TechNetKlub

magazin

2010.DECEMBER

Tartalomjegyzék

Távoli elérés megvalósítása VPN reconnect-tel

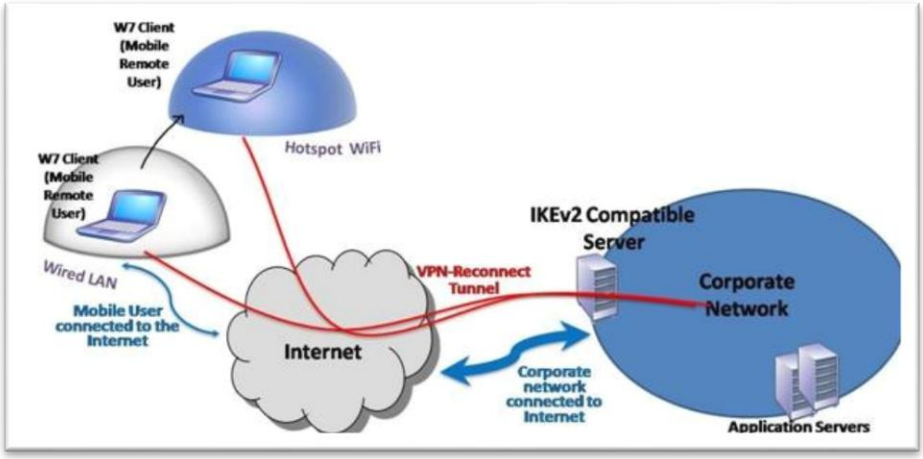
Milánovics Krisztián

MCSA, MCSE, MCTS, MCITP EA, MCITP SA

A különböző munkakörnyezetek fejlődésével párhuzamosan kialakult annak követelménye is, hogy a felhasználók immáron ne csak a belső hálózatról, de minden egyéb tartózkodási helyről is elérhessék a céges állományokat és szolgáltatásokat. Ezzel a rövid kis cikkel a Windows Server 2008 R2 megjelenésével debütált VPN Reconnect szolgáltatásról, és annak üzembe helyezéséről szeretnék egy áttekintő, technikai összefoglalót adni.

Az alapkoncepció

Igen, itt rögtön meg is lehetne jegyezni, hogy: „de már idáig is volt három választásunk VPN hálózatok kialakítására”. És ebben mindenkinek tökéletesen igaza is van. Ott volt – illetve van – a PPTP, LT2P/IPSec és a Vista SP1-gyel megjelent SSTP is. Én magam sokszor használtam és használom is ezeket a megoldásokat, többnyire segítették is megvalósítani a célt, amiért egyáltalán üzembe helyeztem őket. Amiért azonban sokan nem szeretik őket, talán az, hogy egyrészt a felhasználónak magának kell gondoskodnia a csatlakozásról, másrészt amennyiben az internetkapcsolat megszakad, az egész VPN kapcsolatot manuálisan újra fel kell építeni. Lényegében erre a problémára szeretne megoldást találni a VPN reconnect. Alapjába véve ez egy IPsec tunnel módra épülő megoldás, mely az „IKEv2 Mobility and Multihoming Protocol” (MOBIKE) használatának segítségével változtatja meg az „alagút” felhasználó felöli végpontját abban az esetben, ha a felhasználó átvált egy másik internetkapcsolatra. Természetesen ha egy LAN hálózat kábelét kihúzzuk, majd átváltunk egy WiFi hotspotra, fizikai értelemben a kapcsolat egy időre nyilván megszűnik. És itt jön a trükk: a helyett, hogy evvel a VPN kapcsolat is véget érne, egyszerűen átvált „Dormant” módba, és mindaddig vár, még újra képes kapcsolatot létesíteni az RRAS szerverrel. Ha ez ismét teljesül, a VPN kapcsolat újra felépül, és gyakorlatilag ott folytatódik, ahol a váltás előtt abbamaradt.



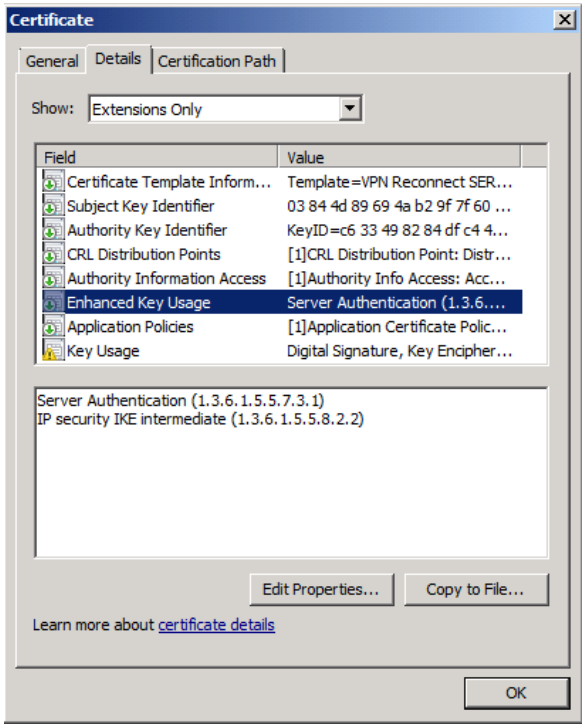
ábra 1: Az alapkoncepció

Technikai megvalósítás

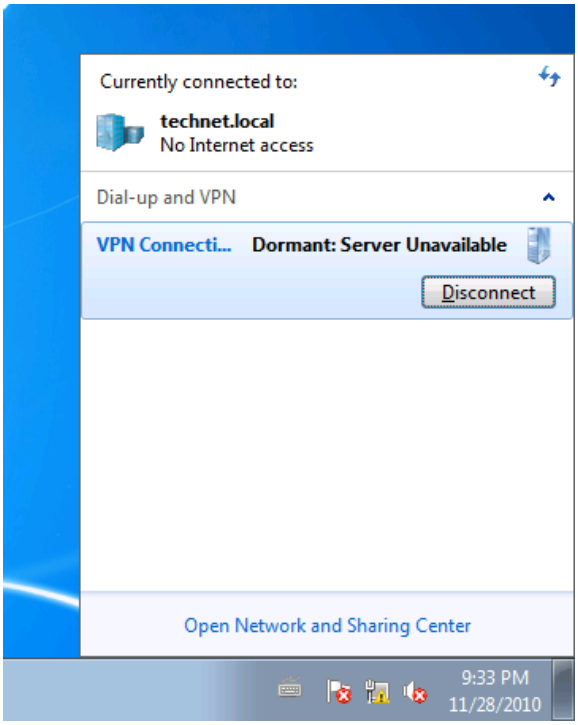
Az egész megvalósításához szerencsére nagyon sok mindenre nincs szükségünk. Amint sejthető, kell egy RRAS szerepkörrel felvértezett, kizárólag Windows Server 2008 R2-t futtató masina, magához a VPN Reconnecthez pedig egy számítógép tanúsítvány. Fontos, hogy evvel a tanúsítvánnyal kapcsolatban két dolognak kell teljesülnie:

- Igényléskor a „Name” mezőbe azt az FQDN nevet írjuk, amellyel kívülről érjük el a szervert. Abban az esetben, ha a tanúsítvány egy belső névre szól, a kapcsolat nem fog felépülni.
- A másik pedig, hogy a tanúsítvány Enchanced Key Usage (EKU) mezejében két dolog szerepeljen: az „IP security IKE intermediate” és a „Server Authentication”. Ezt talán a legegyszerűbb úgy megvalósítani, hogy a Certificate Templates konzolban duplikáljuk az IPsec templatet és az így létrejött másolatot egyrészt elnevezzük VPN Reconnect-nek, valamint az EKU mezőbe felvesszük a Server Authenticationt (a másik eleve ott lesz, mert az IPsec tanúsítvány tartalmazza).

Ha evvel elkészültünk, már csak a „Network Policy and Access Services” szerepkör telepítésére van szükség. A telepítés befejeztével a „Routing and Remote Access” konzolban a VPN szerverre jobb klikket kattintva a „Configure and Enable Routing and Remote Access” varázsló segítségével már könnyedén üzembe helyezhetjük magát a VPN szolgáltatást.



