezután jöhet csak az újraindítás, és a telepítés második fázisa.

Nos, a Vistában már nem így van, a text módú telepítés nincs többé, az adott Vista image-gépre „rüházása” az első lépés, amelynek során szinte nem is kell (nem is lehetséges) közbeavatkoznunk. E folyamat után, gyakorlatilag a telepítés legvégén van csak egy olyan szakasz, ami egyenértékű a korábbi, menetközben lezajló testre szabással.

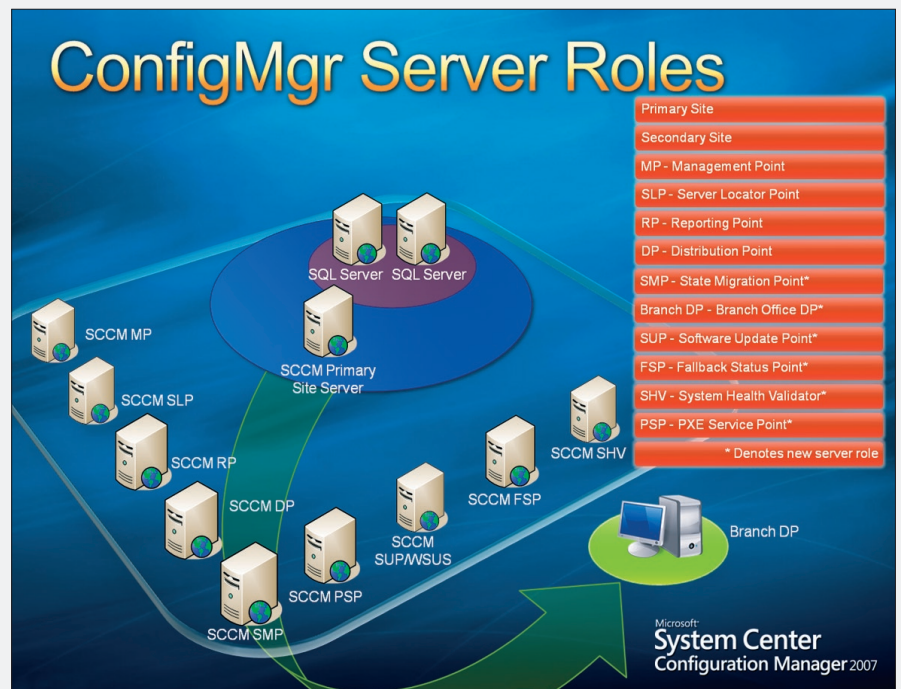
A lemezkép preparálási folyamata is változott. A Vista előtt a Syspreppel végeztük ezt el, rögtön azután, hogy beállítottunk minden jellemzőt, feltelepítettük vagy leszedtük

a komponenseket, és így tovább. A Vistában is megtalálható a Sysprep (%Windir%\System32\Sysprep), de igazából nem szükséges, hiszen a DVD-n található lemezkép (az install.wim), teljesen alkalmas a telepítésre, főképp, ha korábban említett offline módon frissítjük például a biztonsági javításokkal vagy driverekkel.

5. Immár a múlté a boot.ini is. Fontos tudni azt is, hogy a Vistában (és a WinPE 2.0-ában) a rendszerindítás konfigurálása is változott. Az új boot loader egy speciális állományból (BCD) tölti be a beállításokat, illet-

kezelést tekintve szintén használhatjuk a jól bevált Jegyzetömböt, de jó, ha tudjuk, hogy a WSIM sokkal kényelmesebb és áttekinthetőbb erre a célra.

7. Lokalizált változatok. Az XP-ben két módszerünk volt a különböző nyelvű lemezképek létrehozására. Vagy külön-külön generáltunk egy-egy lemezképet az eltérő nyelvű verziókhoz, vagy külön telepítéssel hozzácsaptuk – mondjuk egy angol nyelvű változathoz – a MUI-t (Multilanguage User Interface) és a szükséges nyelvi csomagokat. Egyik sem igazán jó megoldás, de nem volt mit tenni.



A System Center Configuration Manager 2007 szerepkörei, skálázhatósága

ve egy speciális programot (bcdedit.exe, csak az admin módú parancssorban indul el) használunk a beállításra.

6. Unattend.xml. Vista előtt az irányított telepítés konfigurációs állományai több, egyszerű szövegformátumú fájlban tárolódtak. A Vistában mindezek egyetlen .xml fájlban ötvöződnek, ennek neve Unattend.xml, és a BDD 2007-ből egyből meg tudjuk nyitni a WSIM-mel. Ez a fájl egyben tartalmazza a korábbi Sysprep.inf (a mini-telepítés beállításai), a Winbom.ini (a WinPE konfigurációs fájl) és a Cmdlines.txt (amely a mini-telepítéskor használható parancsok listáját tartalmazza) fájlokat. Ennek ellenére továbbra is lehetséges a szeparált fájlokat is alkalmazni, nem muszáj összerakni mindent az xml-ben. A

A Vista viszont teljesen mértékben nyelvfüggetlen felépítésű, pár napja meg is jelent az első 16 nyelvi csomag a Windows Update-en (egyszerű telepíteni, kiválasztjuk, letöltjük, és váltunk a Control Panelen, csak egy kilépés/belépés kell, és működik). Így aztán természetesen elhelyezhetünk a lemezképbe nyelvi csomagokat, sőt üzemeltetési szempontból még talán ennél is fontosabb, hogy a legtöbb esetben elég lesz egyetlen biztonsági javítás az összes nyelvi verzióhoz. Vélhetően nem kell ecsetelni, hogy ez mennyire hasznos dolog... Ahogy az is, hogy az összes nyelvi változathoz egyetlen Unattend.xml konfigurációs fájlra van szükség.

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

SYSTEM CENTER ESSENTIALS: FEGYVERT A HŐSÖKNEK!

Az informatikát alkalmazó szervezeteket jól el lehet különíteni aszerint, hány végfelhasználói berendezést üzemeltetnek. Ha ez a szám 25 alatti, IT-szempontról beszélünk, 500 felett pedig már mindenképpen nagyvállalatról van szó. A 25–500 végberendezést üzemeltető szervezetek a középvállalatok – informatikai Középfölde sok-sok IT-hőssel.

A középvállalatok kiterjedésben, szervezeti felépítésben már eléggé összetettek ahhoz, hogy meglepően komoly elvárásokat fogalmazzanak meg informatikai egységeikkel szemben. Egy fejlett IT-rendszerrel rendelkező közepes cég szinte mindenféle üzleti alkalmazást használhat az ERP-rendszertől kezdve az üzletiintelligencia-alkalmazásokon át a vezetőknélküli kommunikációt biztosító eszközökig. A széles spektrumhoz azonban nem kapcsolódik megfelelően nagy üzemméret, így az egyes rendszerekhez IT-specialisták alkalmazása túlságosan drága multság lenne.

Az általában járt út az olyan szakemberek elcsábítása, akiket a „Mindent tudni akarok” attitűd jellemez, s akik akár éjt nappallá téve is igyekeznek megfelelni a szinte lehetetlennek: széles szakmai spektrumban kellően mély ismereteket szerezni, hogy a relatíve össze-

tett és nagy IT-rendszert teljesen átlássák, üzemben tartásuk és fejlesszék. Sok mindent ismerni felszínesen – nem nagy tudomány. Egy-két technológiában elmélyedni a végtelenségig – kevesek igénye (vagy kiváltsága). Mindent tudni, nagyon-nagyon alaposan: az IT-hősök kihívása!

Kisvállalat vagy középvállalat?

Szinte minden nagy gyártó, amelyik az IT-üzletben mozog – alapozza akár a hardverre, akár a szoftverre a maga elképzeléseit – kínál a kisvállalatok számára „olcsó”, „egyszerű”, „könnyen

használható”, „azonnal működő”, „instant”, „fogd-és-vidd”, „kapcsold be és működik” stb. jelzőkkel ellátott megoldásokat. A kisvállalatok (kis szervezetek) régóta ismert és bevett részipiacot alkotnak. A fenti megoldások jellemzője, hogy egy nagyjából behatárolható és belátható igényhalmazt próbál meg kielégíteni, azt feltételezve, hogy a végső fogyasztó valami olyasmit vesz, amihez egyáltalán nem ért, nem is akar érteni, csupán használni szeretné. A kisvállalati szoftverek kevés kattintással elindítható, egyszerűsített felületű és minden esetben korlátozott funkcionálisú eszközök.

A középvállalatok igényei ezzel szemben jóval nehezebben megfoghatók. Egy nagyságrenddel több eszköz, három nagyságrenddel bonyolultabb rendszer, néhány jól képzett szakember – itt már nem működik a „fogd-és-vidd”. Ráadásul lehetséges, sőt a kisvállalatokhoz képest sokkal valószínűbb, hogy ezek a középvállalatok növekednek, s egyszer, talán nem is sokára, belépnek a tényleg nagy-

A vállalat mérete	Csináld magad (DIY)		Széles spektrumú IT ismeretekkel rendelkező szakértők			IT Specialisták
	A szervezemeltetés másodlagos feladat	A szervezemeltetés elsődleges, megosztott felelősség	1-2 teljes munkaidős „mindentudó” IT szakértő	5-10 teljes munkaidős „mindentudó” IT szakértő bizonyos szakmai fókuszokkal	Feladattípushoz rendelt szakmai specialista	
Otthoni hálók						
Kisvállalkozások						
Közepes nagyságú szervezetek						
Nagyvállalatok						
# Felhasználók	10	25	50	100	250	500

A szakemberek elvárt tudása a vállalatok méretének függvényében

vállalati kategóriába. A kisvállalati recept – „egyszerűt és korlátozottat” – nem működik – ezért nincs is komoly kínálat a gyártók részéről.

Az informatikus szabadsága

A hamarosan megjelenő System Center Essentials 2007 (SCE) a közepes nagyságú IT-rendszerrel bíró szervezeteket célozza meg: a konfigurációmenedzsment és az operációmenedzsment területén ígér segítséget. Ahogy a neve is mutatja, nem a „mindent bele”, hanem a „lényegét bele” jelmondattal kezdtek a fejlesztésébe. Mielőtt azonban bárki elhúzná a száját, hogy „már megint itt egy szoftver, amellyel korlátozzák a lehetőségeimet”, megfontolásra ajánlható a következő gondolatmenet. Minden valamirevaló informatikust – kezeljen bármilyen forrásból származó szoftvert – legalább négy dolog korlátoz. Középfölde IT-hőse rabja saját tudása korlátozottságának: bármennyit tudhat, de nem tudhat mindent. Rabja a képességei határának is: sok mindent elvégezhet, de nem tud mindent elvégezni. Már csak azért sem, mert rabja a határidőknek: törekedhet a tökéletes megoldásra, de fontosabb, hogy a határidők leteltével legyen valami, ami működik. Végezetül rabja a költségeknek is, mert nemcsak működni kell a megoldásnak, de csödbe sem viheti a költségviselőt.

Érleljük bölcsességgé a fentieket: ha akad egy olyan megoldás, amelyik nem követel őrrepülőgépvizsgát, s még rendszerei is a tudást; ha van olyan szoftver, amelynek segítségével valaki képes többet látni és több munkát elvégezni, talán még precízebben is; ha van olyan termék, amelyik segít betartani a határidőket anélkül, hogy az a minőség rovására menne, akkor az a lehető legtöbb szabadságot adja – mert éppen a valódi igényeket elégíti ki, vagy másképp: a valódi problémákat oldja meg. Nos, a System Center Essentials 2007 ezeknek az ígéreteknek a teljesülését hivatott szolgálni. A konkrét technológiai korlátok: a rendszer 20–30 (még nem eldöntött a szám) szerver felügyeletét és maximum 500 végfelhasználói eszközt (PC) képes menedzselni. Ha ennél több rendszerrel rendelkezünk, akkor egy második SCE megvásárlása segíthet rajtunk – vagy frissíthetünk a System Center család „nagyobb testvéreire”. Van még néhány olyan funkció, amelyet az SCE fejlesztésekor nem imple-

mentáltak a teljes megoldásokhoz képest, ezt mutatja a következő két táblázat:

Konfiguráció-kezelés	SC Configuration Manager 2007 (volt SMS)	SCE
Szoftverfrissítés	x	x
Szoftverterítés	x	x
Leltár (hardver/szoftver)	x (bővíthető)	x
OS-telepítés	x	
Mobilisközök (Windows Mobile stb.)	x	
Elvárt konfigurációmenedzsment	x	
NAP, WoL stb.	x	
Távoli telephely támogatása	x	x (egyszerű)

Monitorozás	SC Operation Manager 2007 (volt MOM)	SCE
Menedzsment-csomagok	x	x
Kiszolgálók, ügyfelek és szolgáltatások	x	x
Jelentések	x	x
Menedzsment-csomag-sablonok	x	x
Felhasználói szerepek	x	
Adattárház	x	
Connector keretrendszer	x	

Többnyire olyan funkciók hiányoznak, amelyeket csak nagyvállalatok használnak (adattárház, NAP – Network Access Protection), alacsonyabb prioritású feladat (mobilisközök konfigurációmenedzsmentje), vagy éppen a Windows rendszerben is létezik implementációja (OS-telepítés).

System Center Essentials 2007

Az informatikai rendszerüzemeltetés mint szakma, lassan kezd beérni és megállapodni. Ennek legfőbb jele, hogy terjedőben van a „közös nyelv” és módszertan, az ITIL, illetve annak derivátumai, mint például a Microsoft Operation Framework (MOF). Ezt a közös nyelvet beszéli a System Center rendszermenedzsment-szoftvercsalád is, azon belül pedig az SCE is. A MOF fogalmaival élve az SCE az első két negyedét támogatja.

Felsorolásszerűen az SCE funkciói:

- proaktív szerver- és kliensmonitorozás;
- tranzakció-elemzés végfelhasználói szem-

- hibadetektálás;
- hardver- és szoftverleltár-készítés;
- szoftvertelepítés;
- javítócsomagok telepítése;
- üzemeltetési és státuszriportok készítése;
- önmaga adminisztrálása (konfigurálás, menedzsmentcsomagok kezelése, összeállítás stb.).

A szoftver tervezésekor elsődleges szempont volt, hogy az üzemeltetők az SCE-t pilanatok alatt elsajátíthassák, és ne csak az SCE szakértői, hanem annak segítségével az üzemeltetés bajnokai lehessenek. A telepítés



A MOF üzemeltetési folyamatmodellje

csak tíz kattintás, s máris előtűnik a konzol. Mindent megtettek, hogy a lehető legegyszerűbb, intuitív felületet alkossák meg. Végül az Outlook 2003/7-ben, az ISA 2004/6-ban, illetve az Exchange 2007-ben egyaránt alkalmazott konzolelrendezést kapta az SCE is, ahol a bal alsó sarokban sorakoznak a legfontosabb feladatok (számítógépek, monitorozás, frissítések, szoftverterítés, menedzsmentcsomagok létrehozása, riportok és adminisztráció). Az egyes fő feladatcsoportokra kattintva gyors áttekintést kaphatunk a feladatcsoport végrehajtásának helyzetéről. A „teljes kép” mint igény más funkciókban is megjelenik: konfigurálható, hogy a rendszerüzemeltetők napi áttekintő e-mailt kapjanak a rendszer állapotról. A munkavégzést pedig olyan okos fejlesztések segítik, mint a hibadetektálásnál felajánlott, „a témához tartozó” diagnosztizáló eszközök. (Ezt a tudást egyébként a menedzsmentcsomagok hozzák magukkal.)

Szerver-, kliens- és eszközüzemeltetés

Konkrét üzemeltetési tudásban az SCE nem marad le a System Center Operation Manager 2007-től. Ez azért van így, mert

az SCOM 2007 lényegében egy keretrendszer – tudással a menedzsmentcsomagok töltik fel. Éppen így van az SCE esetén is: az SCOM 2007 alá fejlesztett csomagok vál-

WSUS nagy sikert aratott az üzemeltetők körében, és vélhetően a 3.0-ás verzió is kedvező fogadtatásra talál majd. Az SCE használói ezt a technológiát kapják meg a színtalpak mö-

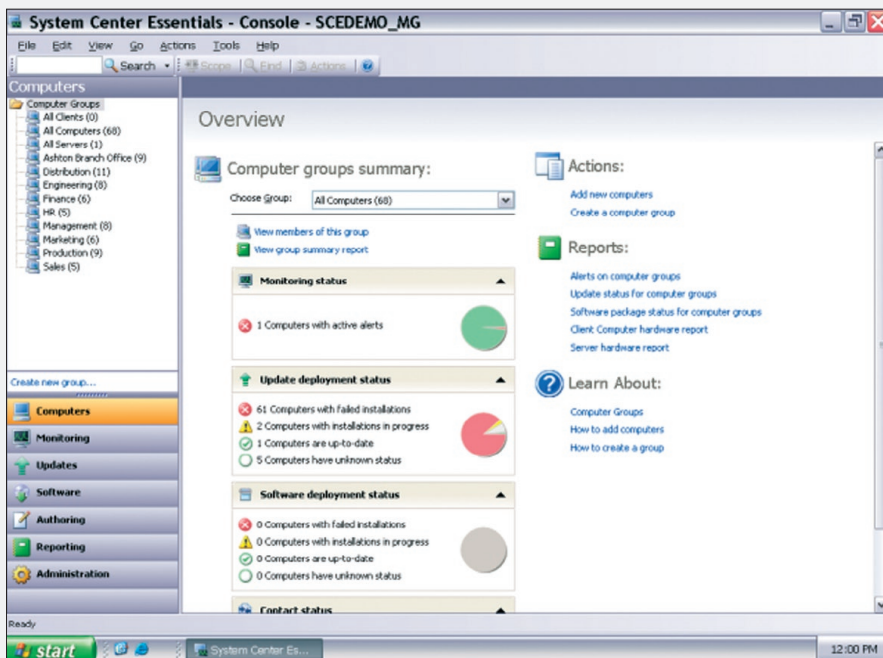
összegyűjtő – és ez már nagyon jó megközelítés a teljes képhez.

Jelentések készítése

Több mint ötven beépített jelentés használható azonnal, de ez tetszés szerint bővíthető. A legfontosabbak természetesen a rendszer rendelkezésre állását és működőképességét leíró riportok, de a napi összefoglalók és a kapacitástervezést lehetővé tevők is rendkívül hasznosak. A riportokat az SQL-szerver jelentéskészítő moduljával (Reporting Service) lehet előállítani, ami ismét csak a szabványosság és hordozhatóság záloga. Az, hogy lehet nyomtatni, levélben elküldeni és publikálni – magától értetődő képesség.

A felszín alatt

Ahogy az már felsejlett, a System Center Essentials valójában az Operations Manager 2007 és a WSUS 3.0, továbbá a Windows Server Active Directory szoftverterítési képességeinek összeforrasztása, testre szabása és kiegészítése. Mégsem egyszerű újracsomagolásról van szó, hiszen a WSUS önmagában nem tud szoftverdisztribúciót, a hardver- és szoftverleltár, illetve a harmadik gyártótól származó csomagok terítése pedig csak API-szinten létezik – ezeket a funkciókat már az SCE valósította meg. A két technológia krea-



A System Center Essentials áttekintő képernyője

toztatás nélkül használhatók az SCE alatt. Mindez hallatlan erőt ad az Essentialst használóknak: az SCOM-hoz illeszthető Cisco, 3Com, APC stb. készített menedzsmentcsomagokkal szinte nincs is olyan általánosan elterjedt mondható hardver- vagy szoftvertermék, amelynek a menedzsmentje ne lenne megoldott. Rendszerfelmérés és csomagimplementálás kérdése az egész. Végül még egy megnyugtató tény: az SCE és az SCOM ügyfélgépekre telepített komponensei teljesen azonosak.

Változáskezelés (szoftverterítés, frissítések)

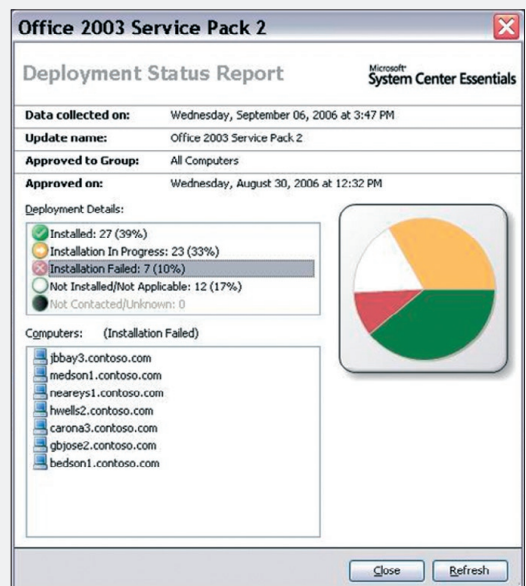
A változáskezelés témakörében érhető tetten a leginkább az SCE komplexitáselrejtési szándéka. A szoftverek terítéséhez teljes felületet nyújt ugyan, ugyanakkor érdemes tudni, hogy a háttérben a Active Directory ilyen irányú képességeivel, vagyis a csoport-házirendekkel operál. Szemben azonban az AD-vel, ahol mindenképpen szükségünk van MSI-csomagokra, itt exe-állományok is disztributálhatók, továbbá az MSI-kapcsolók beállítására is van módunk.

Hasonló a helyzet a frissítéseknél is. A

gött, de olyan fontos kiegészítésekhez jutnak hozzá, mint a harmadik gyártótól származó csomagok terítési lehetősége vagy éppen az eszközmeghajtók kiajánlása, vagyis bármit, amit SMS-sel (vagy hamarosan a System Center Configuration Manager 2007-tel) frissíteni lehet, azt megtehetjük az SCE-vel is. A terítés állapotáról a szoftver egy katintással (tényleg!) jelentést készít, diagrammal együtt.

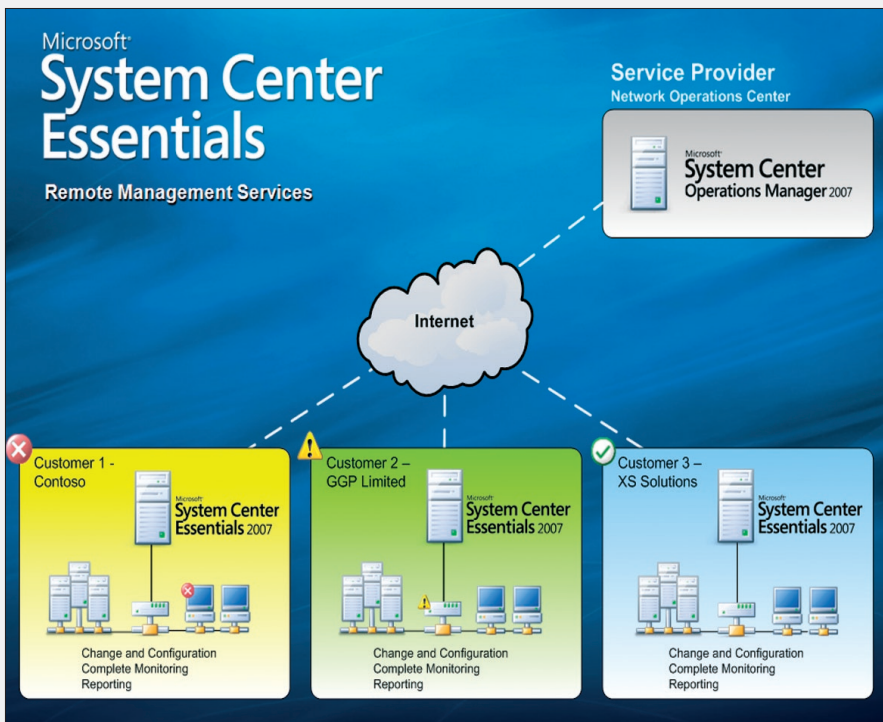
Hardver- és szoftverleltár

Harmincválhány hardvertulajdonoságot gyűjt az SCE, ami tűnhet ugyan kevésnek, de ha egyetlen mozdulattal naprakészen megmondhatjuk, hogy melyik gépben milyen processzor van és mennyi memória, akkor már minőségi ugrást hajtottunk végre a jelenlegi megoldásokhoz (többnyire nem naprakész Excel-táblákhoz) képest. A szoftverleltár hasonlóan lényegre törő: bitről bitre nem nyálazza át a merevlemezeket az SCE kliense, de a vezérlőpultban megtalálható telepített programok listáját



Hány gépen van már fent az Office 2003 SP2?

tív egymás mellé illesztését mutató ábrán jól látható, hogy a konzol, az üzleti logika, a tárolás és az ügynökök is kettős eredetűek, de



Így felügyelhetjük egy SCOM és több SCE segítségével más vállalatok, telephelyek infrastruktúráját

funkcióban kiegészítik egymást, és olyan jól együttműködnek, hogy akit nem érdekelnek a részletek, még csak nem is kell tudnia ezekről a nüanszokról.