ábra 2: A tanusítvány EKU-ja



ábra 3: Dormant mód

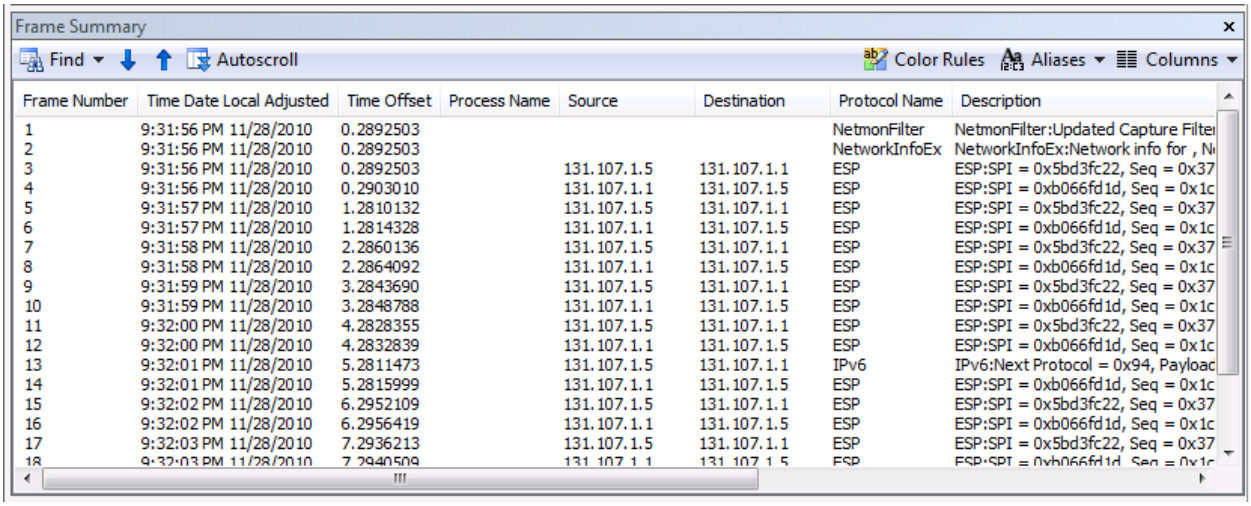
Authentikáció

A VPN megoldások kialakításánál mindig felmerül a hitelesítés és az azt körülvevő problémák kérdése. A VPN Reconnect használatakor vagy a számítógépet (tanúsítvány), vagy a felhasználót (jelszó és tanúsítvány alapon) hitelesíthetjük. Amennyiben az elsőt, akkor attól függetlenül, hogy éppen melyik felhasználó indítja a csatlakozást, semmiféle hitelesítésre nem lesz szükség, egyszerűen a connect-et megnyomva a VPN kliens csatlakozik. Ehhez egy „Client" tanúsítványt kell igényelni a kliens gép részére, valamint a számítógép tanúsítvánnyal való hitelesítését külön engedélyezni kell a VPN szerveren. A felhasználói hitelesítésnél választhatunk jelszó (EAP-MSCHAPv2), illetve tanúsítvány alapút, ahol a felhasználó tanúsítványát tárolhatjuk akár a profiljában, akár smart kártyán.

Összehasonlítva más megoldásokkal

Ebben a végső pontban két összehasonlítást emelnék ki: az LT2P-t, mivel mindkét megoldás IPsec-re épül, illetve a DirectAccess-t, a mobilitási „képessége" miatt. Ahhoz, hogy a VPN Reconnectet az L2TP-vel összehasonlíthassuk, fontos tudni, hogy az L2TP használatakor először egy számítógép authentikáció történik, **amit követ** egy felhasználói hitelesítés. Mivel a számítógép hitelesítése kötelező, ez azt jelenti, hogy az összes kliens gépre telepíteni kell egy számítógép tanúsítványt, ami jóval megnehezíti az L2TP bevezetését. Másrészről tudjuk, hogy a VPN Reconnecthez hasonlóan a DirectAccess is a háttérben újracsatlakozik, ha a felhasználó Internet elérést vált (vagy csak szimplán megszakad a kapcsolat), ám bevezetéséhez IPv6 infrastruktúra szükséges, és ami számomra talán még fontosabb, hogy a számítógép mindenképpen tartománytag kell, hogy legyen (hisz csoportházirenden keresztül kapja a DirectAccess beállításokat). Ez megint csak elénk tár egy igen nagy akadályt, mivel koránt sem garantálható, hogy az összes olyan számítógép, amelyről a felhasználóknak távoli elérést kell biztosítanunk egyáltalán látott már életében Active Directoryt. Összevetve tehát számos távoli elérést biztosító megoldás áll jelen

pillanatban egy rendszergazda rendelkezésére, nyilvánvalóan a döntését mindenki a különböző körülményeknek megfelelően fogja meghozni, ám az biztos, hogy a VPN Reconnect személyében egy gyorsan bevezethető, kényelmesen használható, ámde biztonságos megoldást kapunk.



ábra 4: IPsec ESP csomagok áramlása a hálózati adapteren

Hyper-V – Dinamikus memória alapok

Liszák Gábor

Magyar Posta Zrt.,
Rendszermérnök

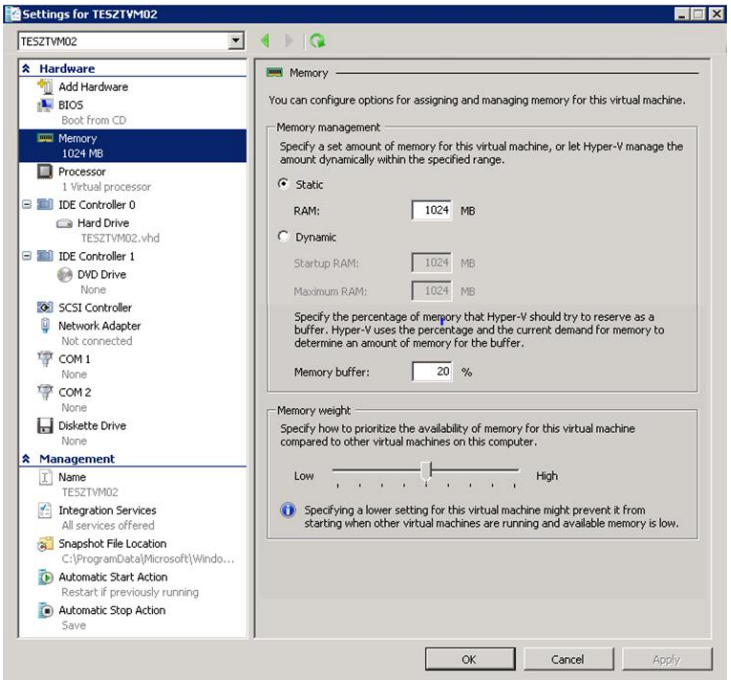
A Windows Server 2008 R2 Service Pack 1 telepítése után, a Hyper-V szerepkörének képességei között megjelenik a dinamikus memória konfiguráció. A dinamikus memória lehetőséget ad arra, hogy a virtuális gépeink számára szükség esetén több memóriát biztosítsunk automatikusan, a szerver leállítása nélkül. Az új képesség használatával több virtuális gépet futtathatunk a hoszt kiszolgálón, gazdaságosabb memóriahasználatot érhetünk el, és felkészülhetünk a gépeink változó erőforrásigényeinek hatékony kiszolgálására.

A korábbi (SP1 előtti) verzióban a VM-ek számára allokált memóriamennyiség egy fix érték volt, amelyet a virtuális kiszolgáló teljes egészében lefoglalt a fizikai memóriából. A memória mennyiségét kizárólag a gép leállítása után módosíthattuk. A fizikai memória egy kulcsfontosságú paraméter, amely meghatározza a hoszton futtatható virtuális gépek darabszámát. A gyakorlatban, legtöbb esetben ez a szűk keresztmetszet. Nem egyszerű feladat méreteznünk egy adott gép memóriaszükségletét. Produktív környezetben kénytelenek vagyunk az előforduló *legrosszabb* (legtöbb memóriát igénylő) esetre felkészülni, akkor is, ha ez az erőforrásigény csak bizonyos időpontokban, időszakokban jelentkezik. A dinamikus memória használatával lehetőségünk nyílik egy optimálisabb memóriahasználat elérésére, a legjobb teljesítmény megtartása mellett.