Mi kell hozzá?

Az SCE egy „előre csomagolt” megoldás minden szükséges összetevővel – beleértve a telepítés előfeltételeit és az SQL Server 2005 Express-t is. Ha valaki inkább preferálja a külön adatbázis-kezelőt, annak sincs semmi akadálya, használható az „igazi” SQL Server 2005 is. Fürtözni nem lehet az SCE-t, de mind a konzol, mind pedig az adatbázis telepíthető más gépre. Az alatta futó operációs rendszer Windows Server 2003 SP1 vagy annál újabb lehet.

Menedzselni kliensként a Windows 2000 Professional SP4 vagy annál újabb, kiszolgálóként pedig Windows 2000 Server SP4 vagy annál újabb operációs rendszer jöhet számításba. A menedzsmentcsomagok (MP) segítségével azonban elvileg bármilyen eszközt – amelyhez írtak MP-t – lehet majd menedzselni, beleértve a hálózati eszközöket vagy a szünetmentes áramforrásokat.

Frissítés és továbbugrás

A belső architektúrát megértve már látható is, hogy mely termékekről frissíthetünk SCE-

re. Természetesen a MOM 2005 Workgroup Edition ezek közé tartozik, ahogy ide sorolható a WSUS 2.0 és a 3.0 is.

a lehető legkisebb szolgáltatás kiesést szenvedjük el. A továbblépés a nagy testvérek – a System Center Operation Manager 2007, illetve a hamarosan megjelenő System Center Configuration Manager 2007 (SCCM) – felé lehetséges.

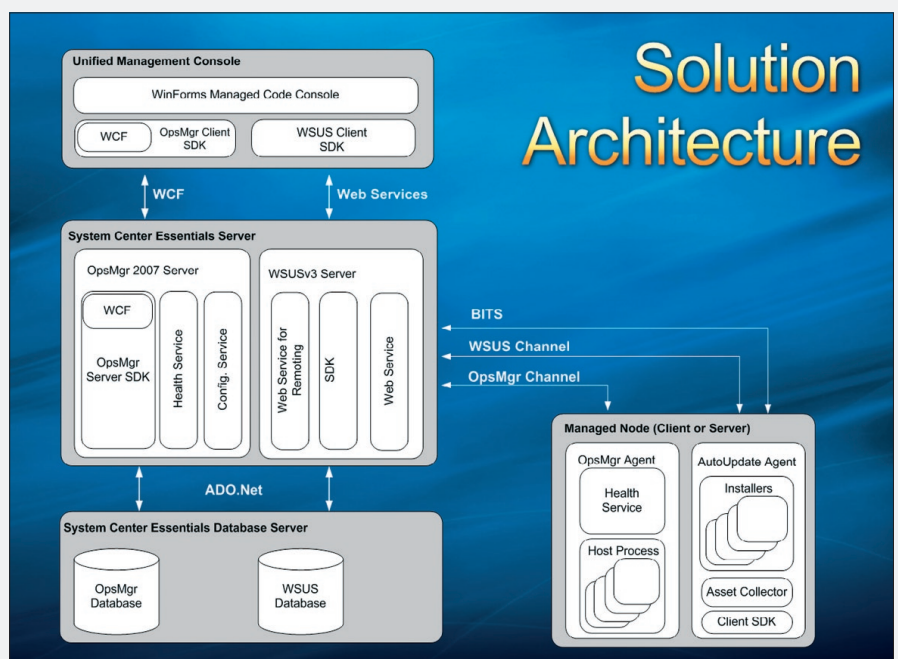
A migrációt lényegesen megkönnyíti, hogy az SCCM éppen azt a WSUS-infrastruktúrát használja, mint a System Center Essentials – vagyis a dolog „családon belül” marad.

Nem csak kicsiknek

Végezetül említsük meg, hogy az SCE remekül működik az SCOM kiegészítéseként is, outsource-környezetben.

Ebben az esetben a „nagy” outsource-szolgáltatást biztosító vállalat központjában egy Operation Manager 2007 működik, ügyfeleinél pedig egy-egy SCE. A System Center-család fel van készítve a WS-menedzsmentre, tehát egyáltalán nem jelent gondot átengedni a szükséges kapcsolatokat a tűzfalakon, a szükséges riasztások és jelentések a központban összefuthatnak.

Talán bátran állítható: informatikai Középfölde IT-hősei jó fegyvert kapnak, hogy a küldetésüket elvégezzék, és a rájuk bízott



A System Center Essentials belső felépítése

A fejlesztők ígérete szerint, amennyiben a migráció a MOM 2005 WE-ről történik, akkor a két rendszer egymás mellett is működhet, hogy a kritikus monitorozási feladatok

rendszereket kisebb erőfeszítéssel is jobban üzemeltethessék.

Lepénye Tamás
(tamasl@microsoft.com) Microsoft Magyarország

MOF: A SZOLGÁLTATÁS- ORIENTÁLT ÜZEMELTETÉS ALAPJAI

Hogyan tekintünk folyamatorientált szemlélettel saját IT-üzemeltetésünkre, és hogyan váljunk jó informatikai szolgáltatóvá?

A mai kiélezett versenyhelyzetben nő az igény a „jó IT-szolgáltatás” iránt. A szolgáltatással szemben egyre többet vár el az üzleti oldal (mint megrendelő), és egyre magasabb szinten kell szolgálatni az üzemeltető csapatnak (mint kiszolgálónak) ahhoz, hogy a megnövekedett elvárásoknak maradéktalanul eleget tegyenek.

Melyek is ezek az elvárások? Üzleti oldalról a nagy megbízhatóságú, hatékony, kiszámítható, stabil IT-háttérre van egyre inkább növekvő igény, valamint arra, hogy a rendszer rugalmasan tudjon reagálni a felmerülő új igényekre. Az „IT mint szolgáltatás” minőségét első kézből tapasztalják meg a felhasználók, érzik előnyét a hatékony üzemeltetésnek, vagy éppen szenvedik hátrányát a kidolgozatlan, folyamatokkal meg nem támogatott, napi események vezérelte üzemvitelnek. Az „IT-oldal” szolgáltatásai révén egyre inkább stratégiai szerepet tölt be az „üzlet” életében azzal együtt, hogy az üzemeltetendő rendszerek egyre komplexebbek, és egyre magasabbak a velük szemben támasztott követelmények.

Egyre kevesebb idő áll a szolgáltató rendelkezésére egy rendszerbeli változtatás megfelelő végigvezetésére, valamint egy meghibásodást követő visszaállásra. Az üzleti szervezetek egyre jobban függenek az informatikai szolgáltatásoktól. Ahány újabb területen lép elő az IT nyújtotta szolgáltatás – hogy elősegítse az üzleti folyamatokat –, annyi újabb lehetőséget teremt arra, hogy szolgáltatáskiesés esetén hátráltassa azokat.

A szolgáltatás eredményessége alapvetően a következő három összetevő függvénye: technológia, eljárások, emberek. A technológiai és az emberi tényezők taglalása kívül esik e cikk keretein, a továbbiakban az eljárások feltérképezésére helyezzük a hangsúlyt.

Hogyan tudhatunk megfelelni a növekvő elvárásoknak? Úgy, ha strukturált folyamatokkal tesszük átláthatóbbá és egyszerűbben kezelhetővé rendszereinket, valamint ha egyre több rész-folyamatot automatizálunk kézi végrehajtás helyett. Ebben nyújtanak számunkra nagy segítség az üzemeltetési módszertanok, mint például az ITIL (Information Technology Information Library) és a MOF (Microsoft Operation Framework).

Mi az a MOF? A MOF az ITIL-t vette kiindulási alapul, majd kiegészítette a platformfüggetlen irányelveket konkrét, technológiaorientált folyamatokkal és termékspecifikus üzemeltetési útmutatókkal. Az ITIL módszertana egy olyan folyamatorientált, minőségbiztosított IT-szolgáltatáskezelést céloz meg, amely bevált gyakorlatokat és ajánlásokat alapul véve koncentrálna az ügyfeleknek nyújtott szolgáltatás minőségének biztosítására. A MOF megalkotásakor szem előtt tartott elképzelés az volt, hogy egy átfogó üzemeltetési útmutatás elkészítésével segítsen a

rendszerüzemeltetőknek nagy megbízhatóságot, rendelkezésre állást és jó kezelhetőséget elérni a Microsoft platformon futó, üzletileg kritikus rendszereiken.

Az alapvető tervezési elvek között szerepel a már bizonyított, bevált módszerek alkalmazása; a széles körben felhasználható üzemeltetési szaktudás biztosítása; valamint ezek földrajzi, ipari és kulturális határoktól független alkalmazhatósága. Mindehhez nagy segítséget adott a Microsoft partnereinek, ügyfeleinek, konzulenseinek, fejlesztőinek üzemeltetési jártassága. Továbbá, mivel a Microsoft, amely nagyvállalként maga is saját informatikai rendszerrel rendelkezik, szintén értékes tapasztalatokat halmozott fel annak üzemeltetésével kapcsolatban.

Hogyan néz ki egy IT-szolgáltatás életciklusa a MOF folyamatmodell alapján?

A MOF nagyon alaposan dokumentált módszertan, gyakorlatilag minden folyamata a legutolsó részletig le van írva, és ez teljesen ingyenesen el is érhető a Microsoft weboldalaról: www.microsoft.com/mof.

Maga a MOF három fő részből áll: a folyamat, a csoport- és a kockázatkezelési modellből – ezeken keresztül éri el céljait, vagyis segíti a rendszer üzemeltetését.

A MOF legnagyobb és leghangúlyosabb

része a folyamatmodell, amely egy, a változáskezelés során az éles környezetbe bevezetett komponens életciklusát hivatott végigkísérni (1. ábra). Az életciklus folytonosságát az ábrán körbefutó nyílak szemléltetik egy szolgáltatás mint üzemeltetési munkaegység szempontjából. A körfolyamatot négy negyedre osztja a modell: a változáskezelési, az üzemeltetési, a támogatási és az optimalizálási szakaszokra. Minden szakasz végén található egy-egy mérföldkő, felülvizsgálati pont (OMR

környezetbe, méghozzá minimális szolgáltatás kiesés mellett. Részfolyamatai (SMF) és teendői:

A változások kezelése (Change Management). Új hardver- vagy szoftvereszközök, új üzemeltetési eljárások, megváltozott szervezeti felállítás, valamint a felelősségi körök módosulása tartozik ide.

A változásbevezetés vagy „kiadáskezelés” folyamata (Release Management). Tervezés, fejlesztés, tesztelés, megvalósítás.

ügyeleti modellben (központi, távoli, elosztott, delegált adminisztráció).

Biztonságfelügyelet (Security Administration). A nagyvállalati adatok bizalmas kezelésének, megfelelő szintű hozzáféréseinek és sértetlenségének biztosítása, valamint a fizikai és szellemi termékek védelme. Jogszulatlan hozzáférések észlelése, megelőzése.

Szolgáltatásfelügyelet (Service Monitoring and Control). Az üzemeltetett szolgáltatás „egészségének” folyamatos, valamint megelőző jellegű megfigyelése a szolgáltatási szint biztosítása érdekében.

Feladatütemezés (Job Scheduling). Az IT-infrastruktúrát érő terhelések egyenletessé tétele, bizonyos műveletek ütemezése, valamint automatizálható folyamatok köteget végrehajtása.

Hálózatadminisztráció (Network Administration). Megfelelő szintű hálózati rendelkezésre állás és teljesítmény biztosítása, hálózati eszközök konfigurációkezelése és protokollmenedzsment (OSI 1–4).

Címtárfelügyelet (Directory Service Administration). Címtár-információk központi elérhetőségének biztosítása, valamint adatkonzisztencia elősegítése különböző címtár-típusok és címtáralkalmazások között.

Tároláskezelés (Storage Management). Biztonságos adattárolás megoldása a legkülönbözőbb adathordozókra vonatkozóan, mentés és visszatöltés biztosítása, valamint nyomtatott és elektronikusan tárolt dokumentumok kezelése.



1. ábra. A MOF folyamatmodell

– Operations Management Review), amely tulajdonképpen az adott negyedben végzett tevékenységek értékelése. Minden negyednek van egy egyedi, elsődleges célja a szolgáltatás szempontjából. Ezekben a negyedekben találhatóak továbbá az elsődleges célt alátámasztó folyamatok (SMF – Service Management Function), amelyekből összesen 21 darab létezik, és 11 közvetlenül az ITIL-ből származik.

Változáskezelési, változtatási szakasz – Changing quadrant

Legfontosabb feladata a jóváhagyott változtatási igények hatékony bevezetése az éles

Konfigurációfelügyelet (Configuration Management). A változások dokumentálása, a konfiguráció nyomonkövetése, konfigurációs adatbázis (CMDB).

Üzemeltetési szakasz – Operating quadrant

Elsődleges feladata a hatékony IT-szolgáltatáshoz szükséges napi (előre meghatározott) üzemeltetési feladatok és tevékenységek végrehajtása és felügyelete. Részfolyamatai (SMF) és teendői:

Rendszerfelügyelet (System Administration). Napi adminisztratív teendők, eljárások végrehajtása az üzemeltetésre jellemző fel-

Támogatási szakasz – Supporting quadrant

A cél ebben a szakaszban a problémák, hibák, incidensek, kérések megoldása a szolgáltatás szint szerint megkövetelt időkorlátokon belül. Részfolyamatai (SMF) és teendői:

Ügyfélszolgálat (Service Desk). Központosított hozzáférést nyújt az IT-szolgáltatásokkal kapcsolatban, ahová a felhasználók fordulhatnak kéréseikkel. Ügyfélkapcsolat kezelése. Az „informatika arca” az IT-n kívüli világ nagy része számára.

Incidenskezelés (Incident Management). Feladata a szolgáltatási szint haladéktalan visszaállítása a megfelelő mértékűre, minimális negatív üzleti kihatással. Tudásbázis felhasználása, kerülő megoldások alkalmazása, ha szükséges. Eszkálációkezelés.

Problémakezelés (Problem Manage-

ment). Az incidens vagy probléma mögött meghúzódó valódi hibák beazonosítása, a hiba elhárítása.

Optimalizálási szakasz – Optimizing quadrant

Legfontosabb feladata a meglévő szolgáltatási szint megtartása vagy javítása mellett költségcsökkentés elérése, erőforrás-optimalizálás. Részfolyamatai (SMF) és teendői:

Szolgáltatásszint-felügyelet (Service Level Management). A szolgáltatás jobbá tétele azáltal, hogy rögzítik az egyeztetett szolgáltatási szinteket (SLA). Az IT és az üzleti oldal kapcsolatának formálása.

Anyagi erőforrások kezelése (Financial Management). A monetáris erőforrások belső kezelése a támogató szervezet hosszú távú céljai érdekében. Költségvetés-készítés, szolgáltatáshasználat alapú számlázás, üzemeltetési befektetések irányítása, felügyelete.

A szolgáltatás folytonosságának kezelése (Service Continuity Management). Katasztrófa vagy váratlan szolgáltatáskiesési események során történő továbbszolgáltatás biztosítása, lépéseinek megtervezése a kockázati faktorok figyelembevételével.

Rendelkezésre állás kezelése (Availability Management). A magas rendelkezésre állás biztosítása mellett minimalizálni a szolgáltatáskiesést. A szolgáltatás-szint-megállapodás szerinti leállási idők vizsgálata.

Kapacitáskezelés (Capacity Management). Előrelátó módon kezelni a várható kapacitásváltozással kapcsolatos igényeket. Üzemeltetési trendek figyelése a szolgáltatási szint biztosításához.

A munkaerő-ellátás kezelése (Workforce Management). A megfelelő szakértelmű és jártasságú szakemberek felvétele, továbbképzése és megtartásának biztosítása. Kompetenciakezelés.

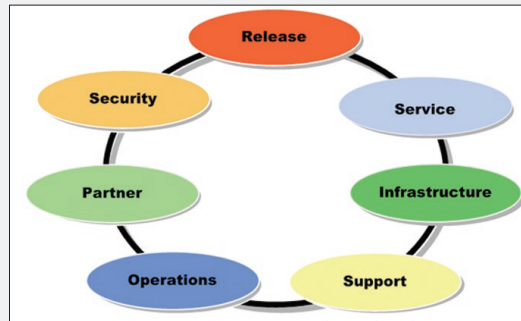
Biztonságkezelés (Security Management). Biztonsági házirendek, szabályozások, tervek készítése és kommunikációja a szervezetben.

Infrastruktúraoptimalizálás (Infrastructure Engineering). Infrastruktúrafejlesztések koordinálása. Annak biztosítása, hogy a technológiai lehetőségek egybeessenek az üzleti igényekkel.

A folyamatmodell minél hatékonyabb megvalósítása érdekében van szükségünk a csoportmodellre (2. ábra).

Csoportmodell

A MOF speciálisan kialakított szerepköröket alkalmaz, hogy enyhítse a szervezeten belül a feszültséget – az informatikai üzemeltetésnek ugyanis nemegyszer ellentétes céloknak kell megfelelnie. Egyszerűbbé és közérthetővé teszi a „ki mit csinál” kérdésre adott választ az üzemeltető-szolgáltató szervezetben. Kipróbált modellen alapszik, hét jól elkü-



2. ábra. Csoportmodell

löníthető szerep jelenik meg benne. Célja a kulcsfontosságú felelősségi körök tisztázása és az egyes szerepkörökhez szükséges szakértelem meghatározása. Segít az embereknek szerepük világosabb megértésében, ezáltal elősegítve a szervezet közös céljainak elérését, és érthetőbbé téve az üzleti prioritásokat. Minden egyes szerepkörnek megvan a saját elsődleges célja (quality goal). A szerepkörökről és az egyes, lebontott feladatokról is részletes leírás található meg a MOF dokumentációjában, amelyek akár feladatlistaként vagy munkaköri leírásként is használhatók az informatikával kapcsolatban álló kollégák számára.

Szolgáltatásbevezetés. A hatékony változáskezelés és szolgáltatásbevezetés elősegítése. Minden IT-szolgáltatás és -rendszer konfigurációjának pontos készletnyilvántartása.

Szolgáltatás. Az üzlet érdekeit szem előtt tartó IT-kiszolgálás biztosítása.

Infrastruktúra. A fizikai IT-környezet és az infrastruktúraeszközök felügyelete.

Támogatás. Kiemelkedő ügyféltámogatás és szolgáltatáskultúra elősegítése.

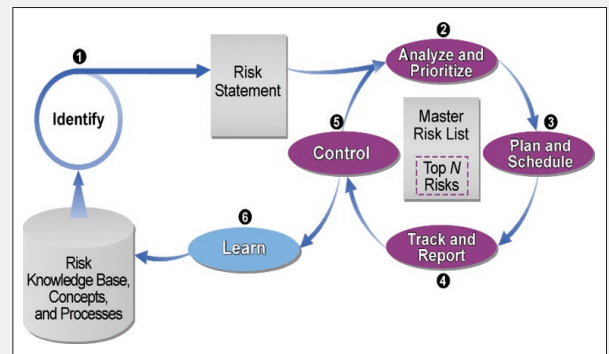
Üzemeltetés. Megismételhető, kiszámítható és automatizálható rendszermenedzsment.

Partner. Kölcsönösen előnyös kapcsolatok kialakítása a szolgáltató és ellátó partnerekkel.

Biztonság. A nagyvállalat értékeinek védelme, ellenőrzött hozzáférés-engedélyezési folyamatok, megelőző célú biztonsági tervek.

Miért célszerű alkalmazni a kockázatkezelés tudományát?

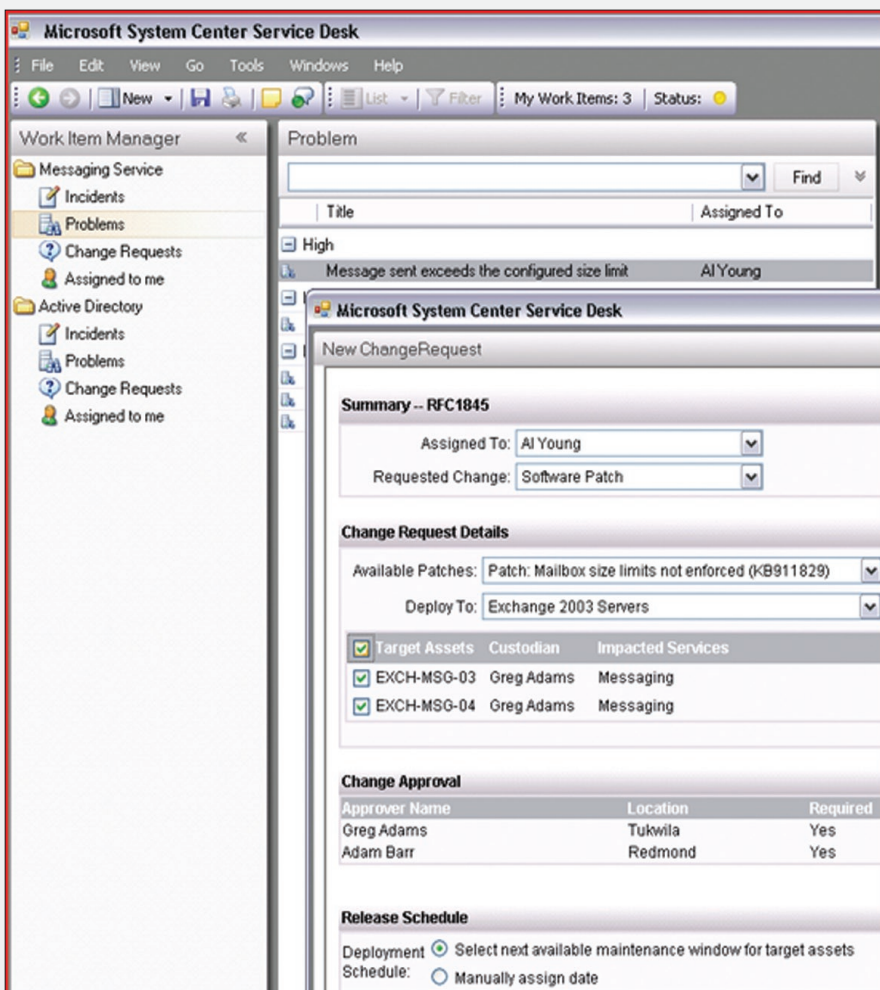
A kockázat egy bizonyos valószínűséggel ($0 < \text{valószínűség} < 1$) bekövetkező, veszteséget okozó eseményt jelent. A biztosan bekövetkező esemény már nem kockázat. A veszteség értelmezése itt viszonylagos, jelentheti akár egy várható nyereség lehetőségének elvesztését is. A kockázat kezelése pedig a kárenyhítés, kockázatmentesítés, kockázatalterülés vagy épp -elfogadás lépéseinek folyamata. A kockázatkezelés fontosságát támasztja alá, hogy az üzleti tranzakciók növekvő módon függenek az IT-től, továbbá a kiszolgáló rendszerek bonyolultabbá váltak. Ennek eredményeként minden hiba fokozottabban kihatással van az üzleti folyamatokra a nagyobb potenciális kihatása és a gyorsabb észlelhetősége miatt.



3. ábra. Kockázati modell

Minden egyes új terület, ahol üzleti folyamatokat támaszt alá az IT-szolgáltatás, egy újabb „lehetőség” arra, hogy szolgáltatáskimaradás esetén teljesen megbénítsa azt!

Kockázati forrásaink a négy alapvető területről eredhetnek: emberek, folyamatok, technológia, valamint környezeti behatások. Ezek szintén négy különböző módon tudnak veszélyes üzleti kihatást eredményezni: teljesítmény, biztonság, rugalmasság és költségességi vonatkozásokban.



4. ábra. Hogyan segítsük elő a MOF folyamatmodell bevezetését?

A MOF hat lépésben közelíti meg a kockázatkezelés alapjait (3. ábra).

- A kockázatos szolgáltatási terület beazonosítása.
- A beazonosított kockázatok kiértékelése és fontosság szerinti besorolása.
- A kockázat elkerülésének megtervezése, bekövetkezésének észlelése, válaszreakciók tervezése.
- A kockázatosnak ítélt folyamat és a megelőzési terv hatékonyságának nyomon követése.
- A kockázat ellenőrzése. Működtek-e a tervek? Változott-e a valószínűség? Változtasuk-e a terveket?
- Vonjuk le a tanulságokat a folyamatkezelésben elért eredményeink szerint.

Mi tekintünk szolgáltatásnak?

Mi az SLA és a szolgáltatástérkép? Az IT-szolgáltatás meghatározását mindig az azt igénybe vevő fél, vagyis az üzleti oldal szemszögé-

ből közelítjük meg, egy egységként tekintve a folyamatra. A jó szolgáltatás hatékony, megbízható és olyan feladatot lát el, ami az üz-

További információ

MOF: <http://www.microsoft.com/mof>
 Tanfolyam: <http://www.microsoft.com/learning/syllabi/en-us/1737bfinal.aspx>
 CIR: <http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/index.aspx>
 Self-Assessment Tool 2.0: <http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/moftool.aspx>
 ITIL: <http://www.itsmf.hu/>
 SCSD: <http://www.microsoft.com/systemcenter/sd/default.aspx>

leti oldal számára funkcionális értékkel bír. Az igényelt szolgáltatásokat szolgáltatáskatalógusban rögzíti az IT, és fontossági sorrend

alapján határozza meg az üzleti oldallal egyeztetett szolgáltatási szintet (SLA – Service Level Agreement). A szolgáltatási szint meghatározása kétoldalú, iteratív folyamat az IT és az üzlet között, ahol a szolgáltatás egyes paramétereinek szintjét igazítjuk az üzleti oldal elvárásaihoz a rendelkezésre álló erőforrások függvényében, a „piaci egyensúly” megtalálására törekedve.

Az üzleti és az IT-szolgáltatás kapcsolatát a szolgáltatási szint rögzítésével tudjuk a leghatékonyabban formalizálni. Az ilyen folyamatokat egyenként meg kell jeleníteni egy úgynevezett szolgáltatástérképben. Ez a térkép minden fontos ki- és bemenő információt tartalmaz a szolgáltatással kapcsolatban, és választ ad azokra a kérdésekre, amelyeket a szolgáltatónak folyamatosan szem előtt kell tartania a minőség biztosítása érdekében. Ilyenek például: a szereplő hardver- és szoftverkomponensek; a függőségben lévő más szolgáltatások; kik a szolgáltatás igénybe vevői; ki a szolgáltatás vagy szolgáltatáslánc mint folyamat tulajdonosa; kik a szolgáltatás támogatói; milyen feltételek mellett szabad változtatni a rendszeren; mekkora rendelkezésre állást várnak el tőle; mi a terv katasztrófaeseményre stb. Fontos, hogy a szolgáltatás szint-kezelés során csak azokat a jellemzőket vegyük bele az egyezésbe (SLA), amelyeknek az értékét folyamatosan tudjuk mérni.

A System Center családjába tartozó „Service Desk” képes lesz arra, hogy a MOF alapú munkafolyamatok legfontosabb összetevőit automatizmusokkal támogassa, és átláthatóbbá, könnyebben kezelhetővé tegye napi szinten a folyamatokat az üzemeltetés számára. A termék jelenleg bétafázisban van. A System Center „Service Desk” első bétája által megvalósított folyamatok közé tartozik az incidenskezelés, a problémakezelés, a változáskezelés, a konfigurációkezelés, valamint a konfigurációs adatbázis (CMDB). Az incidenskezelést integrálni tudjuk a MOM-ból jövő riasztásokkal, a konfigurációs adatainknak pedig részei lesznek az SMS-ből jövő leltárinformációk. A változtatáskérés folyamat elindítása után egy Outlook-szerű kliens segítségével halad végig a jóváhagyás folyamatán. Nagy érdeklődéssel várjuk, hogy kipróbálhassuk a terméket.

Kurucz György
 (gyorgyk@microsoft.com) Microsoft Magyarország
 ITIL Service manager, MOF trainer, MCSE, MCT

KÉZBEN TARTOTT NAPLÓK

Biztonsági audit a System Center Operations Manager 2007-ben.

Dörgelemes álkirohanást intézett a biztonsági alkalmazások által generált naplóállományok halmozói ellen Marcus Ranum információbiztonsági guru, „a tűzfalak atyja”, egy 2005 nyarán elhangzott előadásában. Közölte, hogy a „logok” tökéletesen hasznatlanok, mindenki jobban járna, ha egyszerűen törölné őket. Szavait természetesen nem szó szerint kell érteni, hanem éppen ellenkezőleg: a szervezeteknek jobban kellene élniük (élniük kellene!) a biztonsági rendszereik által szolgáltatott információkkal.

Naplógondok

Naplóállományokkal jócskán el vagyunk látva. Ontják őket az alkalmazások, az operációs rendszerek és a biztonsági eszközök. Fontos adatokat hordoznak az állományok és könyvtárak eléréseiről vagy elérési próbálkozásairól, az Active Directory objektumairól, a szabály- és jogosultságváltozásokról, a jogosultságok használatáról – a legegyszerűbb esetben egy közös bejelentkezéstről – és még sok másról.

A logok azonban nem egyszerűen csak keletkezhetnek, hanem legszívesebben osztódással szaporodnának. Egy helyileg tárolt állományban csak korlátozott számú eseménymennyiségre vonatkozó információ fér el, ez pedig aligha felel meg a védelmi igényeknek és a törvényi előírásoknak. A helyi naplók további problémája, hogy csak annyira hitelesek, amennyire megbízható a hozzájuk férő lokális adminisztrátor. Ha véletlenül vagy szándékosan rossz fát tesz a tűzre, elég törölnie a naplókat, és már el is tűntette garázdálkodásának a nyomait. A szervezetek több operátora által használt, de komoly ellenőrzési lehetőséget biztosító „privilegizált” hozzáférésekkel részben hasonló, részben még komolyabb gondok is akadnak.

A mennyiséggel más bajok is vannak: nehéz a naplók elemzése, ha pedig sok számítógép

sok naplót generál, azokat először is be kell gyűjteni (ez sem könnyű), hogy aztán a sok naplónak még nehezebb legyen az elemzése (emberi mértékkel jószerével lehetetlen). Következésképpen a lekérdezéssel, az adatok értelmezésével és prezentálásával, továbbá az „élő”, valós idejű monitorozással is gondok vannak.

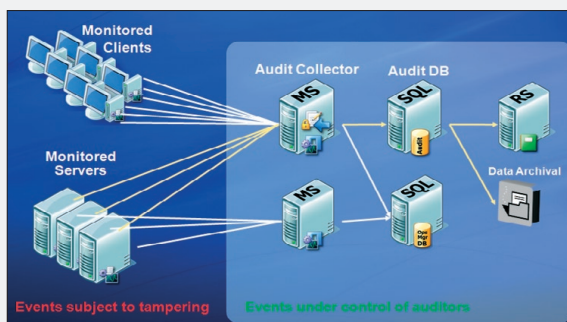
Márpedig az ellenőrzés – akár saját, szervezetben belüli „házi” vizsgálat, akár megfelelőségi audit – problémáját meg kell oldani, mert a biztonsági naplók több okból is fontosak:

- a rendszer változásainak monitorozása;
- a jogosultságok használatának monitorozása;
- biztonsági fenyegetésekre (behatolás, vírusok) utaló aktivitások és forgalmi adatok érzékelése;
- a rendszer erőforrásaival való visszaélés vagy ilyen próbálkozásra utaló jelek detektálása;
- incidensek után a naplók információinak később is előkereshetőnek és értelmezhetőnek, sőt, bizonyítékértékeknek kell lenniük egy esetleges nyomozás vagy jogi eljárás során;
- az egyik legfontosabb szempont: a biztonsági naplók vizsgálatát, kezelését és felhasználását törvények szabályozzák, és mese nincs, ezeknek bizony jó néhány vállalatnál meg kell felelni.

MACS-ból ACS

A fenti problémák nem új keletűek. Az ügyfelek igényei miatt néhány éve a Microsoft is belekezdett egy fejlesztésbe, amelynek az eredménye a MACS (Microsoft Audit Collection Services) próbaváltozata volt. A béta jól végezte a dolgát, de költségek közben megjött a felhasználók étvágya, és felmerült az igény: jó lenne, ha valahogyan hozzá lehetne illeszteni a Microsoft Operations Managerhez (MOM). A 2005-ös változat esetében erre már nem került sor, de a System Center Operations Manager 2007-et (SCOM) már úgy fejlesztették, hogy szerves komponensként – azaz nem kell külön megvásárolni – tartalmazza az utódját: az ACS rövidítéssel aposztrofált Audit Collection Servicest.

Az ACS egy olyan új funkció az SCOM-ban a MOM-hoz képest, amely begyűjti a felügyelt számítógépek eseménynaplóit, és azokat egy központi adatbázisban konszolidálja.



Az SCOM 2007 Audit Collection megoldása

Az adatok segítségével bármikor, bármilyen lekérdezés elvégezhető, követhetők a felhasználói akciók, továbbá elkészíthetők a biztonsági trendekre és változásokra vonatkozó elemzések.

foglalnak, és gyorsabban hozzáférhetőek, feldolgozhatóak;

- nyomozati vagy jogi procedúra esetén nem okoz gondot a bizonyítékgyűjtés.

A mostani információk szerint az ACS ki-

már most támogatják, valamint természetesen a Longhorn platform bétái és majdani végleges változatai is. Maguk az ágensek független jóságok, mert amint érzékelik a biztonsági napló új eseményét, abban a pillanatban lecsapnak rá, és már el is küldik a kollektoroknak – emiatt nevezik őket forwardereknek (továbbítóknak) is. Ez a mozzanat kiküszöböli a de facto megbízhatatlannak tekintett helyi és privilegizált operátorok beavatkozásának lehetőségét, mert a valós időben begyűjtött, majd a kollektoron tárolt adatokhoz ők már nem férnek hozzá. A kollektor megbízhatóságáról persze gondoskodni kell – meg arról is, hogy a lokális admin ne lehessen le a forwardert.

Néhány gyakorlati tanács

Az ACS-ágenseket a telepítőmédián ADTAGENT_X86.MSI állományával telepíthetjük.

Alternatív továbbítás beállítása a forwardereknek:

- telepítsük az ACS-ágenst;
- a DNS SRV bejegyzését konfiguráljuk az „_adtsrv” név- és az 51909-es portbeállításokkal;
- a forwarderek menedzselésére használjuk az Adtagent.adm csoportházi rend sablont.

Az ACS felügyeletére a telepítő „ACS” könyvtárban található ADTADMIN.EXE használatos.

Microsoft-ajánlások a kollektor finomhangolásához. Ez a rendszerleíró adatbázis HKLM\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters szakaszának négy bejegyzésével lehetséges:

- **MaximumQueueLength:** az adatbázisra várakozás közben a memóriában (erre a várakozó pufferre a továbbiakban [1] jellel hivatkozunk) tárolható események száma – akkora legyen, hogy a telítettség a BackOffTresholdban (alább) százalékban megadott érték alatt maradjon.
- **BackOffTreshold:** százalékban adja meg, hogy [1] milyen telítettsége felett ne fogadjon új kapcsolatot az ACS – ajánlás: 80%.
- **DisconnectTreshold:** az ACS [1] milyen százalékos telítettsége felett bontsa a forwarderektől bejövő, már felépült kapcsolatokat.
- **MaxPurgingQueue:** ha [1] ennél a százalékos értéknél nagyobb arányban telített, akkor nem üríthető.

Javasolt a következők betartása:

- $MaxPurgingQueue < BackOffTreshold < DisconnectTreshold$.
- Nem kívánatos a BackOffTresholdnak megfelelő telítettség elérése. Ilyenkor vagy az ACS-kiszolgáló I/O teljesítményét kell növelni, vagy csökkenteni kell az ennek a kollektornak jelentő forwarderek számát.
- A MaximumQueueLength és a MaxPurgingQueue egy egységnek tekintendő.
- Ugyanígy a BackOffTreshold és a DisconnectTreshold is; ennek megfelelően értékeiket együttesen kell állítani.

Telesítménymonitorozás. A kollektor teljesítménymonitorának két számlálókészletével lehetséges:

- az „ACS Collector” magának a kollektornak;
- az „ACS Collector Client” a forwardereknek a felügyeletére alkalmas. Minden forwarder saját számlálót kap. Száznál több forwarder esetén külön kell beállítani, hogy melyek a legfontosabb megjelenítendő számlálók.

Az ACS főbb tulajdonságai:

- eleget tesz a megfelelőségi kívánalmaknak – pontosabban a törvényeknek, például a nemzetközi etalonra vált Sarbanes–Oxleynek és a nálunk az ennek mintájára kialakított előírásoknak;
- támogatja a belső vizsgálatot és a külső auditot;
- kielégíti a közepes és nagyméretű szervezetek igényeit;
- az SQL Server 2005 segítségével központi módon tárolja a biztonsági események paramétereit;
- a konsolidált és normalizált tárolás miatt könnyen lehet áttekinthető beszámolókat készíteni;
- a normalizált adatstruktúra miatt a naplóinformációk lényegesen kevesebb helyet

zárólag az SCOM része, és nem lesz belőle olyan önálló termék, amilyen az egykori elgondolások szerint a MACS lett volna.

Ügynökrendszer

Az ACS rendszerben a monitorozott gépeken futó ágensek egy eseménygyűjtőhöz, a „kollektorhoz” továbbítják a biztonsági események adatait. A kollektor olyan szerverkomponens, amely figyel az ACS-forgalomra, és közvetlenül kapcsolódik az ACS-adatbázisához. Utóbbi nem titkosítva tárolja az adatokat, de a hozzáféréseket alaposan kell beállítani – mint ahogyan azokat a jogosultságokat is, hogy kik és milyen lekérdezéseket, elemzéseket futtathatnak az adatokon.

Az SCOM-ágenseket a Windows XP Pro, Server 2000 és 2003, illetve Vista rendszerek

Forgalmi megfontolások

Alapértelmezésben nem minden esemény információt gyűjtik be, hiszen így pocskék jelzaj arányt lehetne produkálni. A Microsoft összeállított egy sémát a továbbítandó eseményekről, amelyet frissítő- és szervizcsomagokkal folyamatosan aktualizál majd. A hálózat forgalmi viszonyait már az eseményszűrés is javítja, de a további optimalizálás érdekében az ágensek csak a legszükségesebb információkat továbbítják – az esemény ideje, néhány azonosító és egyedi jelzés –, az általános leírásokat pedig nem; ezeket a kollektor regenerálja a kapott adatokból.

Próbamérések alapján egy átlagos biztonsági esemény normalizált formában 140 bajtnyi adatot tartalmaz, és ez kisebb még az SCOM más üzeneteinek átlagos méreténél is. A hálózati forgalmat a monitorozott eszköz típusa is befolyásolja, ezért jellegtől függően változó lehet a mértéke. Tipikusan a tartományvezérlők a legnagyobb forgalmazók, de adott esetben egy erőteljesen használt fájlszerver nagyobb „nyüzsgést” produkálhat.

Az adatforgalom titkosított, de a kollektoron dekódolt adatok már nem. Ugyanígy nem kódolt az SQL-adatbázis, de fel lehet köré állítani a hagyományos biztonsági korlátokat – ajánlott is, hogy ezekhez az adatokhoz csak az ACS struktúrájának legyen írási, a rendszergazdáknak és külső auditoroknak csak olvasási jogosultsága.

A begyűjtőhely

A kollektor az SCOM-csoporton belül bármilyen felügyeleti kiszolgálóra telepíthető. Csak egy dedikált adatbázis igényel egy SQL

2005 szerveren. Az SCOM 2-es bétában egy kollektornak egy adatbázis jár, és egy ACS-adatbázisba csak egy kollektor írhat. E felállítás mögött főként teljesítményszempontok

hetik saját valós idejű monitorkait is. A biztonságfelügyeleti csoport így gyorsan (azonnal) értesülhet az adott időintervallumban történt sikertelen bejelentkezési kísérletek-

• Reports

- Easy to customize using SQL report builder
- Built in partnership with Windows Security Core

• Subset of reports available out of the box:

<ul style="list-style-type: none"> • Account Management <ul style="list-style-type: none"> • User account created / deleted / enabled / disabled • Detect changes to domain admins and administrators groups • List group membership changes • Changing Someone Else Password • Computer accounts created / deleted • Access Violation <ul style="list-style-type: none"> • Unauthorized access attempts • Account locked 	<ul style="list-style-type: none"> • Policy Change <ul style="list-style-type: none"> • Audit Policy Changed • Object SACL Changed • Object Permissions Changed • Account Policy Changed • Privilege Added / Removed • System Integrity <ul style="list-style-type: none"> • Lost Events • Audit Failure • Log Cleared
--	--

Rengeteg biztonsági eseményt tudunk automatizáltan naplózni

állnak; lehet, hogy a végső változatban más lesz a helyzet.

Ugyancsak az aktuális bétában egy kollektor legfeljebb 100 tartományvezérlőt, 1000 kiszolgálót és 10 000 munkaállomást figyelhet. Ezek az ésszerűnek tűnő metrikák valószínűleg nem változnak – ha ennél többre van szükség, több kollektort kell felállítani, és azoknak új, egyedi adatbázist kell létrehozni. A mostani helyzet szerint nincs olyan Microsoft-megoldás, amely több ACS adatait aggregálná, de egy kis kézimunkával el lehet készíteni azt az SQL-lekérdező eszközt, amely ezt a feladatot is elvégzi.

A kollektorhoz érkező eseményadatok természetesen tartalmazzák a felhasználók és a számítógépek biztonsági azonosítóit (SID), majd az AD lekérdezésével valós felhasználók és gépnevek készülnek, aztán ezek kerülnek az adatbázisba. Az ismételt lekérdezések elkerülése és az AD tehermentesítése érdekében a kollektor a SID-eket gyorstárazza.

WMI-előnyök

A kollektor képes figyelni a WMI (Windows Management Instrumentation) objektummodell adataira is. Az SCOM így a biztonsággal kapcsolatos hálózati történésekről a WMI felügyeleti csomagjaiból rögtön a keletkezésük után is értesülhet, méghozzá „valósabb időben”, mint az eseménynaplók közvetítésével. A mostani helyzet szerint a Microsoft nem tervezi olyan eszköz készítését, amely a WMI-csomagok biztonsági elemzésére alkalmas lenne, de egyrészt külső fejlesztőktől várhatók effélék, másrészt a szervezetek elkészít-

ről, a biztonsági naplók nagy volumenű törléséről és általában az olyan incidensekről, amelyek gyors beavatkozást igényelnek. Az SCOM-ACS így behatolásérzékelő rendszerként (IDS) működhet.

Az adatbázis

A hálózat méretétől és a forgalom mértékétől függően az adatbázis jókora méretűre nőhet. A Microsoft saját hálózatán végzett SCOM-tesztelése

korán az 5000 szerver és 10 000 munkaállomás figyelésekor az ACS-ek 8 terabájtnyi adatot halmaztak fel havonta. Nem kell megjegyezni, mert a környezettől, az auditigényektől és a lehetőségektől függően erőteljesebben is lehet szűrni a tárolandó adatokat, másrészt a könnyebb kezelhetőség érdekében az adatbázist particionálni lehet. Így az akár több gép és lemez között is elosztható, ráadásul a friss adatok a leggyorsabb lemezen, a régebbiek lassabb lemezekre is tárolhatók.

Jó hír, hogy lehet archiválni is, ugyanis noha az SCOM béta 2-ben ez a funkció még nincs megvalósítva, a végleges változat képes lesz rá.

Audit Collection

- Redundancy
 - Multi-Collector supported (but data goes to separate db)
 - Alternative: cold standby (copy AcsConfig.xml) Collector can run on Gateway
- Mutual Authentication Enforced
 - Default: Kerberos Authentication (works with cross forest trust scenario)
 - Workgroup/Domains without 2-way trust => Certificate Authentication
 - Collector requires AD for certificate mapping
- Partition consolidation
 - Documented, but no tools and not tested
- Non-Windows security events can be collected through custom app inserting events into Windows security log
 - Unix -> Syslog -> custom event writer -> Windows sec log -> ACS

Az ACS igen sok mindenre képes

A Microsoft mindenesetre melegen ajánlja, hogy az ACS dedikált adatbázisa külön kiszolgálóra kerüljön a tranzakciók várható tekintélyes száma miatt.

Az adatbázis egyébként normalizált, azaz jól kell ismerni és érteni a szerkezetét a lekérdezésekhez, de egy eszközzel – AdtServer.dvAll – eseménynapló-szerű formában is át-

tekinthető. Nem mellékesen ez a „szerszám” a célzott lekérdezések és egyedi beszámolók készítéséhez is jól használható.

A beszámolók

Az SCOM béta 2 már bőségesen tartalmaz sablonokat, de ezek száma még messze nincs véglegesítve. A minták alapján biztosan lesz néhány érdekes és hasznos jelentésfeladás: jogosulatlan jelszóváltoztatási kísérletekről, csoporttagság-változásról, naplótörlésről, helyi biztonsági szabályok megváltoztatásáról és egy sor másról (például objektumok felhasználói elérési- és felhasználók objektumelérési kísérleteiről) tudósító riportok.

Az auditon túl

Láttuk, hogy az SCOM szükség esetén kiterjeszhető a behatolásvédelem felé is, de ha belegondolunk, némi összefüggés-vizsgálattal is megköszönhetjük saját fejlesztésű monitorozó

További információk

SCOM-dokumentumok (ingyenes Microsoft Connect-hozzáférés szükséges) – <https://connect.microsoft.com/SystemCenter/Downloads/DownloadDetails.aspx?DownloadID=4743>

eszközünket. Az ACS adatbázisának segítségével máris előáll a sokak által kissé utópisztikusnak tartott biztonsági incidenskezelő

(SIM), ha pedig a WMI-csomagok adatait vesszük alapul, akkor az azonnali beavatkozást is lehetővé tevő biztonsági eseménykezelő (SEM), vagy a kettőt kombinálhatjuk is (SIEM) – ráadásul mindezt a kereskedelmi rendszerek áránál jóval olcsóbban.

A lehetőségre nyilván lecsapnak majd a külső fejlesztők is. A Microsoft elsődleges célja mindenesetre az volt,

hogy az ACS struktúrával egy, a belső szervezeti felülvizsgálat és a külső audit céljaira alkalmas, a megfelelőségi igényeket is kielégítő funkcióval lássa el az SCOM-ot, és az eddig látottak alapján az ACS tisztességesen teszi a dolgát.

Kelemen László
kelemen@hungary.com

IT-BUSINESS TODAY

goes mobile ...

Az IT-BUSINESS TODAY SMS küldésével WAP rendszerben már mobiltelefonon is elérhető, így számítógép segítsége nélkül is elérhetővé válnak a legfontosabb ICT-piaccal kapcsolatos hírek, történések, események.



Próbálja ki most!

Küldje el az ITBTODAY szót SMS-ben a +36 30 285 5441 számra és kövesse az instrukciókat!

WAP cím: wap.it-business.hu

HÁZIREND ÉS JÓHISZEMŰSÉG

Akár tetszik, akár nem, mind a cégek közötti, mind a cégen belüli kapcsolattartásban az e-mail mint kommunikációs csatorna kritikus fontosságúvá vált.