A dinamikus memória működési elve

A Hyper-V hoszt és a megfelelő, *virtualizációt ismerő* (enlightened) operációs rendszert futtató virtuális gép folyamatosan kommunikál egymással, annak érdekében, hogy meghatározzák a VM aktuális memóriaszükségletét. Amennyiben a virtuális gépünk erőforrásigénye növekszik, a hoszt automatikusan több memóriát biztosít számára. Amennyiben az erőforrásigény csökken, vagy egy magasabb prioritással konfigurált virtuális gépnek több memóriára van szüksége (és a rendelkezésre álló fizikai memória elfogyott), a hoszt csökkenti a gép számára biztosított memória mennyiségét.

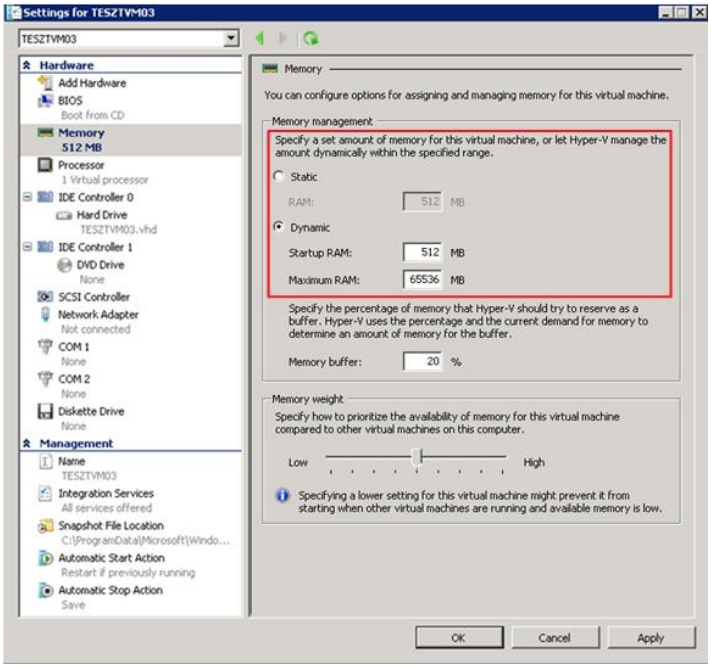
A szervizcsomag telepítése után a virtuális gépek beállításlapján, a memóriakezelés alatt az alábbi ablak jelenik meg:



ábra 5: Settings

Választható memóriakezelés

A **Memory management** rész alatt az alábbi konfigurációs lehetőségek jelennek meg:



ábra 6: Memory management

Static: Statikus memóriahasználat. Ezen lehetőség kiválasztásával nem engedélyezzük az adott virtuális gépen a dinamikus memóriahasználatot. A Hyper-V, az itt megadott memóriamennyiséget osztja ki a VM

számára induláskor. Az érték menet közben nem változik, kizárólag a gép leállítása esetén módosítható. A beállítás megegyezik az SP1 előtti memóriakezeléssel.

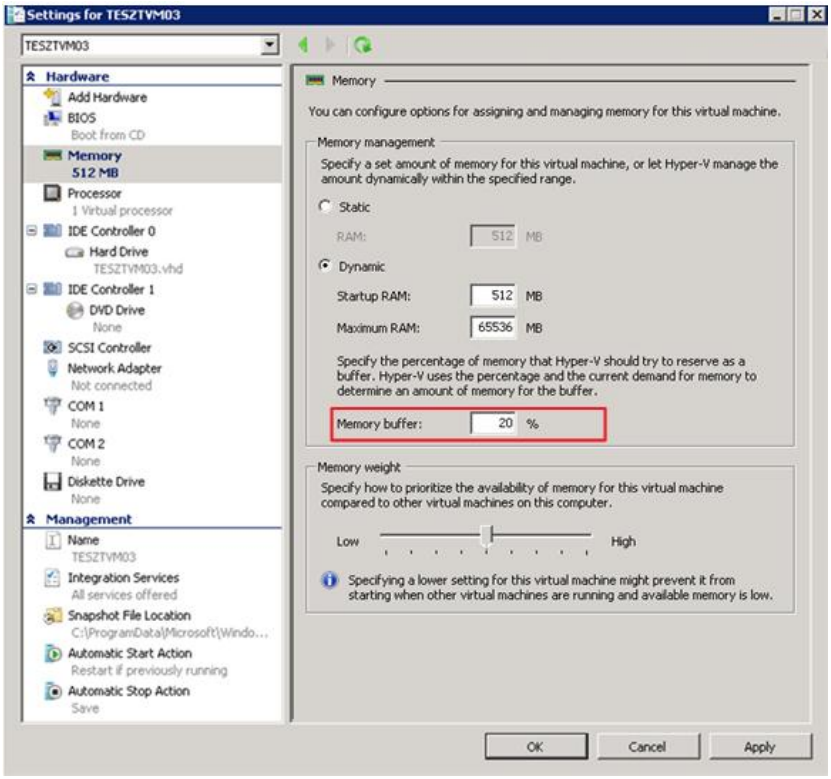
Dynamic: Engedélyezzük a dinamikus memóriahasználatot. Amennyiben ezt a beállítást választjuk, meg kell adnunk a kezdeti memóriamennyiséget (Startup RAM) és a maximális memóriamennyiséget (Maximum RAM).

> **Startup RAM**: A virtuális gép indulásakor ez a memóriamennyiség kerül kiosztásra és a memória soha nem mehet ezen érték alá. (alapértelmezett érték 512 MB).
>
> **Maximum RAM**: Ez a virtuális gép számára kioszthető maximális memóriamennyiség (alapértelmezett érték 65536 MB).

Amennyiben a beállítást olyan virtuális gépen engedélyezzük, amelyiken a dinamikus memóriahasználatot nem támogató operációs rendszer fut, a Hyper-V a Startup RAM alatt megadott memóriamennyiséget allokálja a VM számára induláskor, mint statikus memóriamennyiség. A beállításokat a gép leállítása után módosíthatjuk.

Buffer

Dinamikus memóriakezelés használata esetén a Hyper-V, a VM-be telepített teljesítményszámlálókon keresztül folyamatosan figyeli az aktuálisan használt memóriamennyiséget, és ennek függvényében határozza meg a virtuális gépünk memóriaszükségleteit. A Hyper-V által számított memóriaszükséglet a gépünk által használt aktuális memóriamennyiségből és további tartalék memóriából (buffer) tevődik össze. A tartalék memória mennyiségét virtuális gépenként konfiguráljuk, és százalékos értékben adjuk meg.



ábra 7: Memory buffer

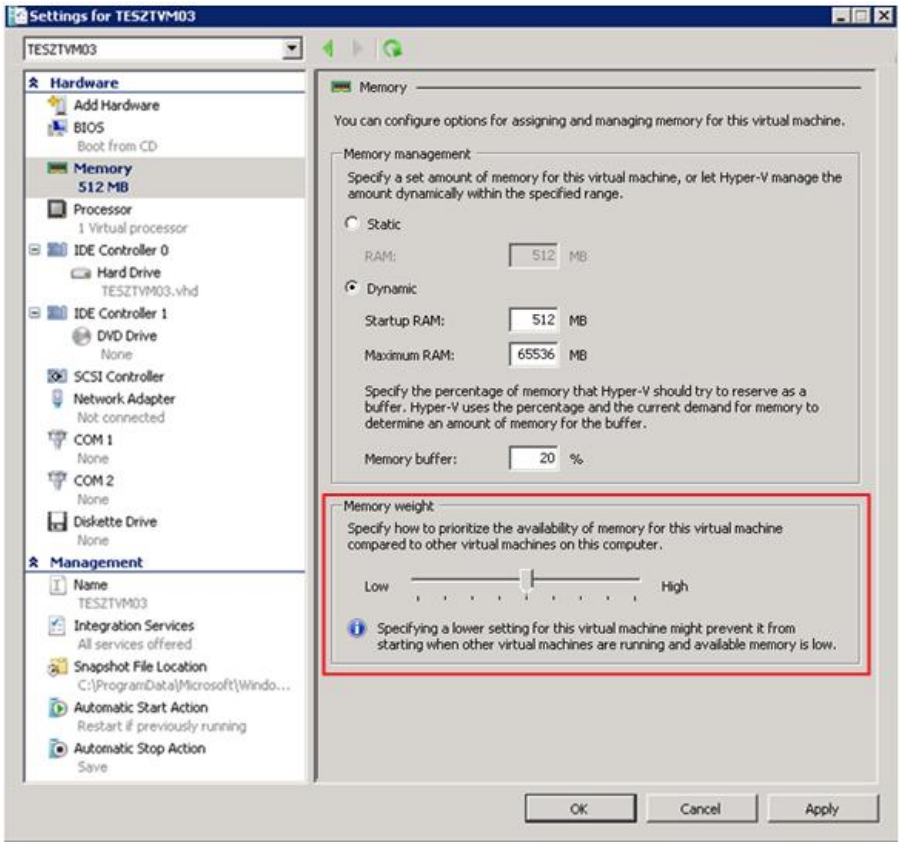
A virtuális gép számára kiajánlott összes memória értékét, a bufferbeállítás függvényében az alábbi képlet határozza meg:

Virtuális gép memóriája = aktuálisan használt memóriamennyiség + buffer [%]

Például: ha a VM aktuális memóriaszükséglete 2000MB és a buffer értékét 20%- ra állítjuk akkor a virtuális gép számára 2400MB memóriát fog allokálni a hoszt. Természetesen a **Maximum RAM** alatt definiált értéket nem haladhatja meg. A buffer értékét az adott virtuális gépünk és az azon futó szolgáltatás memóriahasználatának szokásaihoz kell igazítanunk.

Súlyozás

Ez a képesség kizárólag akkor jön a képbe, ha a hoszt összes rendelkezésre álló fizikai memóriája elfogyott. Amennyiben van szabad fizikai memória, úgy a virtuális gépeken megjelenő memóriaigény abból kerül kielégítésre. Amikor nincs elég fizikai memória a virtuális gépeket futtató kiszolgálón, és egyszerre több VM-nél jelentkezik a többletmemória igény, a Hyper-V-nek el kell tudni döntenie melyik gép(ek) igényeit szolgálja ki. Ebben segíti a memória prioritás. A csúszka az alacsony (Low) és a magas (High) közötti tartományban mozgatható relatív érték.



ábra 8: Memory weight

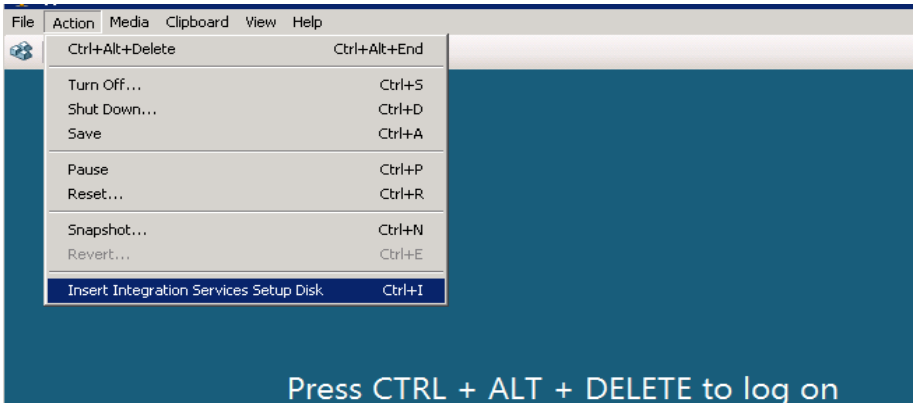
A memória prioritás a következőket befolyásolja:

- A Hyper-V először a magasabb súlyozással rendelkező gépeket szolgálja ki, számukra biztosítja többletmemóriát.
- Magas súlyozással konfigurált gépek többletmemória szükséglete esetén, a legalacsonyabb súlyozással rendelkező géptől fog először memóriát elvenni (természetesen, ahogy ezt már korábban is hangsúlyoztuk, erre csak akkor lesz szükség, ha a hoszt összes fizikai memóriája kiosztásra került).

A szervizcsomag telepítése

Upgrade esetén, a hoszton futó gépek beállításai alatt, a korábban (SP1 előtt) konfigurált memóriamennyiség a Static RAM mezőben jelenik meg. Tehát frissítés után a dinamikus memóriahasználat automatikusan nem lesz engedélyezve.

A Windows Server 2008 R2 SP1 telepítése után a virtuális kiszolgálóinkon telepítsük újra az Integration Services-t.
A VM **Virtual Machine Connection** ablakában kattintsunk az **Insert Integration Services Setup Disk** lehetőségre az **Action** menüpont alatt, majd a szerverre belépve kövessük végig a telepítés folyamatát (amennyiben Windows 7 vagy Windows Server 2008 R2-t futtatunk a virtuális gépünkön, az is megfelelő, ha itt is telepítjük az SP1-et).



ábra 9: Insert Integration Services Setup Disk

A szervizcsomagnak egyelőre a Release Candidate (RC) változata érhető el.

Letöltés: http://technet.microsoft.com/hu-hu/evalcenter/ff183870(en-us).aspx

Természetesen a jövőben foglalkozunk még a dinamikus memóriával, alkalmazásának feltételeivel, javasolt használatával stb. a www.technetklub.hu oldalon.

Alternatív kliens stratégia

Somogyi Csaba

BCSS kft

MCP, MCSE, MCT, MCITP, MCTS, ITIL Foundation

Sokan úgy gondolják, hogy csak azok a nagy, fontos és drága rendszerek alkotják az informatikát, amelyeket a számítóközpontok bombabiztos falai mögé rejtünk. Pedig azok a rendszerek sem kevésbé fontosak, amiket a felhasználóink kezébe adunk napi használatra: az ő számukra ugyanis nagyrészt az az informatika és a kapott megoldás minősége döntően meghatározza a véleményüket – a mi munkánkról. A következő cikkben arra keresek választ, - főleg IT vezetői szemszögből - milyen szempontok alapján érdemes a kliens környezetet megtervezni, miért célszerű a hagyományos, nagy, statikus és zárt rendszer helyett, kisebb egységekből felépülő, kompozit egységeket létrehozni.

Az kliens stratégia választás során felmerülő első kérdés mindjárt az, hogy milyen részekből áll(hat) ez a kliens stratégia és ezek hogyan függenek össze az egyes területek egymással. Íme, egy koránt sem teljes lista és a leggyakoribb kérdések:

Hardver választás

- Egy vagy több gyártó? (Az egyszerűbb garanciális ügyintézés ér többet vagy az olcsóbb ár?)
- Mennyire legyen egységes a géppark? 3-5 év alatt ez mennyibe kerül, fenntartható-e egyáltalán?
- Valóban mindenkinek egyforma gép kell? Mi kerül többe, túl erős gépeket adni vagy többfélét felügyelni?
- Mi legyen a VIP igényekkel? (A “trendi” eszközök kezelése: Mac-ek, tabletek és egyéb kütyük)

Operációs rendszer választás

- A drága az olcsóbb, vagy az olcsó a drágább? Olcsó-e az ingyen operációs rendszer, ha senki sem ért hozzá a cégnél? Számít-e, mérik-e a kliens támogatásra fordított időt?
- Hány operációs rendszer generációt támogassunk egyszerre? Milyen gyors lehet egy átállás (megvárjuk-e az SP1-et)?

Lemezkép startégia

- Mennyi lemezkép optimális egy cégnél? Létezik-e univerzális image?
- Vékony, félkövér vagy vastag lemezkép? (Melyik, mit is jelent?)

Alkalmazások

- Tudjuk-e egyáltalán, milyen alkalmazásokat használnak munkatársaink? Mennyiért fizetünk, amit nem használ senki? Miből van sok vagy éppen kevés?
- Alkalmazáskatalógus és portfólió (A “jövő-levő-menő” alkalmazások dilemmája és ezek finanszírozása)
- Van-e értelme (legalább egy riport erejéig) kimutatni, ki mit használ?

Felhasználói adatok

- Hol a helyük? Helyi vagy központi tárolás?
- Bizalmasság és adatvédelem – együtt vagy egymás ellen?
- Ki a tulajdonos -az egyén vagy a vállalat?

A lista koránt sem teljes, inkább csak szemléltetésnek szántam, hogy lássuk: valóban összetett kérdésről van szó. Mielőtt azonban részletesebben körüljárnánk a felvetett területeket, következzék egy kis közgazdasági kitérő.