Mivel cégen belül is kritikus fontosságú az e-mail, rendszerhiba esetén a rendszergazdáknak úgy kell rohángászniuk, mint zseblámpafényben pókoknak a falon. Sokkal fontosabb, hogy cégen belül le legyenek fektetve azok a levelezési szabályok, amelyek garantálják a rendszer folyamatos működését és az elfogadható felhasználói élményt.

Persze ez nem ilyen egyszerű.

- Léteznie kell cégen belül egy informatikai szabályzatnak.
- Nagyon fontos, hogy a cégvezetésnek ki kell állnia emellett a szabályzat mellett – és természetesen el kell fogadniuk, hogy ezek a szabályok rájuk is vonatkoznak.
- Végül kell egy eszköz, amellyel egyfelől monitorozhatjuk a rendszer működését, másfelől automatizmusokkal segíthetjük a szabályok betartását.

Itt érdemes egy kicsit elgondolkodni. Hogyan tudnánk elképzelni ezt egy ideális világban?

- Például beültetünk egy Mesterséges Intelligenciát a rendszerbe. Egy olyat, amelyik ismeri a Házi rendet, tudja, mi a jó a cégnek. Minden levél rajta megy keresztül és ő szintaktikai, szemantikai elemzésnek veti alá ezeket, majd mérlegeli, hogy a konkrét levél mennyire veszélyes a cég hírnevére. Ez jó ötletnek látszik, kár, hogy az MI-kutatás fényévekre jár ettől a szinttől.

- Létrehozunk egy részleget, mondjuk Kopasz Cenzor néven. Minden kimenő/bejövő levelet elolvasnak és döntenek. Ez se rossz, csak éppen napi milliós levélforgalmat lebonyolító cégeknél igen nagyra hízna ez a részleg.

Látszik, hogy a probléma erőszakos megoldása egyelőre nem járható út.

- Fel kell tételeznünk a felhasználó jóhiszeműségét – és biztosítanunk kell azokat az eszközöket, amelyek segítenek nekik a szabályok betartásában... és nekünk a szabályok betartatásában.

Milyen szabályokra kell itt gondolni? Pusztán felsorolásként néhány:

Etikai fal. Megakadályozni, hogy egy bizonyos részleg dolgozói e-mailben tudjanak kommunikálni egy másikkal. Mondjuk, egy tőzsdei cégnél.

Megőrzési és visszakeresési szabályok. Mindegyik levél a számára megadott ideig elérhető és visszakereshető legyen. Ez nemcsak megőrzést jelent, hanem megadott idő múlva törlést is.

Forró tartalmak cégen kívülre jutása. Személyi kódok, bizalmas adatok.

Garancia a levelek hivatalosságára.

Az Exchange ezen a téren a következőket nyújtja:

1. Managing Message Classification,
2. Managing Message Records (MMR),
3. Managing Transport Rules.

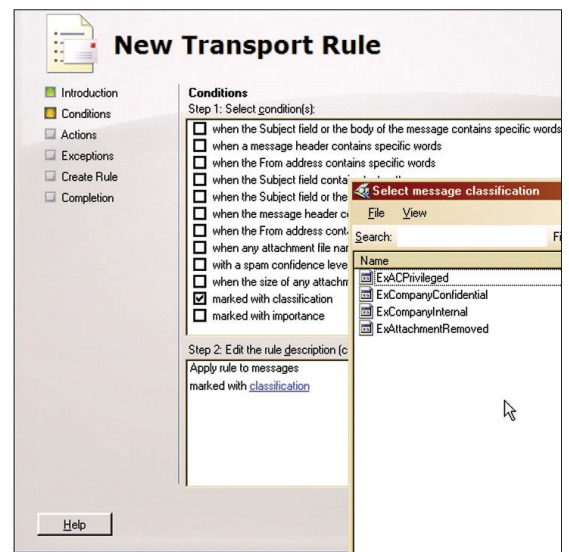
A továbbiakban egyenként nézzük végig ezeket az elemeket – bár fontos megjegyezni, hogy az adott célokot legtöbbször kombinált megoldásokkal érhetjük el.

Managing Message Classification

Megjelölhetjük leveleinket különféle meta-adatokkal. Jelölni eddig is tudtunk, nem is keveset: van olyan, hogy sürgősség, léteznek különböző nevű/színű zászlócskák, játszhatunk a lejáratí időkkel. Az Outlook/Exchange páros már eddig is a jelölömánia-kusok kánaánja volt.

Nos, most van egy óriási különbség.

Immár olyan egyedi jelölési módokat ve-



1. ábra. Transport Rule + Message Classification

zethetünk be, amelyek az egész organizációban egységesen értelmezettek. Nemcsak kliens-, hanem szerveroldalon is. Azaz nemcsak a kliens kategorizálhatja be az általa elküldött levelet, hanem – amennyiben eleget tesz bizonyos feltételeknek – akkor a Hub Transport szerver is. De nemcsak adjonisten létezik, értelmezett a fogadjisten is: tehát a Hub Transport szerver a kategorizálástól függetlenül mindenféle trükkökre képes a levelekkel kapcsolatban – természetesen Transport Rule-ok segítségével.

Csak nagyon gyorsan: egy tisztességes Transport Rule három komponensből áll – feltételből, akcióból és kivételből. Teljesen úgy, mint egy átlagos Outlook-szabály.

Az 1. ábrán pedig azt láthatjuk, hogy a képzeletbeli admin egy szabály feltételétől éppen levélklasszifikációt szeretne beállítani. Amennyiben a szabálynak az akció része lenne a megjelölés, természetesen hasonló ablakot látnánk.

Mely ablakban eléggé nehezen értelmezhető opciók mosolyognak ránk, hökkent adminokra. Ezek nem mások, mint a termékkel gyárilag érkezett jelölési lehetőségek.

Egész konkrétan:

- A/C Privileged,
- Company Confidential,
- Company Internal,
- Attachment Removed.

Nagyon fontos, hogy különválasszuk a jelölést és az akciót. Attól, hogy egy levelet elküldése előtt bejelölünk bármelyik beépített jelöléssel, nem fog történni semmi különös. A levél csupán meg lesz jelölve. Ha azt szeretnénk, hogy akció is történjen, nekünk kell legyártani hozzá a Transport Rule-t.

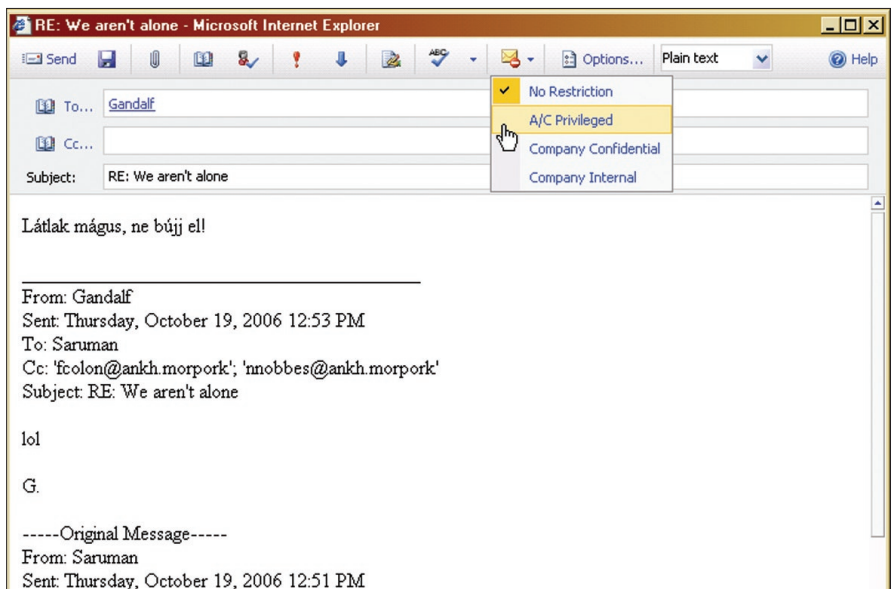
Egy konkrét klasszifikáció annyival is több a zászlócskánál, hogy komponensekből áll össze.

Display name. Ezt fogja látni a felhasználó, amikor a menüben kevereg.

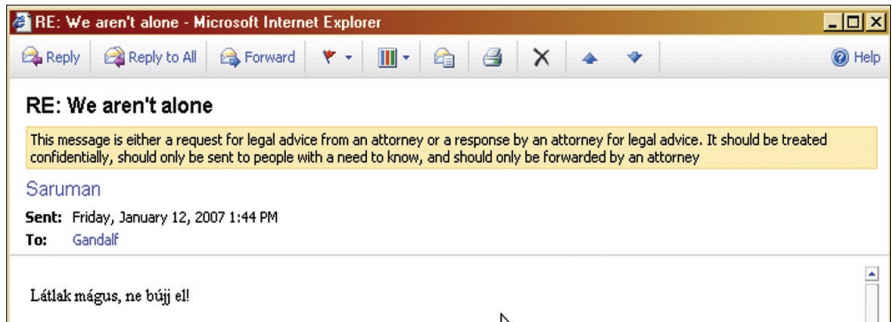
Sender description. Ez a hosszabb szöveg jelenik meg a feladó által összerakott levél fejléc mezőjében. Gyakorlatilag tájékoztatja a feladót, hogy az általa kiválasztott jelölésnek mi az értelme.

Recipient description. Szintén hosszabb szöveg. Ezt látja a címzett a levél fejlécében, amikor megnyitja azt.

Locale. Meghatározhatjuk, hogy különböző nyelvi beállítású klienseknél különböző nyelvi szövegek jelenjenek meg.



2. ábra. A Message Classification megjelenése az OWA-ban



3. ábra. Recipient description a címzett levélpéldányában

Nos, épp itt van már az ideje, hogy lássunk egy példát. Nézzük meg, mondjuk, az A/C Privileged klasszifikációt. Kezdjük a rövidítés feloldásával: az A/C az az Attorney/Client rövidítés feloldása, azaz magyarul Ügyvédi Beavatkozásnak lehetne fordítani.

Amint kiválasztjuk a jelölést, a fejlécben megjelenik a tájékoztató szöveg (sender description). Majd miután a címzett megkapja, nála is megjelenik a neki szóló tájékoztató szöveg (recipient description).

A leírásból már sejthetjük, hogy mi is az értelme ennek a jelölésnek. Azt mutatja meg, hogy ez egy olyan levél, amelyet az ügyvédnek küldtek véleményezésre, illetve olyan, amelyben az ügyvéd küldi vissza a véleményét. Azaz mindenképpen olyan levél, amelyet ügyvéd látott – és így egészen biztos, hogy a cég álláspontjával megegyező a tartalma. (Tulajdonképpen ez a jelölés a sokkal elterjedtebb disclaimer fordítottja: azt mondja, hogy igenis, ami ide le van írva, az a

cég véleménye.) Természetesen bízhatunk felhasználóink jóhiszeműségében. Bizhatunk abban, hogy tényleg csak akkor alkalmazzák ezt a jelölést, ha előtte valóban konzultáltak ügyvéddel.

Amennyiben viszont nem ma jöttünk le a falvédőről, beüzemelhetünk egy olyan Transport Rule-t, hogy amennyiben egy ilyen módon jelölt levelet talál, és a feladó nem a Jogi Részleg, akkor mindenképp térítse el a levelet a Jogi Részleg disztribúciós listájának irányába.

Miután eddig elég rendszeren összekarcoltuk a felszínt, itt az ideje, hogy egy kissé elmélyedjünk a technikai részletekben.

Például próbáljuk meg bekattintani ezt az A/C Privileged jelölést az Outlook 2003-kliensünkben. Nemigen fog menni. Megint az Outlook 2007-klienst használók jártak jobban. Bár bekattintási lehetőség náluk sincs, de legalább ki lehet erőszakolni.

Először hegesztünk egy kicsit a registryben.

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\
Common\Policy]
„AdminClassificationPath”=“c:\Classifications.xml”
„EnableClassifications”=dword:00000001
„TrustClassifications”=dword:00000001
```

Ne lepődjünk meg, Policy kulcs nem lesz, nekünk kell létrehozunk – mint ahogy a többi változót is.

Az első változó azt mondja meg, hol van a klasszifikációkat tartalmazó xml-fájl. A második arra vonatkozik, hogy a konkrét felhasználónál engedélyezve van-e a jelölgetés. A harmadik pedig arra utal, hogy a felhasználónak vajon Exchange 2007 szervertől van-e a postafiókjá? Mert ha máson, akkor úgysem fog működni ez az egész.

Vessünk most egy pillantást a C: partíció gyökerére, és számoljuk össze, hány darab Classification.xml fájlt találunk ott. Segítség: elég lesz az egyik kezünk a számoláshoz. Sőt. Még az egy szem ujjunk is sok lesz. Nincs. A mi dolgunk lesz odavarázsolni.

Persze, előbb le kell gyártanunk.

Mint írtuk, alaphelyzetben négy klasszifikáció érkezik az Exchange 2007 szervertől, ezeket tölthetjük fel a fájl. Ebben a lépésben egy Export-OutlookClassification.ps1 szkript és a GetMessageClassification cmdlet lesz a segítségünk. Az A/C Privileged jelölést például úgy tudjuk fájlba rakni, hogy a HUB Transport szervertől nyitunk egy Exchange Management Shell promptot, és beírjuk, hogy:

```
„ExACPrivileged” |Get-MessageClassification | ./Export-
OutlookClassification.ps1 > c:\exports\Classifications
```

És már készen is vagyunk. Persze ezt az egész miskulanciát megspórolhatjuk, ha OWA-t használunk, ott ugyanis helyből engedélyezve van a négy alapklasszifikáció.

De nehogy már itt megálljunk! Mint ahogy az elején szó volt róla, ennek a jelölősdinek az egyik fő értelme az, hogy saját magunk alakíthatunk ki a cégünk adminisztrációjának megfelelő klasszifikációs folyamatokat – azaz szabadon bővíthetjük a négy alapjelölést.

Egy dolog már előre garantálható: nem fog inhüvelygyulladást okozni a túl sok egértologatás. Ezt a folyamatot – mint minden más, kicsit komolyabb folyamatot sem – nem vezették ki a grafikus felületre. A cmdletek, valamint az Exchange Management Shell lesznek a barátaink.

Új jelölést a New-MessageClassification cmdlet segítségével hozhatunk létre. Természetesen mindazon elemeit meg kell adni a klasszifikációnak, amelyekről korábban már szó esett, sőt, olyan paraméterek is vannak, amelyekről eddig nem, ilyen például a precedencia. Mivel a paraméterek egyike a nyelvi lokáció, így annyi példányt hozunk létre a jelölésből – azonos néven –, ahány nyelvre szeretnénk, ha lenne külön jelölésünk.

Amennyiben már meglévő klasszifikációt szeretnénk piszkálni, használhatjuk még a következő eltagokat is: Get-, Remove-, Set. Ha olyan kedvünk van, akár a beépített jelöléseket is módosíthatjuk.

Managing Message Records (MMR)

Ez a témakör a levelek pontosan definiált ideig történő megőrzéséről, illetve ennek kikényszerítéséről szól. Természetesen itt is beleütközünk abba a problémába, hogy megpróbálunk ugyan mindent gondosan leszállítani, de a házirend csak akkor tartható be kellő alapossggal, ha a felhasználóink is jóhiszeműek.

A legjobban ugyanis a felhasználó tudja eldönteni, hogy egy konkrét levele melyik megőrzési kategóriába kerül. Ha megszületett a döntés, akkor már csak a megfelelő managed folderbe kell pottyantania a levelét – és a többit már tudja az Exchange.

De ehhez nekünk is meg kell tennünk néhány dolgot. Először például át kell rágnunk magunkat egy csomó száraz, zavaróan hasonlóan hangzó fogalom definiálásán.

Managed Folder. Az egész elképzelés azon alapul, hogy kijelölünk bizonyos foldereket, majd ezekre megmaradási szabályokat rakunk.

Managed default folder. Mindegyik felhasználó induláskor kapott postafiókjában tartalmaz ügynevezett alapfoldereket. Ezek az Exchange 2007-ben helyből menedzseltek folderek – azaz nem lehet őket törölni, máshová mozgatni.

Managed custom folder. Gyárthatunk saját menedzseltek foldereket is. Ezeket hozzárendelhetjük az egyes felhasználókhoz – így a

rendszerfolderekhez hasonlóan szigorú folderek jönnek létre a felhasználó postafiókjában.

Managed content settings. Ezek a beállítások tartalmazzák a korábban említett megmaradási szabályokat. Mindegyik menedzseltek folderhez hozzárendelhetünk egy – és pontosan egy – content settinget.

Managed folder mailbox policies. Az előbbi két komponensből csinos csokrot formálhatunk: azaz összemarkolunk több menedzseltek foldert – természetesen hozzátűzve a megfelelő content settingeket – majd ezt a csokrot elnevezük házirendnek. Az így létrejött policyt rendelhetjük hozzá az egyes felhasználóhoz. Tetszőleges mennyiségű házirendt gyárthatunk, de egy felhasználóhoz csak egy rendelhető.

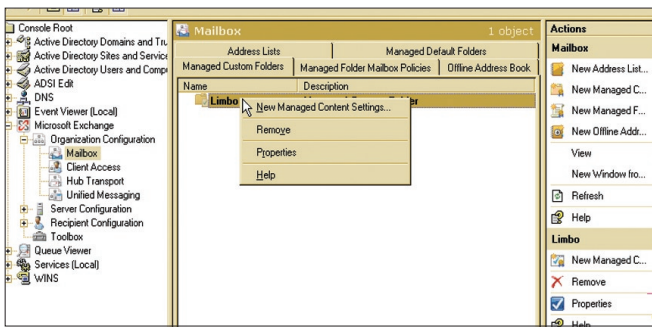
És akkor lássuk, hogyan is néz ki ez belülről! Képzeljünk el egy céget és azt, hogy a következő szabályozást szeretnék megvalósítani, mondjuk, a Jogi Osztály összes dolgozójára nézve:

- Az Inboxba érkező levelekről kerüljön másolat egy journaling célú postafiókba.
- Harminc nap után minden levél, amely még az Inboxban van, automatikusan kerüljön át egy Limbo nevezetű menedzseltek folderbe.
- Kilencven nap után minden levél végleg töröljön ebből a folderből.
- Kapjon minden felhasználó egy Archiv nevezetű menedzseltek foldert – egy olyat,

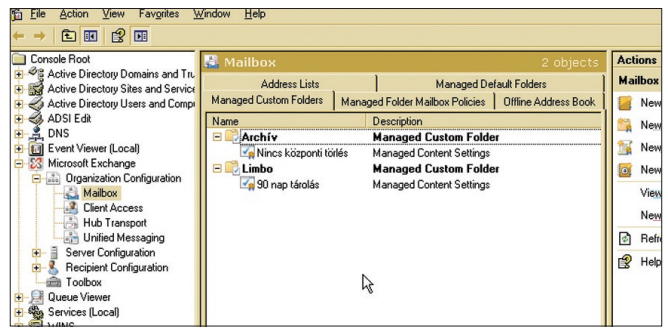


4. ábra. Új menedzseltek folder létrehozása

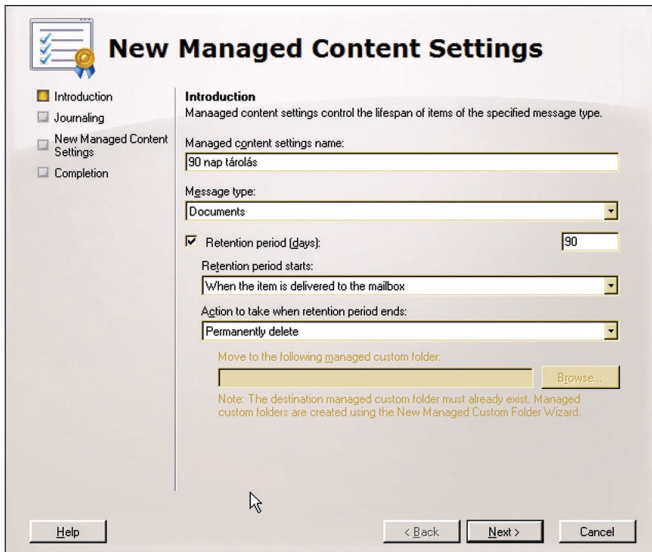
amelyre garantáltan nem esik rá semmilyen automatikus törlés. A felhasználó feladata, hogy milyen leveleket tesz át ide.



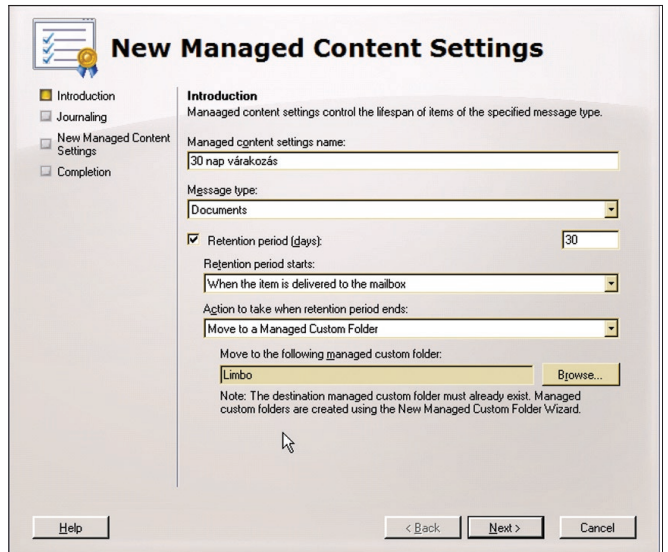
5. ábra. A content settings hozzárendelése a menedzselte folderhez



7. ábra. Menedzselte folderek, legyártás után



6. ábra. A content settings paraméterek beállítása



8. ábra. Az Inboxhoz rendelendő content settings-beállítások (1)

- Mindegyik saját menedzselte foldernek legyen maximálva a mérete.
- A karácsonyi ünnepek alatt ne működjen ez a házirend. Csapjunk bele!

Első lépésben le kell gyártanunk a Limbo nevű menedzselte foldert. Mivel az MMR organizációs szintű konfiguráció, logikus, hogy az Organization Configuration/Mailbox menüponthoz tartozó panelben találjuk a beállítási lehetőségeket (5. ábra).

Miután kiválasztottuk a New Managed Custom Folders opciót, a 4. ábrán látható panelhez jutunk.

Az egyes beállítási lehetőségek magukért beszélnek. Csupán egy érdemel kiemelt figyelmet: itt állíthatjuk be a folder maximális méretét. Jelen esetben ez 50 megabájt. Szigorúak vagyunk.

Az elkészült menedzselte folderhez illendő content settings hozzáadása is. Mivel szigorúan 1:1 az összerendelés, így új content settings létrehozása csak a folderen történő

jobbklattintással indítható. (Vagy a folder kijelölése után a jobb oldali task menüből.)

Végre, most már tényleg konfigurálunk. Azonkívül, hogy adunk egy beszédesebb nevet a beállításoknak, egész pontosan hangolhatjuk a visszatartás – retenció – paramétereit:

- Milyen adattípusra vonatkozzon a beállítás.
- Hány napból álljon az időintervallum.
- Milyen esemény számít az intervallum kezdőpontjának?
- Mi történjen, ha letelik az intervallum?

Habár a varázsló ad még nekünk ablakokat, de azokat a „Next” gomb intenzív nyomkodásával kezeljük le. Majd később foglalkozunk velük.

Itt most ugrottunk egy nagyot a történetben. A kép tanúsága szerint létrehoztunk egy új menedzselte egyéni foldert „Archív” néven, és gyártottunk hozzá egy új content settings-beállítást is – ebben gyakorlatilag minden beállítást üresen hagytunk.

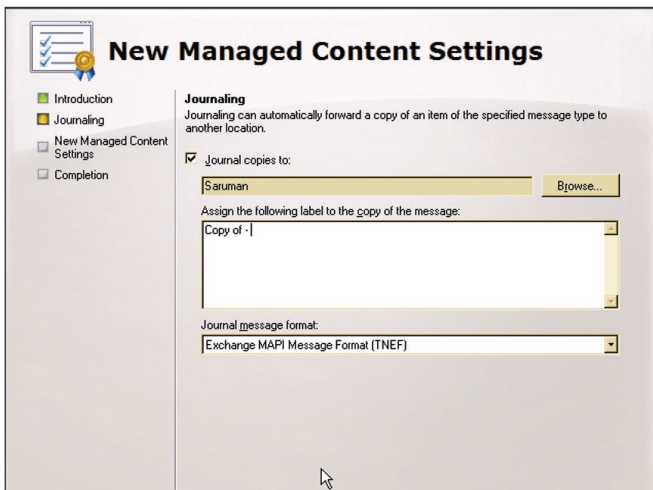
Jöhet az Inbox megfelelő preparációja. Mivel ez helyből menedzselte folder, itt csak content settings legyártására lesz szükségünk.

Ez egy új panel, eddig még nem találkoztunk vele. Itt tudjuk beállítani, hogy melyik postaládába kerüljenek mentésre (journaling) a levelek. Természetesen egy keveset ezen is konfigurálhatunk. (A TNEF beállítás az alap – bár saját tapasztalatok szerint sokkal kezelhetőbb az .msg formátum. Kész szercse, hogy ezt is lehet választani.)

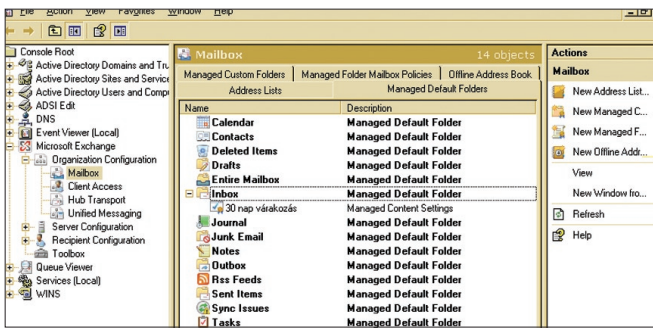
Ezzel is megvolnánk. Elkészült az összes folder, mindegyikhez legyártottuk a content settings-beállításokat. Jöhet a házirend.

Mint ahogy szó volt már róla: a házirendet közvetlenül a felhasználókhöz rendeljük. Ez nem túl jó hír azok számára, akik több ezer postafiókkal rendelkező szervert üzemeltetnek. Persze minden csak nézőpont kérdése: számukra az a jó hír, hogy hamar meg fogják tanulni az Exchange Management Shell kezelését.

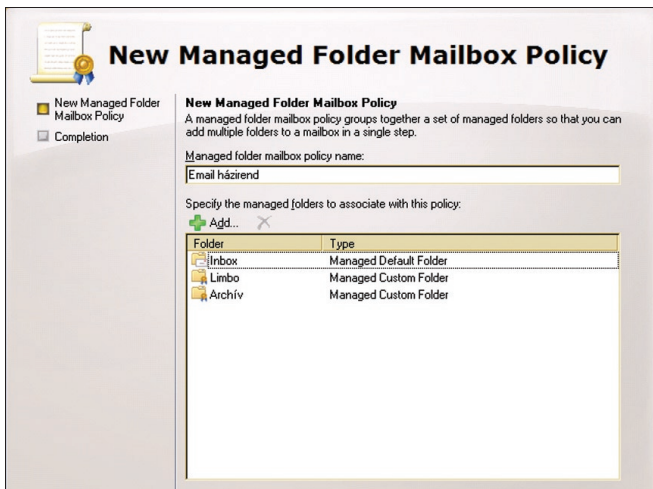
Még egy érdekességre kell felhívni a figyel-



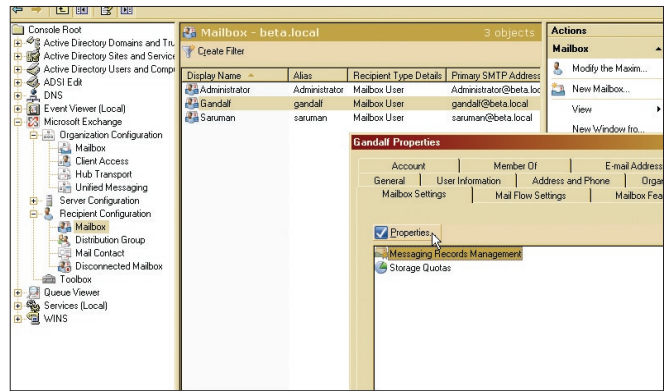
9. ábra. Az Inboxhoz rendelendő content setting-beállítások (2)



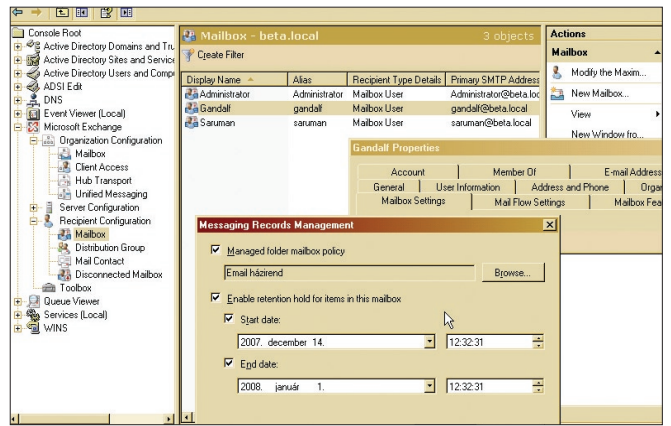
10. ábra. Az Inbox kiperparálása



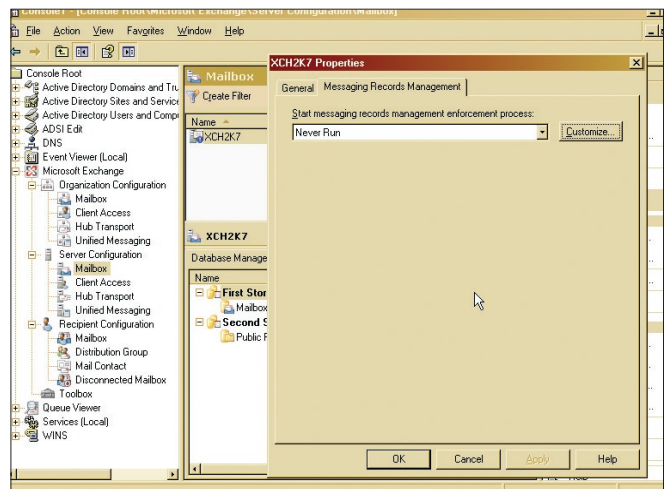
11. ábra. A Managed folder mailbox policy-összeállítás



12. ábra. A házirend felhasználóhoz rendelése



13. ábra. A házirend érvényességi idejének beállítása



14. ábra. A Messaging Record Management ütemezése

met: azt az időintervallumot, amikor nem szeretnénk, ha a házirend működné, szintén felhasználói szinten tudjuk csak beállítani.

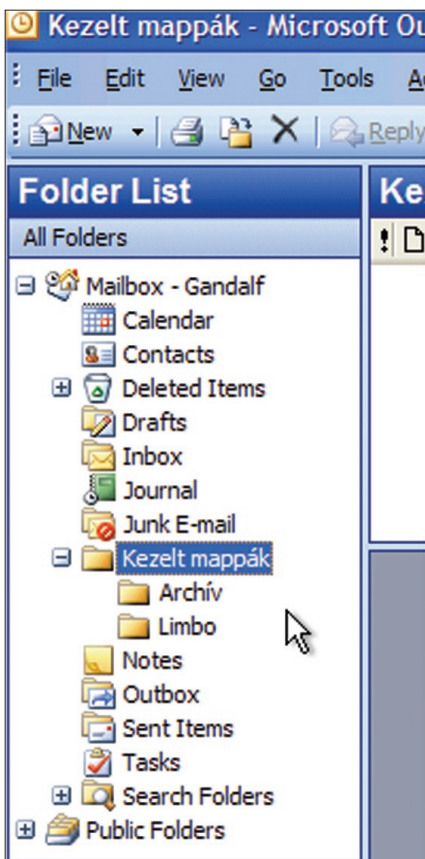
Itt jön az első rejtett akna.

Szépen beállítottunk mindent, ahogy a kézikönyvben le volt írva, várjuk a termés beérését... aztán nem történik semmi. Rutinos adminisztrátorok nem is számítottak másra,

tudják, hogy ami házirend, az minimum lassú. Várjunk.

Csakhogy a házirend továbbra sem érvényesül. És magától nem is fog, tekintve, hogy alapállapotban az enforcement process ütemezése „never” állapotú. Ezt bizony át kell lökni „custom” állapotba, majd bejelölni: ténylegesen mikor is szeretnénk, hogy fusson.

Közben azért elsiklottunk egy fontos dolog mellett: a házirend ütemezésének állítása ugyanis már nem az organizáció szintjén történik. Gyakorlatilag mindegyik Mailbox szerverre más-más ütemezést tudunk beállítani – mint ahogy a 14. ábrán ez látszik is. A mélyben ennek az az oka, hogy a házirend érvényre jutását egy úgynevezett Managed



Folder Assistant komponens végzi – és ennek az ügyködése igen erőforrás-igényes feladat. (Emiatt van a default tiltás is.)

És itt van. Elkészült.

Apró hátrány, hogy az Inboxra tett MMR-beállítások mindenkire vonatkozni fognak. Egyformán. Persze, persze, mondtuk az elején: a vezetőknek tisztában kell lenniük azal, hogy a szabályzat rájuk is egyformán vonatkozik. Nos, ez az ideális állapot, amely felé törekednünk kell. A valós világban viszont az adminisztrátor leginkább az állással játszik, ha kiderül róla, hogy olyan szabályt gyártott, amely a vezér leveleit pakolászza ide-oda.

Mi a megoldás?

Csinálni kell alternatív Inbox foldert.

Ugyanis nem csak managed custom foldert készíthetünk, hanem managed default foldert is. Természetesen továbbra is egyegy Inbox folderük lesz a konkrét felhasználóknak – de mi adhatjuk meg, hogy az melyik legyen: az eredeti vagy a preparált.

Transport Rules

Ez önmagában is egy akkora terület, amely simán megérdemelné egy önálló cikket. Jelen

írásban meg sem próbáljuk teljeskörűen bemutatni, inkább csak arra koncentrálunk, hogyan kapcsolódnak ezek a szabályok a házirend, illetve a jóhiszeműség témakörébe.

Példát már eddig is láthattunk szabályok alkalmazására: említettük korábban az A/C Privileged levelek terelgetését.

Anélkül, hogy túlzottan belemennénk a részletekbe, érdemes felsorolni, milyen lehetőségeink vannak még:

- Company Internal klasszifikációval megjelölt leveleknél biztosítani, hogy ne mehessenek ki.
- Etikai fal: be lehet állítani, hogy mely disztribúciós lista tagjai mely más disztribúciós listáktól legyenek elzárva. (Elzáráson azt kell érteni, hogy a levelek világosan érthető üzenet kíséretében pattanjanak vissza.)
- Rögzített formátumú bizalmas adatok kijutásának megakadályozása.
- Disclaimer automatikus hozzáadása a levelekhez.
- És minden egyéb, amelyet kellő paranóiaival rendelkező biztonsági felelősök ki tudnak találni.

A disclaimer hozzáadása a leg-egyszerűbb – habár a többi sem sokkal bonyolultabb.

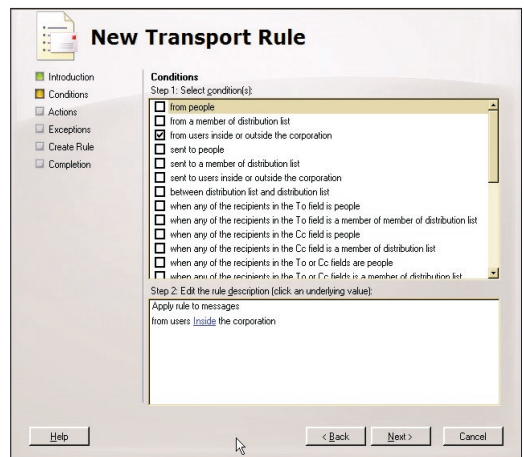
Lépésről lépésre

Az első lépésben kijelöljük, milyen feltételnek kell megfelelnie annak a levélnek, amelyet el akarunk látni disclaimerrel.

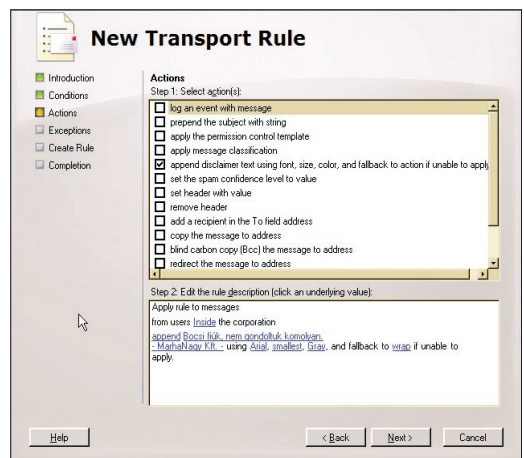
Jelen esetben ez mindösszesen annyi, hogy céges felhasználó legyen a feladó.

A következő lépésben adhatjuk meg a feltételhez rendelt akciót. Alul a késsel jelölt szövegre kattintva pontosíthatjuk a számunkra fontos változó értékét. Vegyük észre, hogy még formázni is tudjuk bizonyos mértékben a szöveget.

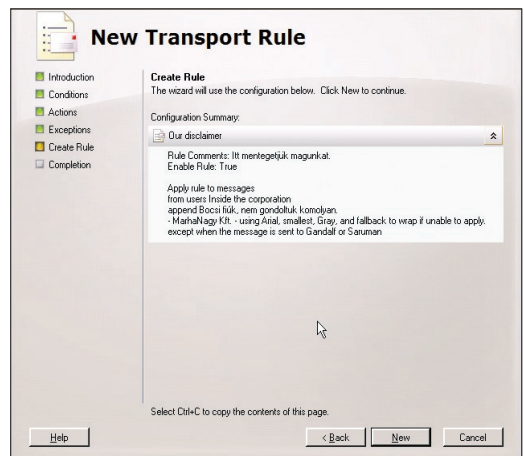
A kivételek kiválasztása után jutunk el ahhoz a képernyőhöz, ahol visszanezhetjük, mit is akarunk csinálni igazából. Majd a Next gombra kattintva kapunk még egy ablakot:



15. ábra. Disclaimer létrehozása – a feltétel



16. ábra. Disclaimer létrehozása – az akció



17. ábra. Disclaimer létrehozása – összefoglalás

ott jelenik meg, hogy amit összekattogtattunk a grafikus felületen, hogyan lehetett volna parancssorból is összehozni.

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

WINDOWS VISTA – A BIZTONSÁG JEGYÉBEN

A rosszindulatú kódok létezése nem csupán városi legenda.

A Microsoft 2002 elején indította el Trustworthy Computing (TwC) programját, részben azért, hogy válaszoljon a biztonsági kihívásokra. A TwC egyik alappillére az SDL (Secure Development Lifecycle), ami röviden annyit jelent, hogy valamennyi 2002 után kiadásra kerülő Microsoft-alkalmazás fejlesztésénél a biztonság az egyik legfontosabb alapelv.

Nemcsak az a fontos ugyanis, hogy egy alkalmazás sokkal több új funkciót tartalmazzon, mint az azt megelőző verzió, hanem jól is kell megírni azt. Ebben az összefüggésben pedig a „jól” „biztonságosan”-t jelent. A Windows XP két évvel a TwC előtt született, ezért annak fejlesztése során a TwC által lefektetett biztonsági irányelvek még nem kaptak olyan hangsúlyt, mint a most megjelent Windows Vista esetében.

A teljesség kedvéért meg kell említenünk, hogy a Windows XP életpályáján is megtaláljuk az SDL-t alkotó kezek nyomait, egészen pontosan az XP SP2-ben. Itt jelentek meg először a biztonságra hangolt alapbeállítások (secure by default).

A Windows Vista ezt a hozzáállást természetesen megörökölte, és itt már a szoftver tervezésénél is a biztonság volt az egyik legfontosabb szempont (secure by design).

Nézzünk kicsit a dolgok mélyére, és vizsgáljuk meg, mit is jelent a „secure by default” és „secure by design” a Windows Vista esetében.

Meghajtók és olajak – Kernel Mode Code Signing (KMCS) és Kernel Patch Protection (KPP)

Minden autó motorjához adott típusú és minőségű olajat ajánl a gyártó. Ezt igyekszünk betartani, hiszen nem szeretnénk, ha baja esne a család négykerékű kedvencének. Sajnos számítógépünk operációs rendszere már nem minden esetben részesül ilyen kegyben. Az egyes hardverelemekhez tartozó meghajtóprogramok sok esetben ellenőrizhetetlen forrásból származnak, és ki tudja, milyen egyéb – kártékony – kódot rejtnek.

Az ilyen módon terjedő rosszindulatú kódok kiszűrésének egyik lehetséges módja, hogy csak ellenőrzött forrásból származó meghajtókat használunk. Ez azért különösen fontos, mert a meghajtók kernel módban futnak. Míg egy felhasználói módban futó kód hiba esetén csak a programot fagyasztja le, egy kernel módban futó a rendszer stabilitását veszélyezteti. Jön a kék halál, az operációs rendszer minőségének és fejlesztőinek magasztalása, pedig valójában a kétes meghajtóprogram okozta a problémát.

Ezeknek a minőségi követelményeknek a kötelezővé tétele – a piacon már régóta futó 32 bites rendszerek miatt – nem is olyan könnyen kivitelezhető, hiszen a jelenlegi meghajtóprogramok jelentős része – még neves gyártók esetében is – aláíratlan, így ellenőrizhetetlen

azok eredetisége. Az inkompatibilitást elkerülendő, az aláírt kernel módú eszköz-meghajtók (KMCS – Kernel Mode Code Signing) csak a 64 bites Vista-verzió esetén kötelezőek. Ebben az esetben minden, kernel módban futó kódnak digitális aláírással kell rendelkeznie, ami egyértelművé teszi, ki a program kiadója, továbbá, hogy a kód eredeti, és azt senki nem változtatta meg.

Windows Vista x64 esetén a nem aláírt, kernel módú kód nem tölthető be – még rendszergazdai jogosultsággal sem.

A 32 bites verzióban az aláírt kód használata nem kötelező, kivéve a jogvédett tartalmak lejátszásához szükséges meghajtók esetén, amelyek a Protected User Mode Audio, a Protected Audio Path és a Protected Video Path – Output Protection Management hívásokat használják.

A digitális aláírás megléte mellett, a kernel módban futó programnak, kódnak, meghajtónak be kell tartania néhány alapvető szabályt:

- nem módosíthatják a system service-táblák függvénymutatóit (kernel hook), az Interrupt descriptor táblát (IDT) és a Global descriptor táblát (GDT);
- tilos bármely kernelverem használata (kivéve, ha azt maga a kernel kezdeményezte), és nem tolerált semmilyen szintű kernelmódosítás, bővítmény, patch.

Ezt hívják kernelvédelemnek (Kernel Patch Protection vagy más néven PatchGuard).

Ami egyébként nem kifejezetten új technológia, ugyanis még a Windows Vista előtt, a 64 bites Windows Server 2003 Service Pack 1-ben debütált, és megtalálható a Windows XP Professional x64-ben is.

Az eredeti az igazi – Code Integrity (CI)

A kódintegritás-vizsgálat alapvető feladata az operációs rendszer lelkének – a kernelnek – a védelmében tett biztonsági rendszabályok (KMCS és KPP) betartatása. A rendszerindítás során a WINLOAD.exe (az NTLDR utóda) tölti be és vizsgálja meg az úgynevezett boot-start meghajtóprogramokat, a HAL-t (HAL.dll) és az NTOS-kernel (NTOSKRNL.exe), hogy történetesen azokban változás az eredetileg telepített kódhoz képest. Ezt úgy végzi el, hogy összehasonlítja azok SHA1-es hash-értékeit a rendszerkatalogusban (nt5.cat) eredetileg tárolt értékkel, és ellenőrzi a program aláíróját.

Ha azok SHA1-es hash-értéke nem egyezik a hozzájuk tartozó aláírásban szereplővel (meghajtók esetében), a folyamat nem folytatódik, és a rendszer hibaüzenettel leáll. Ezt a folyamatot megelőzi az SHA1 és PKCSI aláírás-ellenőrző algoritmusok tesztje. A követ-

kező lépésben az NTOSKRNL.exe veszi át a felügyeletet, és ellenőrzi a rendszer- és a futás közben betöltődő meghajtóprogramokat.

Az NTOSKRNL.exe ad otthont a PatchGuardnak is, amely az operációs rendszer futása közben periodikusan ellenőrzi, hogy történetesen változás a kernelben (IDT, GDT).

A betöltődő meghajtók ezt követően véletlenül helyezkednek el a memóriában (ASLR), hogy az esetleges – tipikusan verem-túlszordításos – támadások ne tudják pontosan memórián belüli elhelyezkedésüket. A DEP (Data Execution Prevention) az adatmemória-területeket védi, hogy azokon ne lehessen kódot futtatni. A DEP és ASLR technológiákat a TechNet magazin tavaly augusztus-szeptemberi számában (<http://tinyurl.com/2caajj>) részletesen ismertettük.

A rendszer magját védő megoldások áttekintése után vizsgáljuk meg, hogy milyen biztonsági fejlesztések történtek az egyes Windows-szervizek és az alkalmazások megővására.

Service Hardening

A Windows-szervizek saját biztonsági szinttel rendelkeznek, ami sok esetben nem egyezik meg a bejelentkezett felhasználó hozzáférési szintjével. Mint minden szoftver esetében, az egyes szervizekben is előfordulhat sérülékenység (például verem-túlszordításos hiba), és ezt kihasználva a rosszindulatú kód írója a szerviz nevében (jogosultságon) hozzáférést

tud szerezni az operációs rendszerhez. Az XP esetében sok szerviz magas privilégiumokkal, biztonsági hozzáférési szintekkel rendelkezik (gondoljunk csak a mindenható RPC szervizre amely LocalSystem-joggal futott

SVCHOST		
Windows XP Service Pack 2	Wireless Configuration	RemoteAccess
LocalSystem	System Event Notification	DHCP Client
m	Network Connections	W32time
	COM+ Event System	Rasman
	NLA	Browser
	Shell Hardware Detection	6to4
	Themes	Help and Support
	Telephony	Task Scheduler
	Windows Audio	TrkWks
	Error Reporting	Cryptographic Services
	Workstation	Removable Storage
	ICS	WMI Perf Adapter
	BITS	Automatic updates
		App Management
		Secondary Logon
Network Service	DNS Client	
Local Service	SSDP	
Service	WebClient	
	TCP/IP NetBIOS helper	
	Remote Registry	
Windows Vista	Removable Storage	WMI
LocalSystem	WMI Perf Adapter	App Management
Network restricted	Automatic updates	Secondary Logon
	TRWks	
LocalSystem	BITS	
Demand started		
Network Service	DNS Client	Browser
Restricted	ICS	6to4
	RemoteAccess	Task scheduler
	W32time	IPSEC Services
	Rasman	Cryptographic Services
Local Service	Wireless Configuration	Network Connections
Restricted	WMI	Rasauto
No network access	System Event Notification	Themes
	Shell Hardware Detection	COM+ Event System
Local Service	Telephony	Error Reporting
Restricted	Windows Audio	Event Log
	TCP/IP NetBIOS helper	Workstation
	WebClient	Remote Registry
		SSDP

A rendszerszolgáltatások jogosultsági változásai a szervizfiókok tekintetében

egészen XP SP1-ig). A híres Nachi és Blaster féregtámadások pont az RPC egyik interfészének túlszordításos hibáját használták ki.

A Windows Vista esetében ahol csak lehetőség volt, a szervizek már nem Local System-fiókkal futnak, de ha ez mégis elkerülhetetlen, akkor lehetőség van azok „kettévágására”, hogy ne a teljes szerviz, csak a szükséges komponense fusson magasabb jogosultsággal.

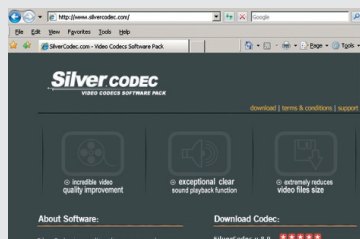


„Kettévágott” szervizek

További újdonság, hogy a szervizek egyedi SID azonosítót kaptak: S-1-80-<a szerviz nevéből képzett SHA-1 hash>. A Vista hozzáférési listáiban (DACL) ez alapján, szerviz-SID-enként egyedileg (ACE) lehet korlátozni, hogy azok milyen erőforrásokhoz (állományok, hálózat) férhetnek hozzá. Korábbi operációs rendszerekben a szervizek nem rendelkeztek egyedi SID-del, csak a felhasználók és a csoportok. Az egyedi S-1-80-as azonosító alapján a Windows Vista tűzfalában is lehet szervizekre vonatkoztatva szabályokat definiálni. Lehetőség van továbbá arra is, hogy bizonyos szervizek ne tudják módosítani a regisztrációs adatbázist, né férhes-

Nincs ingyen ebéd!

Az elmúlt hónapokban egyre több csali oldal jelent meg, ahol adott hang- és videokártyákhoz kínálnak olyan meghajtóprogramokat, amelyek használatával jobb képminőség és tisztább hangzás érhető el... Az ősi szabály itt is igaz: nincs ingyen ebéd!



A letöltést és telepítést követően – meglepő módon – a video- vagy hangkártya teljesítménye nem javul, de helyette kapunk néhány rootkit-programot, amelyek a kernelben megbújva, a kerneltáblák és kernelhívások módosításával remekül el tudnak rejtőzni. A téma további részletei iránt érdeklődőknek érdemes elolvasniuk Mark Russinovich nagyon izgalmas előadását arról, hogyan szabadulhatunk meg a rootkitektől: <http://tinyurl.com/yji7zs>.

Hash-ellenőrzés

Windows-kód	Igen
WHQL-minősített meghajtóprogramok	Igen
Aláírás nélküli meghajtók	Lokális vagy csoport-házirend szerint
Nem Windows-alkalmazások	Nem

senek hozzá a rendszerállományokhoz vagy csak egy bizonyos állományhoz: például a SysEvent.evtx-hez csak az Eventlog szerviznek legyen írási joga, másoknak csak olvasási joguk legyen, vagy még az sem. Minden egyes Windows-szerviznek van egy előre elkészített szervizprofilja, amelyik pontosan ezeket a megkötéseket definiálja.

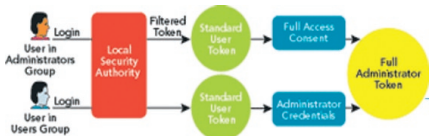
További védelmet jelent a session 0-izoláció. Ennek lényege, hogy a Windows indulásakor létrejövő első, úgynevezett 0-s futtatási szinten csak olyan szervizek és alkalmazások futhatnak, amelyek nem kapcsolódnak más – magasabb – felhasználói szintekhez, és nem rendelkeznek felhasználói interfésszel (ennek okán nincs is hozzáféréstük a grafikus hardverhez).

A szervizek megerősítése nem tud megakadályozni egy, az adott szerviz sérülékenységére épülő támadást, de magán a szervizen keresztül az operációs rendszer többi része nem érhető el. A támadások kivédése a Windows Vista új tűzfalának és a többi proaktív, többszintű védelmi megoldásnak a feladata.

Mandatory Integrity Control

Az ACL alapú kontrollnak van azonban néhány hiányossága. Egy ACL-lista specifikusan, adott objektumokhoz definiál hozzáférési jogot vagy tiltást, szervizekre, felhasználókra vagy felhasználói csoportokra vonatkoztatva. Valójában mindenki részese valamelyik virtuális listának, hiszen ha az adott listán nem szerepel, akkor beletartozik a „mindenki más” csoportba, és az arra értelmezett szabály vonatkozik rá. Ez akár végzetes is lehet. Tegyük fel, ha egy objektumhoz tartozó Security Descriptor nincs DACL-hez rendelve, az objektumhoz egy NULL DACL rendelődik hozzá. Ennek a DACL-nek az egyik ACE-sora pedig így szól "Everyone: Full control".

Hozzáférési listákkal nem lehet hierarchikus, alá-fölé rendelt viszonyt definiálni programok és folyamatok között. A Mandatory Integrity Control (MIC) viszont pont ezt valósítja meg. Lényege, hogy egy alacsonyabb integritási szinttel rendelkező folyamat vagy program nem módosíthat magasabb integri-



Felhasználói tokenek

Defined integrity levels				
System	High	Medium	Low	Untrusted
400	300	200	100	0
Local System	Local Service Network Service Elevated (full) user tokens	Standard user tokens Authenticated Users	World (Everyone)	Anonymous All other tokens

Shell runs here

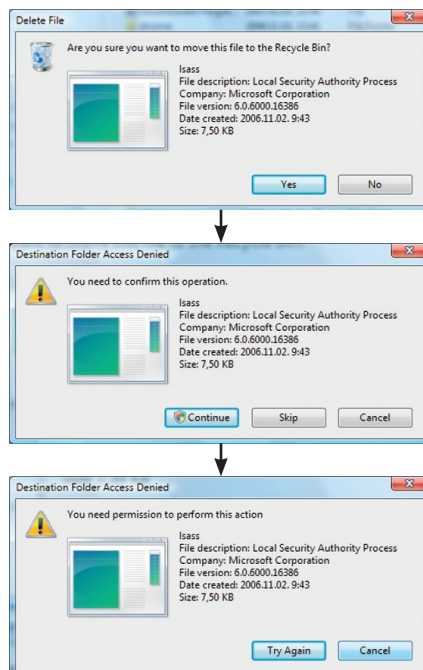
Windows Vista: integritási szintek

tási szinttel rendelkezőt, még akkor sem, ha az objektum DACL-je engedné is azt.

Bejelentkezéskor a felhasználó kap egy egyedi, saját integritási szintjét jelölő Security Identifiert (SID), ami ezt követően a saját tokenjéhez csatolódik. A SID formája S-I-16 <címké>, ahol a címké tartalmazza az integritási szintet.

Minden, MIC által védett objektum (állományok, mappák, eljárások, registry-kulcsok, szervizek, nyomtatók, megosztások) szintén kap egy SID-et, amelyet az adott objektumhoz tartozó security descriptor tárol – ez egy új ACE-sor az DACL-ben. (Ennek a SID-nek semmi köze a Service Hardeningnél említett egyedi S-I-80-<a szerviz nevéből képzett SHA-1 hash> szervizazonosítóhoz.)

A hozzáférés-ellenőrzés (immáron, hogy MIC is van) két lépcsőben zajlik. Az ACL-lista ellenőrzését megelőzően a Vista meg-



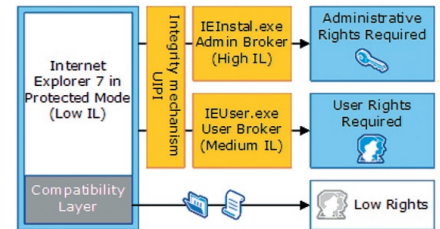
Kísérlet – rendszergazdai joggal – az lsass.exe törlésére... Nem sikerült

vizsgálja, hogy például a felhasználó által indított program milyen szinttel rendelkezik, ha az egyenlő vagy magasabb az objektum szintjével, akkor az írás/törlés engedélyezett. De az is csak akkor, ha – és itt jön a második lépcső – a DACL-lista is engedi.

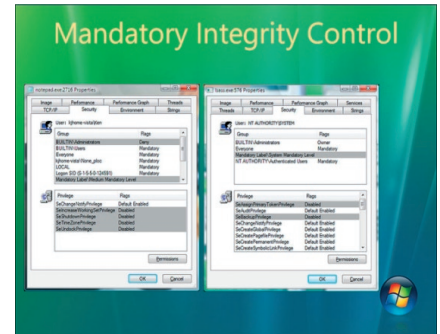
Látható, hogy az operációs rendszer elemeinek magasabb integritási szintje van, mint a rendszergazdának, így rendszergazdaként sem lehet például az lsass.exe állományt törölni. Próbáljuk ki: érdekes lesz...

Lássunk még néhány példát erre!

- E-mailben csatolt állomány érkezik. Ha lementjük vagy futtatjuk az állományt, ala-



Internet Explorerben egy internetzónába tartozó oldalról töltünk le egy állományt. Az csak az IE átmeneti mappájába tud írni, mivel alacsony integritási szinten fut



A notepad.exe integritási szintje közepes, az LSASS.exe – mint rendszerfolyamat – rendszerszinten fut

acsony integritási szintet kap, így nem tud írni még a felhasználói könyvtárakba sem.

- A rendszergazda futtat egy internetről letöltött programot. A program ennek ellenére alacsony szinten fog futni, megakadályozva az esetleges fertőzéseket.

Ez a technológia az alapja a korábban már ismertetett, és sokak által problémásnak tartott UAC (User Access Control) komponensének is. Ezek után már talán látható, miért is fontos, hogy ne tiltsuk le az UAC-t, még ha rendszergazdák vagyunk is.

Szabó Gábor (gabors@microsoft.com) Microsoft Magyarország

AJAX

– A WEBFEJLESZTÉS ÚJ TÁVLATAI

Szeretjük és egyre több feladattal látjuk el a webes alkalmazásokat: kényelmes, hogy más tartja karban a háttérrendszereket, és bárhonnán elérhetjük a szolgáltatásokat. Azért persze a weben sem minden tökéletes.

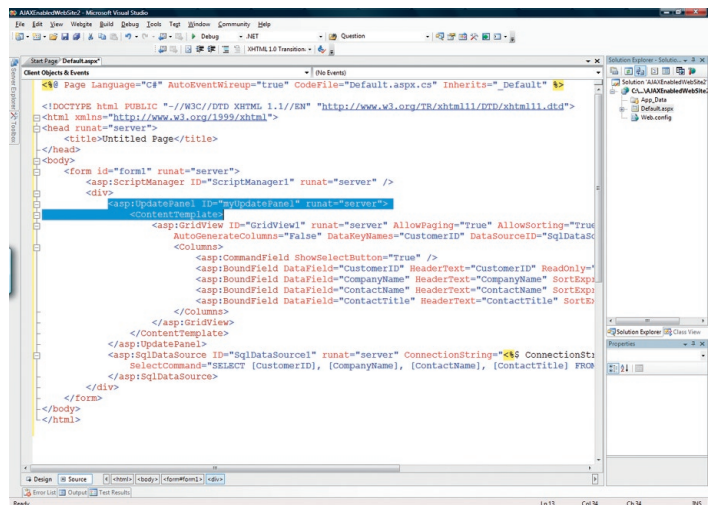
Az egyik legnagyobb kényelmetlenségi tényező az alkalmazások felületeinek egyszerűsége és az állandó oldallekérések miatti villódzás és ide-oda forgalom. Az ASP.NET jelentős haladást hozott a programozók számára azzal, hogy a szerveroldalon egy megszokott, kényelmes, objektum- és eseményorientált környezetet teremtett. Az egyetlen hátrány: ahhoz, hogy a szerveroldalon történjen a feldolgozás, el is kell juttatni az információkat a szerverhez. Ez a post-back.

Ekkor az oldal vezérlőinek állapota (ViewState) és a legutóbbi letöltés óta történt változások visszautaznak a szerverre egy HTTP-kérés keretében, ahol az ASP.NET-motor újra összerakja az oldal objektumait, ezek kezelik a megfelelő eseményeket, a kliens pedig visszakap egy frissített oldalt. Ez a programozási modell máris sokkal kényelmesebb, mint az, amikor a klasszikus ASP-ben még nekünk kellett az HTTP paraméterek életútját is követnünk. De persze nekünk ez sem elég. Sokszor van olyan ugyanis, hogy az oldalnak csak egy részét kellene frissíteni, mégis – teljesen felesleges – az egész oldalt újratöltjük.

A kezdetek

Tipikus ilyen szituáció például a webes levelezőfelületek megvalósítása, ahol egy levél törlése egy listából – ez, mondjuk, a képernyő 10 százalékát teszi ki – nem kellene, hogy a teljes oldal frissülését okozza. Erre jutottak anno az Internet Explorer 4.0 fejlesztői is, akik elsősorban az Outlook Web Access céljaira egy új objektumot, az XMLHttpRequest szerveroldali komponenst hozták létre. Ennek segítségével kliensoldali Jscript segítségével lehet HTTP-kéréseket intézni a kiszolgálóhoz, ezeket aztán Jscriptben tudjuk feldolgozni, és a válasz alapján frissíteni tudjuk az aktuális oldal HTML-objektummodelljét és így a megjelenített tartalmat.

Nincs más teendő, mint a szerveroldalon a megfelelő XML-webszolgáltatásokat implementálni; ezekhez lehet kérdéseket intézni, majd a válaszok alapján a megfelelő felületeket már könnyen frissíthetjük. Az



1. ábra. Az UpdatePanellel körbevett szekció mindig frissül

XMLHttpRequest lehetővé tette, hogy az Outlook Web Access kényelmes és elegáns legyen, ám maga a technológia mégis hamar feledésbe merült. Ennek a legfontosabb oka

az volt, hogy Jscriptben programozni elég könnyelmenten feladat. A böngésző a maga egyszerű módján segít ugyan megtalálni a hibákat, de a fejlesztőeszközök nem sok segítséget nyújtanak hozzá.

Az AJAX visszatérése

A webes alkalmazások elterjedésével az XMLHttpRequest újra a programozók érdeklődésének homlokterébe került. Az Outlook Web Access egyes változatai továbbra is nagymértékben használják, de más alkalmazások fejlesztői is vették a fáradságot ahhoz, hogy felületeiket kiegészítsék ezekkel a lehetőségekkel. Az egyik legismertebb ilyen alkalmazás a Gmail levelezőrendszer, de említhetnénk akár a Flickr fényképmegosztó oldalakat is. A technológia második virágzásakor kapta az AJAX nevet is, ami az Asynchronous JavaScript And XML rövidítése.

A visszatérés oka elsősorban az, hogy a lényegesen több felhasználó sokkal nagyobb igényeket támaszt a webes alkalmazások minőségével kapcsolatban, és hozzájárul az is, hogy több olyan programozói keretrendszer is megjelent, amelyek megpróbál minél több nehézséget levenni a fejlesztők válláról. Az AJAX új lehetőséget is hozott, mégpedig a kompozit, több webes alkalmazás lehetőségeit összekombináló alkalmazások, az úgynevezett mashupok kategóriájának megteremtésével (példaként gondoljunk, mondjuk, egy ingatlankereskedelmi weboldalra, amelyik egy külső szolgáltató térképeit használja a saját weboldalán). Az elterjedést nagyban segítette, hogy a Firefox böngésző is támogatja az XMLHttpRequest-objektumot.

Lehetne így is...

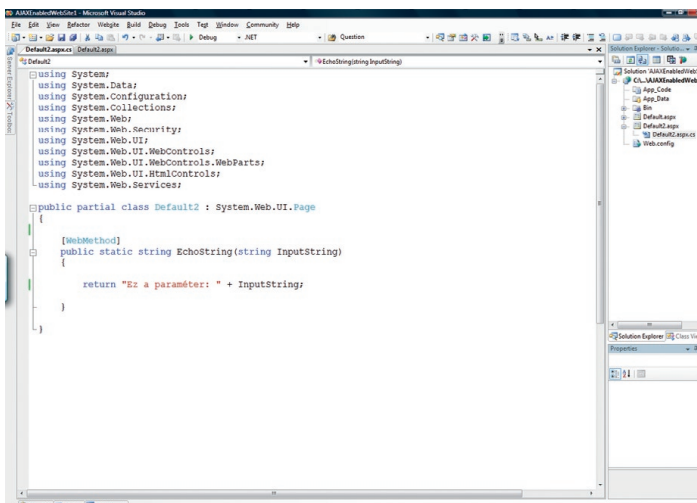
A technológiai elemek adottak: kliensoldalon egy Jscript-interpreter, amelyik képes a letöltött oldal teljes objektummodelljét elérni és módosítani; egy XMLHttpRequest-komponens, amelyik képes aszinkron HTTP-kéréseket intézni a szerverhez; kliensoldalon a Jscript képes a válasz-XML-t feldolgozni és aztán a HTML-tartalmat módosítani.

Nincs más teendőnk, mint létrehozni egy

olyan webservice-t, amelyik a választ fogja adni. Kliensoldalon egy Jscript-eseménykezelőben létrehozni egy XMLHttpRequest-objektumot, annak megadni a webservice-címét és egy másik eseménykezelőt, amelyik az aszinkron hívás utáni callbackt lekezeli. Ebben a második eseménykezelőben vesszük a visszaadott választ, azt értelmezzük, és a Document objektum megfelelő gyermekein keresztül frissítjük az oldal tartalmát. Ha va-

hogyan minél kevesebb tanulással tegyék lehetővé egy ASP.NET-fejlesztő számára az AJAX előnyeinek kihasználását. Ahhoz, hogy egy oldalt „ajaxosítsunk”, és lehetővé tegyük az oldal részleges, post-back nélküli frissítését, mindössze két dolgot kell megtennünk egy klasszikus ASP.NET-projektrel (a megfelelő szerelvények hivatkozásán kívül, de ha feltettük az AJAX keretrendszert, akkor ezt elvégezzük helyettünk a projektsablon is).

Az egyik, hogy az oldalon el kell helyezni egy <ScriptManager> vezérlőt. Ez biztosítja a megfelelő JavaScript-könyvtárak letöltődését a kliensoldalra. Azonnal felmerülhet a kérdés, hogy ha sok JavaScriptet töltünk le a kliensoldalra, az vajon hogyan befolyásolja az oldalak méretét és így a letöltés sebességét. Megnyugtató, hogy a teljes scriptkönyvtár néhány tucat kilobájt, de pont a teljesítmény okán még kisebb darabokra is szétszedték, és a <ScriptManager> feladata, hogy csak a szükséges fájlok töltsenek



2. ábra. Nagyon egyszerűen tudunk webservice-nélkül is függvényeket publikálni

laki bátor, akkor nekiállhat kézzel Jscriptet programozni – ez néha feltétlenül szükséges is –, de a fentiekből még mindig hiányzik a programozói egyszerűség.

... de mi lusták vagyunk

Ezért alkotta meg a Microsoft az ASP.NET AJAX keretrendszert. Több komponense is van, a legfontosabb az ASP.NET AJAX 1.0 csomag, amelyet most január 23-án adott ki a Microsoft. A korábban Atlas kódnéven ismert projekt elemeit két részre bontották, hogy minél előbb támogatott környezetként élvezhessék a fejlesztők a központi elemek előnyeit. A még fejlesztésre szoruló részek a 2.0 „Futures” CTP-be kerültek. Emellett a kliensoldali fejlesztéseket segíti az ASP.NET AJAX Control Toolkit, ez egy osztott forráskódú projekt a Microsoft támogatásával. A teljes ASP.NET AJAX keretrendszer letölthető a <http://ajax.asp.net> címről és a „Learn more” linkre kattintva elérhetjük a „futures CTP” és a Control Toolkit elérési útját is (<http://ajax.asp.net/about/default.aspx?tabid=47>).

Miből is áll az AJAX-beli programozás a keretrendszer segítségével? A cél az volt,

és azok úgy legyenek megcímelve, hogy a gyorsítótárak elkapják őket (a keretrendszerrel telepített Visual Studio-projektsablon egyébként ezt a komponenst is elhelyezi a projekt indulólapján, így erre sem kell külön figyelmet fordítanunk).

A következő módosítás, hogy a részlegesen frissítendő oldalrész körül kell venni egy <asp:UpdatePanel>, illetve azon belül egy <ContentTemplate> taggel. Így adjuk

További információk

<http://www.json.org>
<http://ajax.asp.net>
<http://ajax.asp.net/about/default.aspx?tabid=47>
<http://ajax.asp.net/docs/default.aspx>

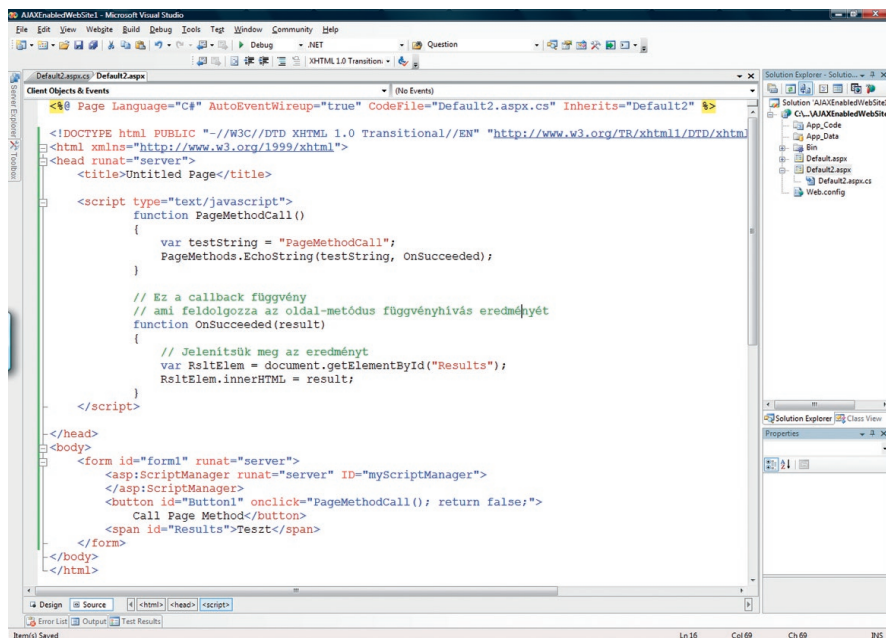
meg az ASP.NET-futtatókörnyezetnek, hogy az ezek között lévő tartalmat egy kicsit másképpen kell kezelni. Ezután pedig az történik, hogy a tagek között előforduló összes post-back-kérést elkapja az AJAX-runtime (a HTML-vezérlők eseménykezelői az AJAX keretrendszerre vannak irányítva) és aszink-

ron HTTP-kérésként scriptből küldi vissza a szervernek, ahol felépül ugyan az oldal objektummodellje, de csak azok a részek utaznak vissza a kliensre az oldal tartalmából, amelyeknek frissülniük kell. Ezután a kliensoldali script frissíti a böngészőben látható dokumentum tartalmát anélkül, hogy a teljes oldal frissülne.

egy vezérlő értékéhez is (például egy lenyíló menü kiválasztott értékéhez). Ugyanígy meghatározhatjuk azt is, hogy milyen feltételek mellett frissüljön egy panel.

Az `<asp:UpdatePanel>` komponenseket egymásba is lehet ágyazni, így a triggerek, feltételek és panelek kombinálásával egész komplex frissítési modelleket is meg lehet ha-

A több panel megadásán túl további lehetőség, hogy ha egy adott időintervallumnál tovább tart az aszinkron hívás és így a frissítés, akkor megfelelő kommunikációt jeleníthetünk meg a felhasználó felé, ami megmutatja, hogy éppen dolgozik az oldal, miért is kell várni. Erre szolgál az `<asp:UpdateProgress>` vezérlő, amelyet szintén akár több példányban is elhelyezhetünk az oldalon, és az egyes panelek frissüléséről külön-külön is hírt adhatunk.



3. ábra. Egy aszinkron callback megvalósítása

Mindössze két tag. Vegyük észre, hogy egy sor JavaScriptet sem láttunk, azt a keretrendszer elrejtí, mégis élvezzük az AJAX előnyeit.

Az 1. ábrán egy egyszerű ASP.NET-oldal forrását láthatjuk; ez egy GridView-ban jelenít meg adatokat a NorthWind adatbázisból, és ezen a GridView-n bekapcsoltuk a lapozást és a sorba rendezést. Klasszikusan ezek a műveletek az oldal teljes újratöltődésével járnak, de ha a kijelölésben látható sorokat és azok zárótagjeit hozzátesszük (és nem felelkezünk meg a ScriptManager-komponensről sem), akkor azonnal láthatjuk a különbséget az AJAX-beli felületen.

Az UpdatePanel lehetőségei

Alapértelmezésben egy `<asp:UpdatePanel>` mindig frissül, ha egy benne található vezérlő AJAX-beli post-backet okoz. Ezt korlátozni lehet azzal, ha úgynevezett triggereket határozunk meg, ilyenkor a panel csak akkor fog frissülni, ha a triggerek ezt kívártják. Triggereket lehet kötni egy vezérlő eseményéhez (például egy gomb megnyomásához) vagy

tározni. Lehetőség van arra, hogy a frissítést szerveroldali kódból érzük el, ilyen szituáció lehet például, ha az egyik aszinkron hívás eredményeként az oldal más részeit is frissítenünk kellene. Ezt az `<asp:UpdatePanel>` vezérlő Update() metódusával érhetjük el.

Sokszor lehet szükségünk arra, hogy egy oldal valamely része rendszeresen frissüljön. Gondoljunk csak mondjuk egy híroldal „friss hírek” részére. Az eddigiek alapján egy `<asp:UpdatePanel>` segítségével könnyen megoldhatjuk a részleges frissítést, már csak az időzített post-back hiányzik. Erre szolgál az `<asp:Timer>` vezérlő, amely a Tick eseményt váltja ki a megadott intervallumonként, ehhez viszont már könnyedén hozzákötethetjük a panel frissítését. (Felmerülhet bennünk a kérdés, hogy miért nem a kliensoldali JavaScript timerét használjuk, de egyrészt így nem kell kilépnünk a megszokott ASP.NET-világból, másrészt aki már próbálkozott böngészőfüggetlen JavaScript előállításával, az sejtí, hogy miért is előnyös, ha ennek részletei elrejtí előlünk a keretrendszer.)

Aszinkron kommunikáció