A kliens stratégia választás vitathatatlanul komoly következményekkel járó döntés, mindenképpen célszerű számokkal alátámasztani pl. a lehetséges megtakarítások, az élőmunka ráfordítás vagy a munkaidő kiesés vonatkozásában. Persze egyáltalán nem mindegy, mit mérünk és hogyan. A klasszikus vicc jutott erről eszembe:

"Gépház! Mennyi? Háromszázhúsz. Mi háromszázhúsz? Mi mennyi?"

Elméletileg lehet egy olyan mutató, ami segíthet az egyes megoldások összehasonlításában, úgy hívják TCO (Total Cost of Ownership). Gyakorlati alkalmazása, kiszámítása azonban egyáltalán nem gyerekjáték, lássuk mik a fontosabb fenntartások a TCO-val kapcsolatban.

A leggyakorlatiasabb kifogás az, hogy annyiféle paraméterét kell(ene) ismernünk az informatikai ökoszisztémánknak (ugye, milyen szép, tudományos kifejezés?), ami az esetek döntő többségében nem áll rendelkezésre. A hardver és szoftver költségeket a számlák alapján még csak-csak össze tudjuk gyűjteni. De van-e adatunk arra, hogy mennyi élőmunkát kell egy-egy számítógépre fordítani évente? Ennek az élőmunkának milyen a szakmai mélysége és ebből következően a költsége? Tíz-húsz incidens, amit egy kezdő technikus is el tud hárítani valószínűleg lényegesen kevesebbe, kerül, mintha egy rendszermérnök dolgozik egy-két órát (történetesen a főnök) notebook-ján. Tudjuk-e számszerűsíteni azt a veszteséget, amit a munkakiesés okoz egy-egy számítógép üzemképtelensége alkalmával? Egy elvesztett hordozható gép tényleg csak annyit ér, amennyi a főkönyvi értéke? Tudjuk-e mérni az elvesztett adatok értékét (reprodukálás költsége, esetleges üzleti hátrányok, presztízsvesztés stb.)?

Aztán ha a jelenlegi költségekkel meg is vagyunk, hogyan derítsük fel az alternatívaként felmerülő megoldások költségeit (ezeket jelenleg nem üzemeltetjük, tehát hiányosak a bemenő adataink), és hogyan biztosítsuk, hogy ezek összevethetők legyenek egymással? Meg tudjuk-e előre mondani, mennyibe fog kerülni egy másfajta technológiai megoldás? Hogyan kezeljük a bevezetés többletköltségeit (mert ilyenek biztosan lesznek)?

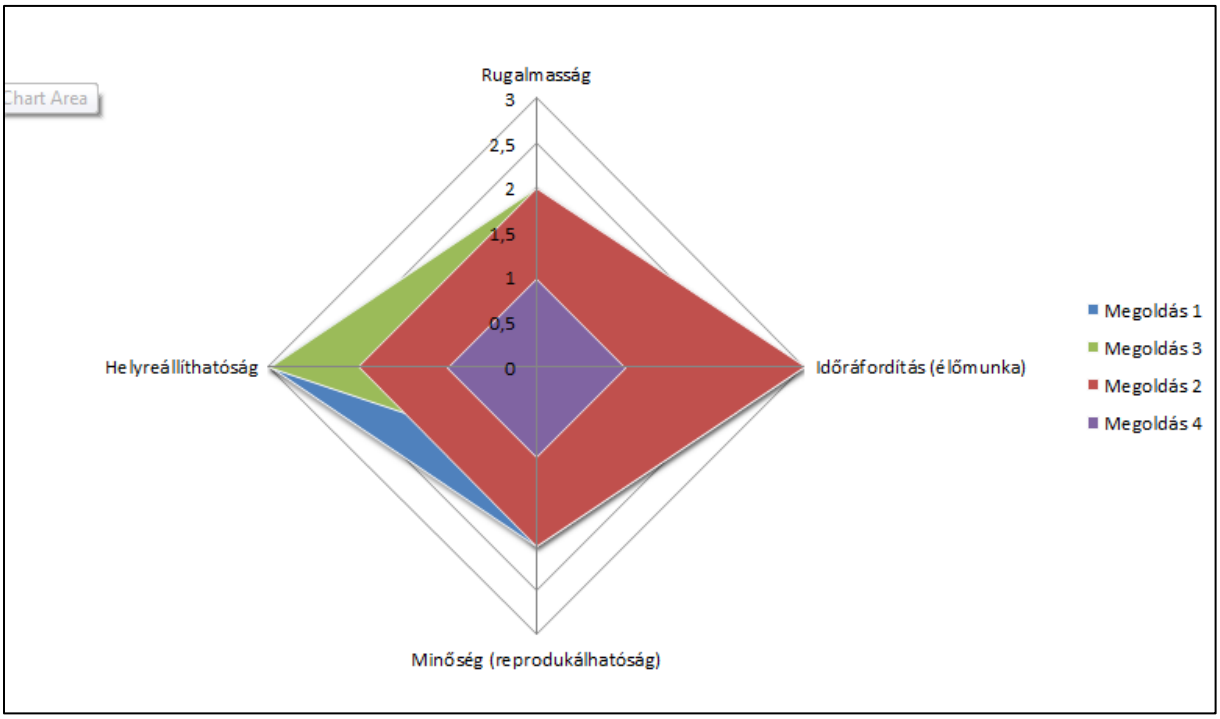
Ha pedig megszületik valamiféle összehasonlítás, még mindig szembesülhetünk azzal a ténnyel, hogy a TCO, mint egyedüli mutató torzíthat is. Ha kicsit közgazdászosabbra vesszük (bár, megjegyzem, nem vagyok az): ha a kapitalizmusban minden gazdasági vállalkozás profitjának maximalizálására törekszik, akkor csak a fele utat teszi meg a sikerhez az előállítási költségek minimalizálásával. Az út másik fele, a bevétel maximalizálása pl. monopolhelyzet, versenyelőny, piaci trend kihasználásával.

Röviden lefordítva a mi kérdéskörünkre: a leghatékonyabb kliens stratégia az, amelyik a teljes költség (TCO) és az üzleti eredmény között a legnagyobb különbséget képes kialakítani. Hiába alacsony a TCO, ha

az adott technológiai megoldás nem segíti az üzletet az eredményességben, viszont egy drágább technológia bevezetésének is lehet értelme, ha extra magas profit megszerzését segíti elő.

A közgazdaságtanról mára ennyit.

Mi lehet akkor az értékelés módja? Mit tegyünk, ha nem tudunk, nem akarunk valódi TCO-t számolni? Az egyszerűsített modell lehet például rangsorolás: állítsuk sorba az egyes technológiai területeken felmerülő megoldásokat, majd a helyezéseket összesítsük. A legkisebb helyezési számú megoldáscsoport lehet a nyertes. A modellt bonyolíthatjuk azzal, hogy jelöljük azokat a technológiákat, amik műszaki okokból vagy költségességük miatt nem alkalmazhatók együtt. Az eredmény akár grafikusan is ábrázolható, ha jól választottunk szempontokat, akkor a legkisebb területet lefedő technológiai megoldás lehet a számunkra optimális. Az illusztrációként készített ábrához nem is teljesen önkényesen választottam értékelési szempontokat: a rugalmasság, az időráfordítás, a reprodukálhatóság és a helyreállíthatóság négy jelentős tényező, amikor választanunk kell, de ezekről essék szó a technológiai részleteknél.



ábra 10: A négy fontos tényező

A kliens stratégia természetesen nem lineáris, folyamatosan előrehaladó tervezési folyamat eredményeként születik. A cikk elején található lista elemeit többször, újra át kell gondolni, hogy valamennyi függőséget és azok kihatásait átlássuk. Az átláthatóság megteremtésében lehet segítségünkre a Microsoft Desktop Optimization (MDOP) megoldása, ami - a remek technológiai megoldások mellett - módszertani segítséget is nyújt a sikeres stratégia kidolgozásához.

A rendrakást kezdjük azzal, hogy számba vesszük, mire is fogják használni a felhasználók a nekik biztosított informatikai eszközöket (szigorúan maradjunk az üzletileg indokolt tevékenységeknél)! Igyekezzünk a felhasználói igényeket néhány tipikus kategóriába sorolni! A kategóriák felállításánál használhatjuk az MDOP dokumentáció öt kategóriáját (feladat munkás, irodista, szerződéses munkaerő, mobil felhasználó, távmunkás) vagy létrehozhatjuk a saját típusainkat. A felhasználói típusokhoz keressük meg a számukra optimálisnak tekinthető kliens megoldást. Az átláthatóság kedvéért ebből akár táblázatot is készíthetünk, amiben a cikk elején felsorolt szempontokat is feltüntethetjük.