A szerveroldali AJAX keretrendszer másik fontos eleme, hogy könnyebbé teszi a kliens- és szerveroldal aszinkron kommunikációját. Segítségével könnyedén hívhatunk webszolgáltatásokat aszinkron módon a kliensoldali scriptből. Ezek lehetnek olyan hívások, amelyek valamit lekérdeznak, vagy olyanok is, amelyek valamit elindítanak a szerveroldalon az oldal teljes újratöltése nélkül. Az ASP.NET AJAX oldalán részletes dokumentáció található (<http://ajax.asp.net/docs/default.aspx>), és ebben le van írva, hogy hogyan tudunk például ASMX webszolgáltatásokat meghívni.

Végezetül lássunk valami egzotikusát is: az ASP.NET-oldalak metódusait. A lényeg, hogy nem kell egy külön webszolgáltatás-osztályt felépítenünk, hanem az ASP.NET Page osztály metódusait jelölhetjük meg a [WebMethod] attribútummal (ne feledjük publikusként megjelölni a metódust!), amelyeket így egy egyszerű script segítségével már meg is hívhatunk. A 2. és 3. ábrán egy ilyen oldal kódját és a mögöttes C#-kódot láthatjuk.

Összefoglalás

Amint láthattuk a most megjelent ingyenes ASP.NET AJAX keretrendszer segítségével a megszokott ASP.NET programozási modellben élvezhetjük az AJAX előnyeit. Oldalaink működését elegánsabbá és gördülékenyebbé tehetjük a részleges frissítések segítségével, és az aszinkron kommunikációs lehetőségek új távlatokat nyitnak.

Minden érdeklődő webfejlesztőnek javasoljuk, hogy töltsse le a keretrendszert, és játsszon vele egy kicsit (jól működik a Visual Studio 2005 saját mini-webszerverével is). A dokumentációban található példák szemléletesek, és nagyon gyorsan megérthetők, így könnyen haladhatunk előre.

Nagy Levente
(nagy.levente@microsoft.com) Microsoft Magyarország

A MICROSOFT ÜZLETIINTELLIGENCIA- ESZKÖZEI

A Microsoft üzletiintelligencia-eszközei az alkalmazások széles körét támogatják, az egyszerű jelentéskészítéstől a vállalati teljesítményértékelésen keresztül a komplex pénzügyi elemző, tervező rendszerek kialakításáig.

Az üzleti intelligencia (Business Intelligence, BI) fogalma a kilencvenes években vált általánossá, a döntéstámogató, üzleti elemző rendszerek elterjedésével. Manapság olyan gyűjtőfogalomként használjuk, amely magában foglalja mindazokat az alkalmazásokat, technológiákat, amelyek lehetővé teszik az adatok üzleti információs célú felhasználását. Üzletiintelligencia-rendszeren pedig olyan komplex alkalmazást, megoldást értünk, amely gondoskodik az adatok összegyűjtéséről, üzleti célú felhasználásra kész tárolásáról, és tartalmazza az adatok információvá alakításához, felhasználókhöz juttatásához szükséges elemző, továbbító és megjelenítő funkciókat.

Az üzletiintelligencia-rendszerek legfontosabb építőelemei:

- az adatok strukturált tárolását, gyors elérhetőségét biztosító adattárházak, adatbázisok;
- az adatok hozzáférését, különböző rendszerekből történő kinyerését, tisztítását, a rendszerek közötti adatcserét támogató adatintegrációs, adattranszformációs és alkalmazásintegrációs rendszerek;
- az adatok üzleti elemzését támogató teljesítményértékelő, tervező, adatbányászati, statisztikai és egyéb általános célú adatelemző rendszerek;
- a vállalat egyes folyamatait, működését támogató speciális információkezelő és -elemző rendszerek.

Az üzletiintelligencia-rendszerek fejlődése az elmúlt néhány évben jelentősen felgyorsult. A hálózatok, a tárhelykapacitások és az információfeldolgozási sebesség jelenlegi szintje lehetővé teszi, hogy gigantikus mennyiségű adatot dolgozzunk fel, alakítsunk használható információvá, és továbbítsunk az adatok keletkezési idejét követően minimális idővesztéssel.

A versenyképesség, a piaci pozíció, a profitabilitás megőrzése vagy a versenyelőny megszerzése érdekében a vállalatok egyre nagyobb összegeket költenek üzletiintelligencia-rendszerek kialakítására. Ennek megfelelően a BI-eszközök gyártóinak kínálata is óriási. Ma már nem az a kérdés, hogy szükség van-e BI-rendszerekre, hanem az, hogy a vállalat folyamatait, tevékenységeit milyen BI-megoldásokkal támogassuk.

Az alábbiakban összefoglaljuk az üzletiintelligencia-rendszerek legfontosabb építőelemeit,

és bemutatjuk, hogy a Microsoft üzletiintelligencia-megoldásai hogyan támogatják a BI-rendszerek kialakítását.

Adatok, adathozzáférés, adattárházak

Minden üzletiintelligencia-rendszer alapját az üzleti adatok képezik. Az üzleti adatok általában nem egyetlen egységes rendszerben állnak rendelkezésre, hanem különböző forrásokból származnak, különböző formában léteznek, és nem egy időben keletkeznek.

A legerjedtebb és legmegbízhatóbb adattároló rendszerek a relációs adatbázis-kezelők, amelyek az adatok tárolását logikailag absztrakt, relációs adatmodell alapján oldják meg, az adatok lekérdezésére pedig az SQL nyelvet alkalmazzák. Sajnos különböző relációs rendszerek különböző SQL-szintaktikát, különböző adattípusokat, adatelérési interfészeket használnak. Az adatbázisok szerkezete ráadásul cseppet sem barátságos: az adatszerkezet legtöbbször bonyolult, sok a kódolt információ és nehézkes az adatok emészthető információvá alakítása.

A relációs adatbázisokon kívül minden vállalatnál számos egyéb belső és külső adat-

forrás van, amelyek általában egymástól elszeparáltan, redundánsan, más rendszerek számára nehezen hozzáférhetően tartalmazzanak fontos információkat.

Az üzletiintelligencia-rendszerek építésénél fontos feladat tehát az adatok kinyerése a különböző forrásrendszerekből, a hibák, elentmondások felderítése, tisztázása, az adatok egységes, összehasonlítható, elemezhető formátumba transzformálása.

Általánosan elterjedt megoldás erre az adatok betöltése az adattárházba. Az adattárház olyan strukturált adattár, amely az adatokat és azok időbeni változását az adatok elemzését támogató szerkezetben és formában tárolja. Az adattárház kisebb, funkcionális vagy az adatok szorosabb összetartozása szerint csoportosított szeleteit adatpiacnak nevezzük. A legelterjedtebb adattárház-megvalósítások egymással összefüggő relációs és multidimenziális adatpiacok kezelését teszik lehetővé.

A multidimenziális adatkezelés az adatok relációs szemlélettől eltérő, azok felhasználását közvetlenebbül támogató megoldás. A multidimenziális megoldásokban az adatokat dimenziók, attribútumok szerint csoportosíthatjuk, összesíthetjük és elemezhetjük, általában a relációs rendszereknél nagyságrendekkel gyorsabban és kényelmesebben.

A Microsoft az adatok kinyeréséhez, tárolásához, gyors és hatékony lekérdezhetőségének biztosításához minden szükséges eszközt a rendelkezésünkre bocsát. Tekintsük át a legfontosabbakat!

SQL Server 2005. A Microsoft üzletiintelligencia-rendszereinek alappillére, zászlóshajója az SQL Server. Az SQL Server ma már minden szempontból megfelel a kihívásoknak:

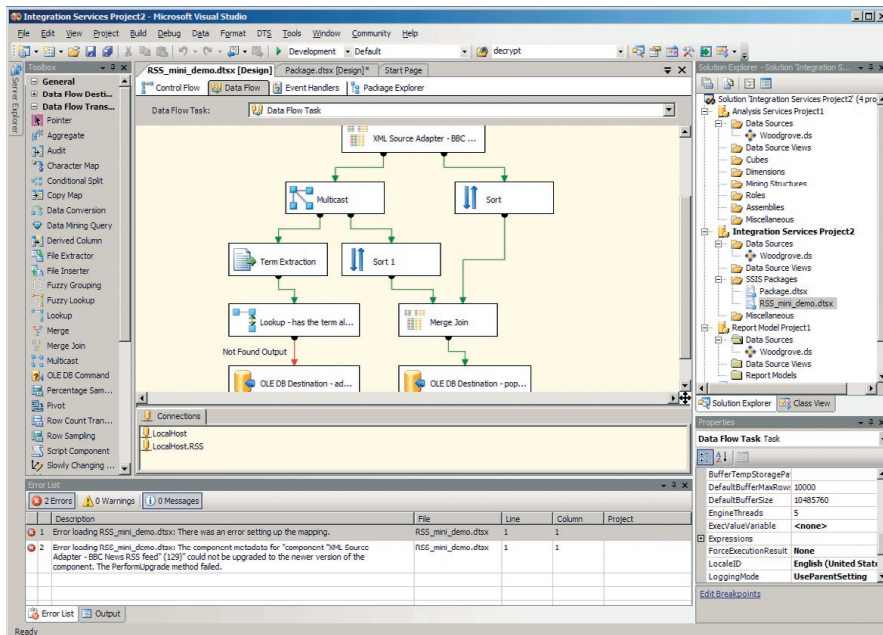
- a nagyon nagy adatbázisokat is hatékonyan kezeli (hatékony scale up, scale out modell, particionálás);
- folyamatos, megbízható működést biztosít (cluster, adatbázis-tükrözés, online karbantartás);
- valós idejű BI-megoldások adatkezelésére is alkalmas (snapshot-izoláció, indexelt nézetek, eseményértesítések);
- flexibilis adattárolást, adathozzáférést és adatfeldolgozást nyújt (XML, teljes szöveges indexelés, .Net-programozhatóság, webszolgáltatások);

- biztonsági rendszere megfelel az egyre szigorodó követelményeknek (biztonságos telepítési, frissítési folyamat, többszintű hozzáférés-szabályozás, adattitkosítás, PKI-támogatás);
- az osztott adatkezelést számos eszközzel támogatja (replikáció, osztott tranzakciók, particionált nézetek, távoli, osztott lekérdezések, csatolt szerverek).

Az SQL Server 2005 a kiváló osztott adatkezelési, adatelérési és programozható-

nyé a relációs adatpiacokkal szemben, hogy az adatokat nemcsak elemi szinten, hanem előre aggregált formában is tárolják. Az aggregációk az elemzési szempontok számát, számosságát, azok kapcsolatait és használatuk módját, gyakoriságát figyelembe véve készülhetnek el, így a jól felépített UDM nagyon gyorsan képes információt szolgáltatni.

SQL Server 2005 Integration Services (SSIS). Az SSIS olyan adatintegrációs eszköz, amely a hagyományos adatok különböző



1. ábra. SSIS-adatfolyam a BI Development Studióban

sági képességeinek köszönhetően relációs adattárházak, adatpiacok építésére valóban ideális választás. A tervezők nagy hangsúlyt fektettek az együttműködésre, az alkalmazásintegrációra, a különböző szabványok támogatására, így bármilyen környezetbe, vállalati architektúrába beilleszthető rendszert hoztak létre.

SQL Server 2005 Analysis Services (SSAS). Az SQL Server Analysis Services a multidimenziális adatpiacok, adattárházak építésének alapeszköze. Egyik legfontosabb eleme a Unified Dimension Model (UDM), amely az adatok multidimenziális strukturába szervezését teszi lehetővé. Az UDM a különböző tartalmú, formátumú, részletezettségű, összesíthetőségű és különböző szempontok szerint elemezhető adatok egységes rendszerbe foglalását támogatja.

Az SSAS alkalmazásával kialakított multidimenziális adatpiacok legfontosabb elő-

rendszerekből történő kinyerésére, feldolgozására és betöltésére szolgáló ETL (Extract, Transfer, Load) funkciókon túl az adatok tetszőleges transzformációját, érvényesítését, tisztítását, konszolidálását és az adatkezelés egyéb mellékmuveleteit (például adattovábbítás, tranzakció-kezelés, elő- és utómunkálatok, naplózás, kivételkezelés) is támogatja.

Saját munkafolyamat- és adatáramlási modellje van, amely a legbonyolultabb feladatok elvégzését is lehetővé teszi. Az SSIS viszonylag egyszerűen illeszthető be komplex rendszerekbe.

Az SSIS azonban nem „out of the box” megoldás: bár az egyszerű rutinfeladatokat néhány kattintással, varázslókból elintézhethetjük, a komplex megoldások kialakítása alapos tervezést és komoly fejlesztési munkát igényel. Az adatintegrációs csomagok fejlesztését viszont számos előre gyártott eszköz, munkaelem és adattanszformációs eszköz

segíti, így a fejlesztés magára az adatkezelésre és nem az eszközök megírására irányul, ami drasztikusan rövidítheti a projektek kivitelezési idejét.

BizTalk Server 2006. A BizTalk Server 2006 a Microsoft alkalmazásintegrációs nagygútyja. A BizTalk Server két alapfunkciója az üzenet alapú információáramlás megvalósítása („BizTalk Messaging”) és az üzleti folyamatok támogatása („BizTalk Orchestration”).

Az üzletiintelligencia-rendszerek kialakításánál elsősorban a speciális információkezelő, -elemző rendszerek (például ügyfélkapcsolat-kezelés, pénzügyi tervezés) és a vállalat egyéb rendszerei közötti adatsere indokolja a BizTalk Server alkalmazását. Azokban az esetekben, amikor az adatáramlás megvalósítása során bonyolultabb üzleti döntéseket kell hozni, számos különböző rendszert kell integrálni, és a folyamatok nyomonkövetése, változásaik kezelése kritikus fontosságú, az SSIS mellett célszerű lehet a BizTalk Server alkalmazása.

Hasonlóan az SSIS-hez a BizTalk Server sem azonnal használható termék, erős infrastruktúrális háttér, üzleti modellezési és fejlesztői ismeretek szükségesek az alkalmazásához.

Adatelemzés

Az üzletiintelligencia-rendszerek lelke az adatelemzés. Az adatok csak akkor válnak értékessé, ha sikerül azokat információvá alakítanunk. Az információvá alakítás az egyszerű kiemelésről, összeadástól a komplex üzleti elemzések, előrejelzések elkészítéséig terjed, és általában számos különböző eszköz használatát igényli. Az üzletiintelligencia-elemző rendszerek lehetnek általános célúak, amelyek számos különböző elemző funkciót tartalmaznak, vagy speciálisak, amelyek egy-egy terület, témakör igényeit fedik le.

A legegyszerűbb adatelemző eszközök a táblázatkezelő alkalmazások, amelyek az adatokkal végzett elemi műveleteket támogatják, kiegészítve számos statisztikai, matematikai, pénzügyi és egyéb elemző eszközzel. Az egyszerűség természetesen nem azt jelenti, hogy ezek az eszközök nem alkalmasak akár nagyon komoly elemző funkcionalitás megvalósítására, hanem inkább arra, hogy nagy mennyiségű adat feldolgozására önmagukban nem alkalmasak, és az alkalmazott elem-

ző funkcióik is csak bizonyos adatmennyiségig használhatóak.

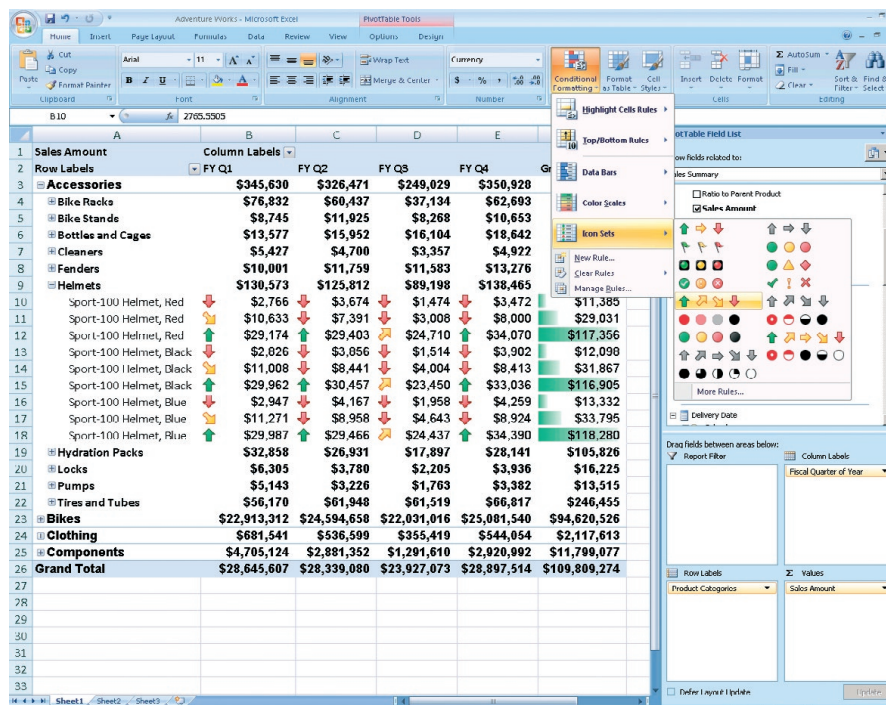
Az adatelemző rendszerek között kiemelkedő jelentősége van a multidimenziós adatkezelésre épülő OLAP- (Online Analytical Processing) rendszereknek, amelyek valós időben teszik lehetővé nagy tömegű adat összetett szempontrendszerek, számítások alapján történő elemzését. Egy másik jelentős terület az adatbányászat, amely statisztikai és matematikai eszközök, heurisztikus adatelemző algoritmusok, módszerek alkalmazásával segít az adatok összefüggéseinek feltárásában és előrejelzések készítésében.

A Microsoft elsősorban általános célú elemző eszközöket fejleszt, amelyek különböző igényeket hivatottak kielégíteni. Ezek közül kiemelkedik az Excel és az Excel Server, az Analysis Services és a hamarosan megjelenő Performance Point Server.

SQL Server 2005 Analysis Services (SSAS). A Microsoft legáltalánosabb üzletiintelligencia-elemző eszköze az SQL Server 2005 Analysis Services. Az SSAS számos le-

- kezeli az időbeni és egyéb speciális (például főkönyvi számla szerinti) összesítéseket;
- kalkulációs motorjával komplex számításokat végeztethetünk;
- KPI („Key Performance Indicator”) definícióinak segítségével elemezhetjük az üzleti teljesítményt, a trendeket, a célok megvalósulását;
- támogatja a „mi lenne, ha” típusú elemzéseket;
- egyszerűen megoldhatjuk a különböző mértékegységű, pénznemű adatok összehasonlítását, konvertálását;
- adatbányászati módszereket használhatunk az összefüggések feltérképezésére, az előrejelzések támogatására;
- előkészíti az adatok megjelenítését, a felhasználói interakciók kezelését (szerveroldali feltételes adatformátumok, akciók, többnyelvűség).

Általában az SSAS sem azonnal működő megoldás, de mind a Microsoft, mind más gyártók kínálnak kész vagy félkész SSAS ala-



2. ábra. Adatmegjelenítés az Excel 2007-ben

hetőséget kínál az adatok elemzésére, ezek közül néhányat példaképpen felsorolunk, bár a lista ennél sokkal hosszabb:

- automatikusan képes az adatok különböző összesítéseinek (összeg, átlag, elemszám stb.) elvégzésére;

pú megoldásokat a termékeikhez. Mielőtt egyedi fejlesztésbe kezdenénk, érdemes lehet ezért a piacon körülnézni, hátha van már számunkra használható termék, megoldás.

Performance Point Server, Business Scorecard Manager, ProClarity Analytics.

Amikor a Microsoft felvásárolta a ProClarityt, már sejteni lehetett, hogy ez egy tudatos stratégia része, és csak idő kérdése, mikor jelenik meg a cég saját márkanévvel ellátott üzleti elemző, tervező és monitoring-funkciókat ellátó terméke. A Performance Point Server, részben a ProClarity Analytics és a Business Scorecard Manager utódjaként, számos fontos területet fed le. A Business Scorecard Manager a vállalati értékelési rendszerek kialakítást segíti teljesítménymutatók, mutatórendszerek kialakításának, kezelésének és megjelenítésének támogatásával. A ProClarity Analytics pedig egy olyan professzionális adatelemző, megjelenítő eszköz, amellyel az SSAS alapú modelljeinket felhasználva és továbbfejlesztve interaktív, sokrétűen felhasználható elemzéseket, nézeteket hozhatunk létre, és ezeket számos eszközzel és formátumban jeleníthetjük meg.

A Performance Point Server egyesíti ezeket a funkciókat; egy olyan adatelemző, tervező és adatmegjelenítő platformot képezve, amely a vállalati teljesítménymérést, tervezést, az előrejelzések készítését, a pénzügyi jelentéskészítést, monitorozást támogatja. A Performance Point Server természetesen teljes mértékben integrálódik az SQL és az Office termékcsaládba, így az elemzések, modellek Excelben készíthetők, a jelentések Reporting Servicesbe publikálhatók, és a felhasználók egyszerűen, a SharePointon keresztül juthatnak azokhoz hozzá. A Performance Point Serverrel kialakított modelljeink központi tárolhatók, menedzselhetők és weben keresztül hozzáférhetők.

A Performance Point Server jelenleg CTP verzióban már elérhető a partnerek, valamint a leendő felhasználók számára, megjelenése pedig 2007 második, harmadik negyedévében várható.

Megjelenítés

Az üzletiintelligencia-rendszerek kritikus eleme a megjelenítés. Felépíthetjük a legjobb adatkezelőre alapuló professzionális adattárházat, feltuningolhatjuk a rendszert a legmodernebb elemző és adatbányászati eszközökkel, mindez semmit sem ér, ha nincs egy egyszerűen kezelhető, átlátható és megfelelően intuitív, interaktív megjelenítő felületünk.

Saját tapasztalatainkból is tudjuk, hogy sokszor egy ábra, egy jól összeállított grafikon sokkal többet mond, mint egy-egy

adatsor vagy többoldalnyi részletes táblázat. Ugyanakkor manapság azt is elvárjuk a megjelenítő felületektől, hogy szükség esetén egy adat, ábra vagy mutatószám mögöttes tartalmát is elérhetővé tegyék, és lehetőleg a kapcsolódó információkhoz is egyszerűen hozzá tudjunk férni.

A megjelenítés kapcsán azonban nem elég csak az információk tállására koncentrálni, hanem biztosítanunk kell az információkhoz való gyors és lehetőleg minél egyszerűbb hozzáférést is. Szükség van tehát olyan szervező,

Store	Automotive	Gardening	Electronics	Jewelry	Sporting	Housewares	Books	Toys
Store 1	14	Soft Assembly	65,960	17,843	34,834	26,263	43,644	27,239
Store 2	14	Soft Assembly	31,694	32,645	54,911	30,932	45,641	49,517
Store 3	4	Remove Filter from Gardening	19,642	69,934	48,752	41,483	47,924	27,523
Store 4	1	Number Filters	1,195	69,860	26,253	26,253	41,834	36,906
Store 5	1	Filter	174	41,895	27,950	43,622	53,434	
Store 6	1	Filter	565	12,656	31,122	16,476	45,324	
Store 7	62,709	41,227	801	63,866	62,230	25,990	49,025	
Store 8	63,956	26,447	781	26,337	24,357	47,634	30,248	
Store 9	65,473	25,602	721	18,512	19,083	54,070	44,914	
Store 10	14,232	48,615	015	24,495	61,290	22,279	13,188	
Store 11	21,491	40,961	393	52,132	39,146	69,504	53,377	
Store 12	14,783	47,626	108	59,154	16,484	33,724	58,118	
Store 13	40,703	24,893	423	14,276	62,370	15,641	44,794	
Store 14	16,569	41,464	391,367	50,486	56,332	43,124	22,814	11,995
Store 15	67,273	62,422	13,023	12,836	46,807	19,213	30,725	45,475

3. ábra. Excel a weben

kereső rendszerekre, amelyek a különböző forrásokból származó információkat integrálják, elérhetővé teszik.

Ezeknek az elvárásoknak nem könnyű eleget tenni. Egy-egy feladat, projekt kapcsán sok kérdést kell magunknak, ügyfelünknek feltennünk ahhoz, hogy megtaláljuk az egyes felhasználói csoportok, szerepkörök számára az ideális megoldást.

A Microsoft által kínált technológiák szerezésére szinte minden felhasználói igénynek meg tudnak felelni.