		Feladat munkás	**Mobil felhasználó**	**Irodista**	**Szerződéses**	**Távmunkás**
Hardver	típusa	vékony kliens	notebook	PC	vékony kliens vagy saját	saját
	teljesítménye	kicsi	közepes - nagy	kicsi - közepes	kicsi	kicsi
Operációs rendszer		Windows ajánlott (RDP verzió miatt)	Windows 7 Bitlocker-rel	Windows 7	Windows ajánlott (RDP verzió miatt)	Windows ajánlott (RDP verzió miatt)
Lemezkép		nincs	vékony	vékony	nincs	nincs
Alkalmazásterítés		APP-V	APP-V (cached)	APP-V	RDS + APP-V vagy VDI	RDS + APP-V vagy VDI
Felhasználói adatok		Átirányított mappa + RDS profil	Átirányított mappa (offline mód)	Átirányított mappa (offline mód)	Átirányított mappa	Átirányított mappa

Természetes, ha a táblázat egyes celláit nem tudjuk azonnal és habozás nélkül kitölteni, minden egyes döntésünk mögött rengeteg megfontolandó szempont állhat. Sőt, akár több ilyen táblázatunk is lehet, amiben a részterületek optimális kombinációit keresgéljük. Mintaként vezessük most végig a fenti táblázatban látható példát!

A feladat munkásoknak vékony klienst szánunk, hiszen ők kevés féle, de gyakran ismétlődő feladatot végeznek, folyamatosan a hálózathoz csatlakozva. A feladataik nem igényelnek különösebb számítási kapacitást és a grafikus megjelenítés minősége sem szempont. A vékony kliensektől nagyobb megbízhatóságot (nincs mozgó alkatrész) és kisebb karbantartási igényt várunk el (noha ez a tévhitekkel ellentétben nem nulla!). A másik oldalon a vékony kliensekkel természetesen szembe kell állítani

valamilyen központi szolgáltatást, amit használhatnak, ez most legyen Remote Desktop Services, mert nagyságrendekkel olcsóbb, mint egy virtualizált deszktop. Az alkalmazásokat az RDS kiszolgálókra APP-V csomagok formájában juttathatjuk el (Windows Server 2008 kompatibilitás ellenőrizendő!), mert ebben a formában jelentősen jobb lehet az RDS szerverünk kihasználtsága – az alkalmazások frissítése nem igényli a kiszolgáló újraindítását. A felhasználóknak szinte nincsenek is a munkájukhoz kapcsolódó tárolandó adataik, ehhez mérten adhatunk nekik tárkapacitást a fájlszerverünkön.

A táblázat egy ágát végigjárva, már látszik az a sajátosság, hogy pl. a kliens formátum (esetünkben a vékony kliens) megválasztása hogyan szűkítheti be a további választási lehetőségeket az operációs rendszer vagy az alkalmazásterítés vonatkozásában.

A második csoport a mobil felhasználók csoportja, és a csoport neve már tartalmazza specifikus igényüket: munkájuk végzése során gyakran nem kapcsolódnak közvetlenül a helyi hálózathoz és lehetnek olyan feladataik, amelyek számítási és/vagy grafikus teljesítményt igényelnek az általuk használt eszközben. Szolgáljuk ki az ő igényeiket a lehető legkevesebb új komponens bevonásával! Megtarthatjuk az alkalmazás virtualizációt, mint alkalmazásterítési technológiát, hiszen van lehetőségünk az alkalmazások cache-be töltésére, amikor a felhasználó a hálózathoz csatlakozik (akár Internet-en keresztül is) vagy MSI csomag formájában adathordozóra is tehetjük virtualizált alkalmazásainkat. Operációs rendszernek válasszuk a Windows 7-et, egyrészt az offline mappák hatékonyabb kezelése, másrészt a Bitlocker miatt. A lemezképet se bonyolítsuk túl: akár Windows Deployment Services-t (WDS), akár Microsoft Deployment Toolkit-et (MDT) vagy éppen System Center Configuration Manager-t (SCCM) használunk az operációs rendszer terítésére, van lehetőségünk arra, hogy a szükséges eszközvezérlő készletet dinamikusan csatoljuk az operációs rendszer gyári telepítő készletéhez. Alkalmazásból pedig mindössze kettő kell: az APP-V kliens és a vírusirtó. Ezeket MDT-vel vagy SCCM-mel telepíthetjük, viselkedésüket pedig házirendekkel központilag szabályozhatjuk. A felhasználói adatokat a mappa átirányítási csoportházirendekkel tereljük át fájlszerverre, ezzel egyszerűsödik mentésük és nem veszítjük el őket, ha notebooknak nyoma vész. (Zárójelben jegyezzük meg, hogy az operációs rendszer választás kihatással van a hardver választásra: még beleszaladhatunk raktárkészletről, nagy kedvezménnyel árult, ámde Windows 7-re nem minősített hardverrel!)

Irodai munkásaink kapjanak mostani példánkban hagyományos PC-t (ezt megszokták, szeretik és tegyük fel szükségük is van rá)! Tartsuk meg hozzá a meglévő vékonyka Windows 7 lemezképünket, persze egészítsük ki a szükséges eszközvezérlőkkel! Telepítsük az operációs rendszert, ahogy a notebook-okét, telepítsük az alkalmazásokat, ahogy a notebook-okra! Kezeljük a felhasználói adatokat, ahogy eddig mindenkiét (legfeljebb adjunk nagyobb kvótát a fájlszerveren, mint szegény feladat munkásoknak). Ezzel a csoporttal bizony nem sok dolgunk akadt, kiszolgálásukhoz minden rendelkezésre állt már.

Az utolsó két felhasználói típus nálunk egyelőre még nem túl gyakori, akár össze is vonhatjuk őket, mert sokban hasonlítanak egymásra. Példánkban sem a szerződéses munkatársnak, sem a távmunkásnak nem biztosítunk hardver eszközt. A szerződő (megbízott) az őt bérbe adó cég gépét használja, a távmunkás a sajátját. Ebből következően hálózati hozzáférésüket a minimálisra szeretnénk csökkenteni, nem is engedünk nekik mást csak RDP használatát (és lehetőleg azt is Network Access Protection mellett). Az esetek többségében biztosan elegendő lesz munkájukhoz, ha egy RDS kiszolgálón biztosítjuk számukra a szükséges alkalmazásokat (mi mással, ha nem ismét APP-V-vel, hiszen adott az infrastruktúra, sőt akár az

alkalmazáscsomagok is). Ritkább esetekben, például ha szerződéses vagy távmunkás munkatársunk egy új alkalmazást fejleszt és ehhez rendszergazdai jogokra van szüksége, ráadásul gyakran kell újraindítania a gépét, biztosítsunk számára egy virtualizált deszktopot. Ehhez ismét használhatjuk a korábban létrehozott vékonyka Windows 7-es lemezképünket, ha Hyper-V virtualizációt használunk, már az eszközvezérlőkre sincs gondunk. Az alapvető alkalmazásokat ide is küldhetjük APP-V-vel, az egyedi dolgok telepítését bízhatjuk a felhasználóra (ha nem boldogul vele, akkor nem indokolt számára a VDI kliens ☺).

Ha visszatekintünk a táblázatra láthatjuk, hogy többféle felhasználói igényt egészen kis számú technológia rugalmas kombinálásával és újrahasznosításával is ki tudunk elégíteni és igazából még csak egyet jártunk végig a lehetséges kombinációk közül. Az ilyen kis részrendszerek kialakítása és fenntartása – bármilyen technológiai szempontból korrekt kombinációban - lényegesen olcsóbb lehet, mint a statikus nagy rendszerek hosszas elkészítése és nehézkes karbantartása, miközben megnyerjük a rugalmas alkalmazkodás képességét a változó üzleti igényekhez.