Excel 2007. Az Excel ideális általános célú megjelenítő és elemző felületet biztosít az SSAS UDM modelljeinkhez és relációs adatpiacainkhoz. Nagy előnye, hogy viszonylag kevés adat-előkészítő munka után gyorsan, látványos eredményeket érhetünk el vele, és a betanítással sem kell sokat bajlódunk. Mivel az Excel a legelterjedtebb táblázatkezelő rendszer, a felhasználók általában igénylik is, hogy az üzletiintelligencia-rendszert Excelből lehessen kezelni, vagy legalábbis támogassa azt. Az Excel 2007 a relációs, a multidimenzionális, valamint az XML adatforrásokkal egyaránt jól boldogul.

A megjelenítő funkciókat sokat javultak az

előző változathoz képest. Az új felület támogatja az SSAS szervertől formátumbeállításait, a KPI-k megjelenítését, flexibilisen állíthatjuk be a szűrőfeltételeket, és a feltételes formázással kiemelhetjük a lényeges információkat, vizuálisan megjeleníthetjük a trendeket, kivételeket. Újdonság, hogy az UDM-ben definiált akciók is elérhetők az Excelből, így további interaktivitást vihetünk a rendszerünkbe.

Az Excelt mint BI-ügyfélalkalmazást, eddig elsősorban azoknak a felhasználóknak javasoltuk, akik az adatok egyszerű megjelenítésén kívül azok sokrétű továbbfelhasználását és nagyfokú interaktivitást is igényeltek. Ez általában a BI-felhasználók szűkebb rétege. A felhasználást tovább korlátozta, hogy az Excel-táblázatok publikálása, karbantartása, adatfrissítése nem volt egyszerű feladat. Ma már azonban a funkciók jelentős része működik webes felületről, az Excel Servicesen keresztül is, így az eddigi alkalmazási lehetőségek kibővültek. Az Excel jól használható lett a távoli adatforrásokkal való munkára is, és a táblázatok karbantartása, publikálása is jelentősen egyszerűsödött.

SQL Server 2005 Reporting Services (SSRS). A Reporting Services a Microsoft jelentéskészítő, -publikáló és megjelenítő platformja. Az előre elkészített jelentések publikálása, online és offline használata mellett támogatja az ad hoc lekérdezések elkészítését és közzétételét is.

Az SSRS önállóan is használható megoldás, azaz nem szükséges hozzá az adatok adattárházba, adatpiacokba szervezése. Egy-egy jelentés akár több különböző adatforrásból származó adatokat is megjeleníthet, a jelentések összekapcsolásával pedig bonyolult, összetett riportokat készíthetünk, amelyek számos interaktív elemet is tartalmazhatnak (például összekapcsolt paraméterek, drill-down, drill-up, url-ek, könyvjelzők).

A Reporting Services kiválóan együttműködik az Excellel, és egyre több alkalmazáshoz készen kapjuk az SSRS-ben futtatható jelentéseket.

A Reporting Services kiváló „belépő szintű” eszköz ahhoz, hogy az üzletiintelligencia-

rendszereket beillesztjük a vállalati informatikai kultúrába. Implementációs ideje, erőforrásigénye viszonylag kicsi, és a licencdíjak is elég kedvezőek (az SQL Serverrel együtt licenccelődik). Az eredmény pedig kellően gyors és látványos ahhoz, hogy a döntéshozókat további beruházásra ösztönözze.

SharePoint Server 2007. Végül, de nem utolsósorban következzen a jéghegy csúcsa, az az építőelem, amellyel mindazt, amiről eddig beszéltünk, összefoghatjuk, és a felhasználó elé tárhatjuk.

A SharePoint Server 2007 számos egyéb funkciója mellett kiválóan használható a BI-megoldások keretrendszereként, portáljaként. A SharePoint 2007 az eddig felsorolt összes rendszerrel integrálható, sőt, számos esetben azok funkcionalitását további elemekkel egészíti ki. A teljesség igénye nélkül álljon itt néhány olyan szolgáltatás, amely nagymértékben leegyszerűsíti a BI-megoldások felhasználócentrikus kialakítását:

- Dashboards – egyszerűen összeállítható BI-portálterületek, amelyekben összegyűjthetjük, rendszerezhetjük a BI-építőelemeinket (Excel-munkafüzetek, KPI-k,

eredménytáblák, jelentések, adatelérési komponensek stb.);

- Excel Services – segítségével weben keresztül, interaktívan, programozhatóan és online kezelhetünk, oszthatunk meg Excel-munkafüzeteket;
- Data Connection Libraries – adatforrásokat publikálhatunk és oszthatunk meg, amelyeket azután a felhasználók az Office- vagy egyéb alkalmazásokban használhatnak;
- Business Data Catalog – a háttérrendszerek adatainak kódolás nélküli elérését, azok egyszerűbb felhasználását támogató kész komponensek;
- Report Center – a jelentések publikálását, rendszerezését és megjelenítését támogató, testre szabható portál-építőelem.

Összegzés

A Microsoft folyamatosan bővülő BI-eszköztára gyakorlatilag bármilyen üzletiintelligencia-megoldás kialakítását lehetővé teszi az egyszerű és olcsó jelentéskészítő rendszerektől egészen a bonyolult adattárházakra, adati- és piacokra épülő portál alapú elemző, tervező rendszerekig. Fontos azonban megjegyez-

nünk, hogy az eszközök önmagukban nem elegendőek ahhoz, hogy jól használható, valódi értéket teremtő rendszereket építsünk. A BI-rendszerek építésénél nemcsak informatikai, hanem igen komoly vállalatveze-



Az üzletiintelligencia-megoldások körképe

tési, pénzügyi és egyéb speciális szakmai ismeretekre is szükség van, ezért komolyabb rendszerek kialakításához mindenképpen érdemes BI-szakértőkhöz, például megfelelő kompetenciával rendelkező Microsoft-partnerhez fordulni.

Kovács Zoltán
(kovacs@szamalk.hu) vezető oktató, Számalk

TRÓJAI FALOVAK VISSZAFORDÍTVA A KAPUNÁL

MICROSOFT.HU/BIZTONSAG
Microsoft

Ismerje meg az üzleti biztonsági alkalmazások legújabb generációját, a betolakodók elleni küzdelem hatékony fegyverét, a microsoft.hu/biztonsag oldalon!

- ▶ **A Microsoft Forefront**
A Microsoft Forefronttal olyan üzleti biztonsági termékcsaládhoz juthat, amely a korábbiaknál átfogóbb, magasabb fokú védelmet biztosít, és tágabb szabályozási lehetőségeket kínál. Az ügyfélgépek, a kiszolgálói alkalmazások és a hálózat pereme számára egyaránt képes védelmet nyújtani.
- ▶ **Teljes körű szolgáltatás**
A Microsoft Forefront a teljes operációs rendszerre, minden alkalmazásra és kiszolgálóra kiterjedő védelmet és hozzáférés-szabályozást biztosít az Ön információi számára, így azok biztonságban lehetnek a folyamatosan változó fenyegetésektől.
- ▶ **Integrált**
Több területen fokozhatja a hálózata biztonsága feletti ellenőrzést, mivel a termékcsalád biztonsági képességeinek integrálása a Microsoft kiszolgálói alkalmazásaival és a meglévő informatikai infrastruktúrával jóval nagyobb hatékonyságot nyújt.
- ▶ **Egyszerű**
A biztonsági termékek felügyeletének, telepítésének és használatának egyszerűbbé tétele nagyban hozzájárul a szervezet biztonságának növeléséhez, és így Ön is egyszerűen bizonyosodhat meg arról, hogy folyamatosan a megfelelő védelemben részesül.

© 2006 Microsoft Corporation. Minden jog fenntartva. A Microsoft, az Antigen és a Windows Server logó a Microsoft Corporation bejegyzett védjegyei az Egyesült Államokban és/vagy más országokban.

Microsoft

FOLYAMATOSAN ÁRAMLÓ VÍZBEN

„Én meg mindig megpróbáltam a konvertálható tudás irányába mozogni” – interjú Szalontay Zoltánnal.

Bizonyára sokakat érdekel, milyen is az élet a Microsoft Magyarországnál, és hogyan dolgoznak rendszermérnökeink, szakembereink. Úgy gondoltuk, az a legjobb, ha ők maguk mesélik el! Az interjú lényegesen hosszabbra sikerült, mint amit két újságcikk között tudunk tenni – így a beszélgetés teljes szövege a TechNet Portálon található meg a <http://tinyurl.com/yw37l8> címen, ahol részletesen olvasható az is, hogyan alakult ki a mai TechNet programsorozat, és mitől voltak emlékeztetések a korábbi termékbejelentéseink.

TechNet: Hogyan és mikor kerültél a Microsofthoz?

Sz. Z.: 1995. szeptember 6. óta dolgozom a cégnél. Bár augusztus 20-a környékén „felvételiztem”, de akkor épp egy *Bill Gates* nevű úriember volt itt Magyarországon az Operaházban, ahol bejelentette a Windows 95-öt. Miután ez az egész hullám elült, és mindenki kialudta magát, szeptember első hetében álltam munkába.

TechNet: Mi volt az első komolyabb kihívás a számodra?

Sz. Z.: 1995 októberében vagy novemberében rendeztek meg egy Compfair kiállítást, ahol 40-50 gépet kellett Windows 95-tel telepítenünk igen rövid idő alatt. Ez már csupán a kiállító gép hardverszükségleteit tekintve is megrázó élmény volt: elég a 2 megabájt RAM-ot említeni – annak idején azért már a Win95 is nagyon szeretett 4 megabájt RAM-mal pörögni. Szerencsére volt néhány gépünk, amiben 6 meg 8 megabájt is volt! De azokban meg teljesen fölösleges volt ennyi memória.

Hozzávetőleg nyolc gyártó szállított le 50-60 gépet, és volt, amire feltelepíteni sem lehetett a Windows 95-öt. Úgyhogy egyet lehetett csinálni: egy óriási kettős könyvelős Excel-táblázatban gyári szám alapján vezetni, hogy melyik gépből szereltük ki melyik memóriamodult, hova tettük át, és működött-e. És arra nagyon büszke vagyok, hogy 50 darab 220-as elosztó kivételével azóta sem hiányzik semmi az egész standról.

TechNet: Hogyan indult útjára a TechNet programsorozat?

Sz. Z.: *Zsoldos Sanyi* kollégánk külföldi ötletre indította be azt a kezdeményezést, ami a későbbi TechNetet alapozta meg. Ennek igazából az volt a lényege, hogy összeraktuk az összes kliens- és szervertermékünket, mind a nyolcat (BackOffice: NT4 Server, Workstation, SMS, SQL Server, Mail szerver – talán ekkor már Exchange volt a neve), és ehhez tartozott még a kliensoldal (Office, Windows) is, és rátettük ezeket néhány CD-re. A termékeket egy képzeletbeli vállalat (Galaxis Irodatechnika Kft.) életével mutattuk be. Az eseményt követően a termékeket fél évre odaadtuk az ügyfeleknek, partnereknek, hogy próbálják ki ezeket a szoftvereket szabadon, majd megkérdeztük róla a véleményüket, mennyire tetszettek nekik a termékek, szeretnék-e használni azokat a jövőben. Nagyon kevés leányvállalat tudta elintézni annak idején, hogy saját CD-gyártásba fogjon. Ez annyira bevált, hogy rendszeresítettük az eseményeket, és kiszélesítettük a meghívottak körét.

TechNet: Milyen volt a legutóbbi TechNet, amit tartottál?

Sz. Z.: A legutóbbi, amin részt vettem, a 2006 májusi Windows Vista TechNet volt. Megjegyzem, ma már nem lenne kunszt megtartani egy ilyen eseményt. Akkor viszont



Szalontay Zoltán

igazán nem volt még információnk az eléggé bétaállapotban lévő Vistáról.

Konkrétan alig működött valami, nem volt információnk sem elég – majd az utolsó utáni pillanatban kaptam egy kis 300 oldalas doksit, xps-formátumban, amit akkor még

XP-n nem könnyen lehetett megnyitni. Az én gépemen például egyáltalán nem. Néhány hét alatt meg lehetett volna szerezni a doc-formátumot is, de az nekem már rég késő volt. Úgyhogy szinte minden külső segítség nélkül kellett felkészülnöm.

A szokásos magyar módszert alkalmaztam. Dokumentáció birtokában, ugye, nem nagy kaland megismerni egy terméket, tréninggel még könnyebb. De ezek hiányában az első és egyben legizgalmasabb feladat az, hogy kitaláld, mit is akar csinálni ez a szoftver valójában. Amikor neked kell kitalálni, hogy melyik gomb, melyik funkció mire való, hogy áll ez össze egy rendszerré. És előjönnek persze új fogalmak is: például a People Near Me. És ilyenkor csak úgy a nevéből saccolom elsőre, hogy People, meg közel, és akkor beregisztrálok egy kis felhőbe, és akkor biztos történik valami, de ezt egy még nem működő szoftveren találd ki, és csinálj belőle jó demót. Szép kihívás!

TechNet: Mi volt a legemlékezetesebb számodra a Microsoftnál töltött idő alatt?

Sz. Z.: Egyértelműen a Windows 2000 bejelentése. BNV, F pavilon, körülbelül 2000 néző. Az itteni karrieremnek szerintem a legszebb pillanata volt, nagyon élveztem. Kitaláltuk *Tarsoly Bazsával* – mert mókázni mindig is szerettünk –, hogy az egyik demóban direkt elrontjuk az egyik gépet. Kikapom a vinyót, és ott hadonászok vele, majd az kicsúszik a keretből, 3 métert repül és összetörik. Jaj! És akkor most adatvesztés van... De nem baj, mert jön a meg nem nevezett hardverszállítónk szervize, és tényleg kicsomagol egy teljesen szűz gépet, majd RIS, Group Policy és Roaming Profile stb. használatával visszaállt a gép tíz percen belül.

Látnotok kellett volna azoknak az arcát, akik az első sorban ültek, és teljesen komolyan ledöbbenek. Erre persze mi még egy kicsit rá is játszottunk: megkérdeztem Balázstól, hogy van-e valami jó kis fejadász ismerőse, mert ez itt most nagy bukta. És persze az sem volt mellékes, hogy ezt nem mondtuk el *Vityi Péternek* sem, aki ott állt végig oldalt. Jó kis móka volt.

TechNet: Melyik a kedvenc technológiád a Windows Vistában?

Sz. Z.: Kedvenc Vista-technológiám? Lássuk csak... Talán a Desktop Search. Meg van egy olyan érdekes Windows Explorer-beállítás is – ezt a héten találm meg –, hogy

Tools, Options, ott, ahol a rejtett fájlok megjelenítését lehet beállítani legalul, a legalsó az angol verzióban.

Ott van egy új rádiógomb. Az alapértelmezett beállítás az, hogy begépeléskor legyen autoselect, vagyis ugorjon oda arra a fájlra a kijelölés, amit éppen begépelek. Persze ez nekem nem volt túl hasznos, elvégre úgyis mindig olyan nézetben vagyok, hogy az fájlnev szerint van szortírozva, egyszerűen odakattintok, odascrollozok, és kész. Viszont van egy olyan kombináció is (ez a felső opció), hogy amit én gépelek, az automatikusan kerüljön be a keresőmezőbe is, vagyis keressen rá arra a mintára, amit beírok. Tehát amit gépelek, arra egyből keresek. Ha kellően lassan gépelek, akkor már entert sem kell nyomnom. Tehát ablak+E, azt mondom, hogy RMS, azt mondom, hogy ügyfél neve, és az összes vele kapcsolatos levelezés, doksik, minden bejön, úgy, hogy entert sem kellett nyomnom, semmit, csak gépelnem, amit akarok. Nekem ez spórolja meg a legtöbb időt.

TechNet: Mivel foglalkozol mostanában?

Sz. Z.: Jelenleg azon dolgozunk, hogy a magyar nagyvállalatok informatikai rendszerét segítsünk modernizálni, és erre szerencsére van egy jó kezdeményezésünk, illetve modellünk, az Infrastructure Optimization (IO), aminek része, hogy a vállalatokat számtalan kérdéssel árasztjuk el az informatikájukkal kapcsolatban, majd az ezekre adott válaszokat rögzítjük és kiértékeljük. Ebben nekem leginkább az tetszik, hogy procedurális lesz a munkám. Tehát nem teljesen ad hoc – ideröppenünk, odaröppenünk a cégekhez –, hanem leválogatás alapján össze lehet gyűjteni azokat az ügyfeleket, akiknek hasonló problémájuk van, hasonló infrastrukturális fejlettségen vannak. És hasonló jellegű dolgok válhatnak meg őket, tudnának hasonló dolgokon spórolni, a meglévő technológiák alkalmazásával.

Még az is lehet, hogy ott van már náluk a termék, csak még nem – vagy nem megfelelően – használják. Ilyenokról szól ez az IO. Nagy előny, hogy nem az ismeretlenbe megyek végre, hanem már van egy pontos profil a cégről, és így sokkal hasznosabb tanácsokat tudok én is szolgálni a számukra.

Az ügyfeleknek ebben az a jó, hogy többnyire a már megvásárolt technológiákból építkezve javaslunk nekik megoldásokat, hogy hogyan lehet olcsóbban üzemeltetni a

rendszerüket. Ezenkívül képbé tudják helyezni magukat, hogy mégis, a többi nagyvállalathoz képest ők hogyan állnak. Tehát iparági átlagokat lehet képezni. Persze ez az egész program akkor ér valamit, ha rendszeresen, sokáig csinálják, és nem változnak a kérdőívek negyedévente – vagyis, ha nem mozgó célpontra lövünk, hanem rendelkezésre áll egy stabil metodológia.

TechNet: Miért szeretsz itt dolgozni így tíz év után is?

Sz. Z.: Meleg van, internet van... dehogyan is. Otthon különben is gyorsabb... Hogy miért szeretek itt dolgozni? Most aktuálisan Principal Technical Specialist a funkcióm, ennél magasabb a szakmai vonalon nem nagyon van.

Ami nekem ebben a pozícióban tetszik, az az, hogy változatlan feltételek mellett, gyakorlatilag a Windows operációs rendszerért és az infrastruktúráért felelek. Állító helyemben is folyamatosan áramló vízben vagyok. Tehát folyamatosan jönnek az újdonságok. Négy évvel ezelőtt ki beszélt itt például virtualizációról? Sokkal jobban rálátunk ezekre a többi

További információ

Az interjú teljes, eredeti szövege megtalálható a <http://tinyurl.com/yw37l8> címen.

munkahelynél. Jobban rálátunk a hardverek fejlődésére, a szoftvertrendekre, hamarabb hozzáférünk az új szoftverekhez, technológiákhoz...

Voltam vevő, sőt, 10 évig fejlesztő is! Az, mondjuk, nagyon tetszett. Csak úgy harmincéves koromban elgondolkodtam: kelle-e a világnak egy 55 éves Szalontay Zoltán, baromi jó fejlesztő, háromszor drágább, mint egy friss srác. És nem, nem, szerintem nem kell. Vesznek 3 vagy 3 és fél darab egyetemistát. Tehát az nem értékálló tudás. Én meg mindig megpróbáltam a konvertálható tudás irányába mozogni. Ez pedig számomra a Windows.

A másik, ami nagyon sokat jelent, az az ügyfeleink visszajelzése, elismerése egy-egy előadás, projekt vagy beszélgetés után. Ha tudunk nekik lökést adni, fel tudjuk kelteni az érdeklődésüket, hogy elinduljanak az új technológiák megismerésében. Ez az igazi kihívás a számomra, és emiatt éri meg igazán ezzel foglalkozni.



BI

MI FELTESSÜK
A BI-RE A PONTOT.

BUSINESS INTELLIGENCE (BI) TANFOLYAMOK A NETACADEMIÁNÁL!

A sikeresen működő vállalatok versenyképességének egyik titka, hogy tudatosan használják, elemzik és értelmezik a rendelkezésükre álló adatokat. Az ehhez szükséges üzleti intelligencia (BI) technikai háttere minden SQL Server vásárlónál elérhető, bevetésre készen áll, hisz benne van a termékben. Itt az ideje, hogy használjuk is!

BI-képzéseinken az alábbi kérdésekre adunk választ:

- ◆ Mire használható egy többdimenziós OLAP kocka?
- ◆ Miként használható jól a Reporting Services 2005?
- ◆ Mik az újdonságai az Analysis Services 2005-nek?
- ◆ Mit csinál az Integration Services 2005?

A képzések már elkezdődtek!

2007-ben a NetAcademia szolgáltatja a hiányzó dimenziót.

További információk:

[HTTPS://WWW.NETACADEMIA.NET/BI](https://www.netacademia.net/bi)

LEGYEN ÖNNEK IS OLCSÓBB!

Képzéscsomagjainkat 2007-ben 20%-kal olcsóbban **keretszerződésben** is megrendelheti. Keretszerződéses partnereink számára további érték növelt szolgáltatásokat nyújtunk:

- ◆ Ingyenes tanfolyami utókövetés
- ◆ Ingyenes szaktanácsadás, egyedi konzultáció
- ◆ Ingyenes vizsgafelkészítő kit
- ◆ Ingyenes EU-pályázatfigyelés és tanácsadás

A keretszerződéssel kapcsolatban keresse
Szántó Zoltánt

E-mail:

SZANTO.ZOLTAN@NETACADEMIA.NET



NetACADEMIA

A LEGJOBBAKAT TANÍTJUK.

Cím: 1062 BUDAPEST, ANDRÁSSY ÚT 62.

TELEFON: (06 1) 472-1214
IRODAI MOBIL: (06 20) 369-6947
FAX: (06 1) 472-1215

INTERNET: WWW.NETACADEMIA.NET
E-MAIL: INFO@NETACADEMIA.NET

Neked lehetőség. Nekünk kihívás.™

Microsoft

MICROSOFT SYSTEM CENTER NAGY DOLGOKRA KÉPES!

A Microsoft System Center termékcsaládja az IT rendszerfelügyeleti megoldásokat fogja össze (a család része a megújult Operations Manager és a Systems Management Server is). A System Center termékek segítségével az informatikusok munkája könnyebbé és hatékonyabbá válik, még a legnagyobb vállalatok informatikai infrastruktúrája is könnyedén felügyelhető vele.

A jól felügyelt rendszer pedig segíti a vállalat felhasználóit is mindennapi munkájuk elvégzésében – az IT végre igazán stratégiai eszközzé válik.

www.microsoft.hu/systemcenter