Adatmentés és visszaállítás a System Center Data Protection Manager 2010 segítségével

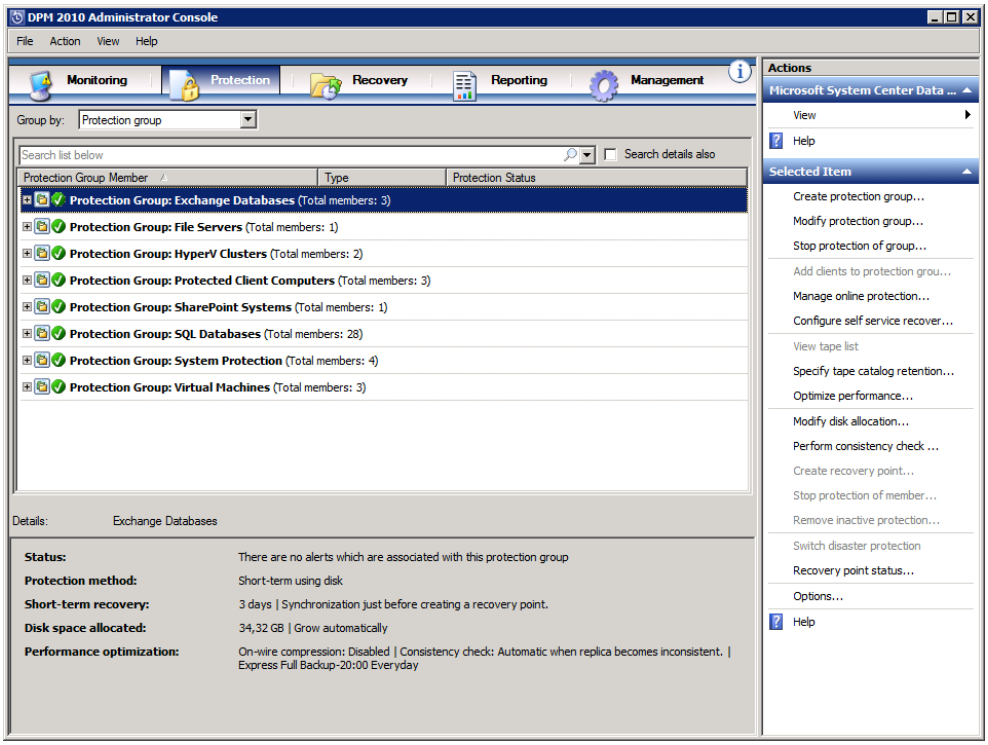
Szirtes István

Szirtes Technologies Kft.,

System Center Operations Manager MVP

A mentendő adatok köre folyamatosan változik. A virtualizáció terjedésével együtt egyre újabb kihívásokkal találják szembe magukat a mentéssel foglalkozó szakemberek. Jellemzően az archiválandó adatok mérete inkább növekszik, mint hogy egy kicsit is csökkenne. Az egyre újabb technológiák bevezetésével együtt ez a helyzet csak tovább romlik, hiszen legtöbbször a bevezetés legfőbb mozgatórugója a nagyobb terhelhetőség, és a magasabb fokú rendelkezésre állás. A mentési ablak csökkenésével együtt egy újabb kezelendő probléma is előtérbe került: ha megtörtént a baj, akkor azt a lehető legrövidebb időn belül el kell hárítani. Ilyenkor jöhet jól a megfelelő eszközökkel és jogokkal megtámogatott végfelhasználó általi adat visszaállítás.
Persze ezek a szempontok csak a „jéghegy csúcsát” jelentik egy mentő szoftverrel kapcsolatos elvárások listájában, cikkemben éppen ezért csak szemezgetek a System Center Data Protection Manager 2010 legfontosabb újdonságaiból.

Az adatmentés területén dolgozó Microsoft szakemberek 2010 áprilisában bizonyára örültek a hírnek, hogy megjelent az SCDPM következő verziója, amely immár a harmadik generációs mentési megoldás a Microsoft palettáján.
Az első változatot még Data Protection Manager 2006 néven ismerhettük meg, melynek a legfontosabb célja a fiókirodákban előálló adatok központosított mentésének megoldása, ezáltal az egyes telephelyek szintjén a szalagos egységek kiváltása.
A következő változat már a System Center termékcsalád részeként debütált, de kezdetben ez inkább csak a névben jelentett összefonódást a termékcsalád többi elemeivel. Az SCDPM 2007-ben sok új fejlesztés látott napvilágot, többek között az Exchange, SharePoint, vagy az SQL alkalmazás kiszolgálók mentési képessége. Az SCDPM 2007 SP1 legfontosabb újítása a Hyper-V környezetek és a felhő alapú adatvédelmi rendszerek (külső gyártók megoldásaival ötvözve, pl. Iron Mountain) támogatása.
A DPM fejlesztési koncepciójának középpontjában a kezdetektől fogva az a megközelítés állt, hogy egyetlen ügynökön keresztül a Microsoft által készített alkalmazások, kiszolgálói szerepkörök, és a felhasználói adatok menthetőek, és szükség esetén visszaállíthatóak legyenek.
A jelenlegi változat egyaránt támogatja a kiszolgáló és munkaállomás operációs rendszerek mentését, amely adatokat akár lemezen, akár szalagon is tárolhatunk.
Az SCDPM 2010 megőrizte a 2007-es változat konzol felépítését és működési hátterét, így ennek elsajátítása sem fog gondot okozni.
A konzol mögötti fejlesztői ideológia teljesen egyértelmű: minél nagyobb a baj, annál stresszesebb folyamat a visszaállítás. Éppen ezért a konzol legyen letisztult és rendkívül könnyen értelmezhető.



ábra 11: SCDPM felügyeleti konzolja

Miután felvettük a rövid távú adatmegőrzési tárterületre szánt merevlemezeket, illetve a hosszú távú archiválást biztosító szalagokat, telepíthetjük a mentési ügynököket, beállíthatjuk az értesítési mechanizmust, rögzíthetjük a megvásárolt felügyeleti licenceinket, és kezdődhet a mentési csoportok létrehozása. A mentésre kijelölhető adattípusok közül lássuk a DPM 2010 legfontosabb újdonságait jelentő funkciókat:

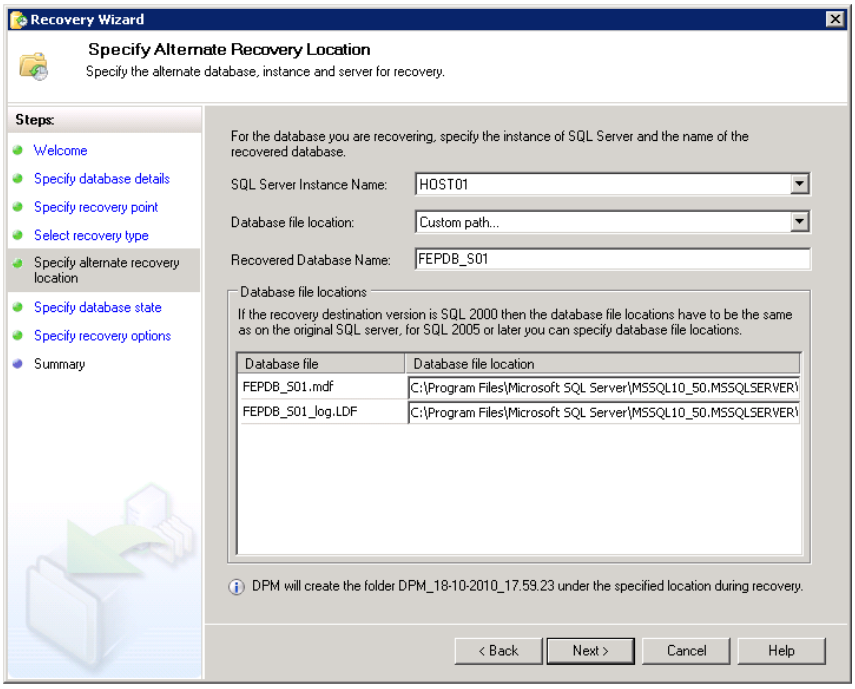
Postafiók elemszintű visszaállítása

Jó dolog, ha egy komplett Exchange adatbázist tudunk mentésre kijelölni, és persze az sem elhanyagolható, ha a mentő szoftver megoldja a feleslegessé vált tranzakciós napló állományok kitakarítását. De egy „véletlenül" letörölt postafiók, vagy még inkább egy levél esetén nem fogjuk a komplett adatbázist visszaállítani a korábbi állapotára, hiszen így az eredi problémánál is nagyobb bajt csinálnánk. A DPM fejlesztői a visszaállítás feladatát részben az Exchange képességeire és annak rendszergazdájára bízzák. Egy elemszintű visszaállítás első lépésében a DPM konzoljából kiválasztott postafiók egy megadott időpontra történő visszaállítását konfigurálhatjuk, de a következő lépésben belebotlunk a Recovery Database igényébe. Ilyet az Exchange 2010-ben nekünk kell PowerShellből létrehoznunk. Ha ez megvan, akkor a visszaállítás első lépésén túl vagyunk, hiszen a postafiók adatbázis és a szükséges tranzakciós és egyéb rendszer állományok a megadott Recovery DB útvonala alatt megtalálhatóak. A folyamat további részei már az Exchange rendszergazda feladatát képezik, ezért csak vázlatosan: adatbázis felcsatolása, majd PS-ből a megadott postafiók és a keresési feltételeknek megfelelő elem(ek) visszaállítása.

SQL adatbázisok automatikus mentése és delegálható visszaállítása

Az SCDPM 2010 újdonságai között két nagyon hasznos SQL támogató funkció található. Az új verzióban akár az egész SQL kiszolgálót is felvehetjük a mentendő erőforrások körébe, ezáltal a rajta kezelt összes adatbázis automatikusan mentésre kerül. A hangsúly nem a védelmi csoport megalkotásakor kezelt adatbázisokon van, hanem azokon, amiket ezt követően hozunk létre. Gondoljunk például egy

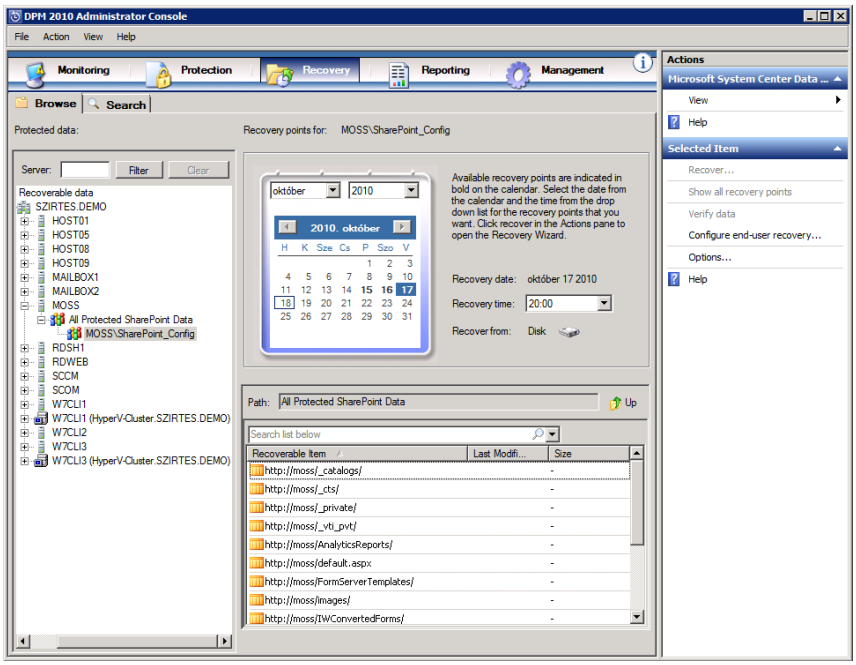
SharePoint rendszer tartalmi adatbázisaira. A rendszer dinamikus változásait képes a mentő szoftverünk automatikusan lekövetni.
Az ügyfél igényekre reagálva a fejlesztők beépítették a SQL rendszergazdák számára delegálható adatbázis visszaállítás képességét, melyhez egy egyszerű és kézenfekvő visszaállító konzol (DPM Self Service Recovery Tool) is társul. Ez utóbbi külön telepítendő a rendszergazdai munkaállomásra az SCDPM telepítő készletén található DpmSqlEURInstaller\DPMSQLEur_x64.msi (vagy …x86.msi) futtatásával.



ábra 12: Az SQL rendszergazda által kezdeményezett adatbázis visszaállítása

SharePoint 2010 elemszintű visszaállítása

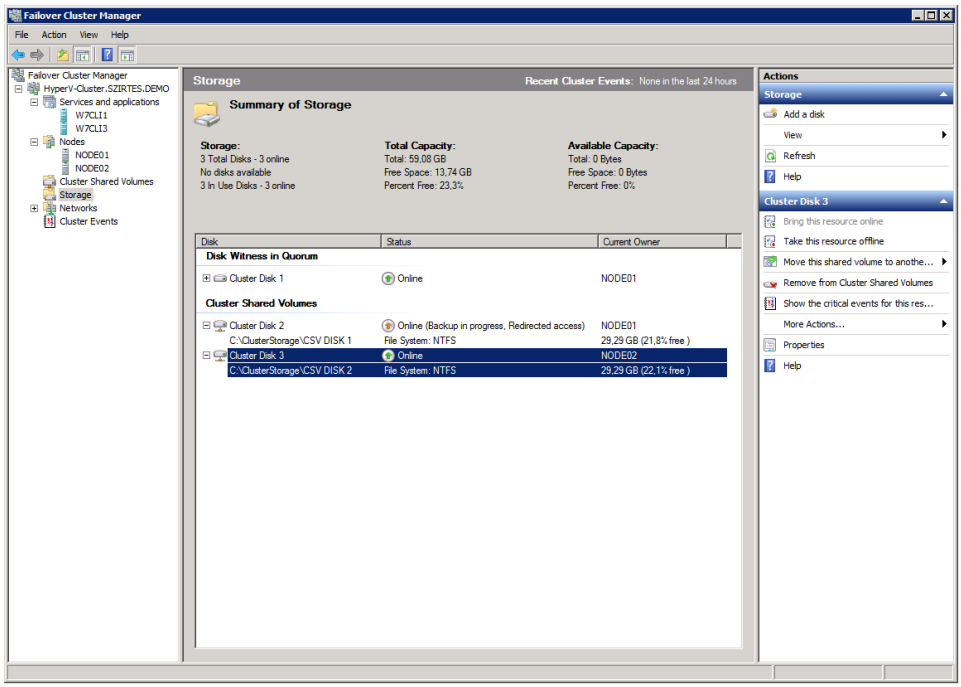
Minél előbb érdemes bevezetni a SharePoint 2010-et, ha másért nem is, akkor az elemszintű visszaállítás indokolttá teheti ☺.
Miről is van szó? A DPM 2007 és a SharePoint 2007 együttesében az elemszintű visszaállítás csak úgy kivitelezhető, ha építetünk egy Recovery Farm-ot, amely tükörképe az éles portál rendszerünknek. Ezt követően jöhet az adatbázis visszaállítása, majd a helyreállított környezetből a szükséges tartalmak átmásolása az éles rendszerbe. Ez egyaránt erőforrás- és időigényes feladat, amire eléggé nehezen szánjuk rá magunkat. Ehhez képest felüdülést jelent a visszaállítás azon módja, ahogy a DPM 2010 ezt elénk tárja. Elegendő a portál tartalmi adatbázisát kinyitnunk és kiválasztanunk a szükséges elemet, amit a varázsló további lépésein végighaladva akár az éles rendszerbe visszatölthetünk.



ábra 13: SharePoint konfigurációs adatbázisa tallózható formátumban

CSV alapú rendszerek támogatása

Amikor mindenhol virtualizációba és a szorosan vele együtt járó magas rendelkezésre állásba botlunk, talán nem túl nagy elvárás az sem, hogy a virtuális gépparkot futás közben tudjuk menteni. Alap szempont, hogy a mentésben szereplő virtuális gép a futó példánnyal konzisztens állapotban legyen a mentés befejezésekor. Ehhez persze megtehetnénk, hogy a mentés idejére mentett állapotba (saved state) hozzuk gépeinket, majd a mentés végén elindítjuk azokat, ám ha rövid időre is, de a kiszolgálók által nyújtott szolgáltatások így kiesnek. Erre ad megoldást a virtuális gépre telepíthető Plugin VDev csoportba tartozó biztonsági mentés (kötetpillanatkép) integrációs komponens, de ehhez a virtuális gépnek „felvilágosultnak” kell lennie, tehát szükséges a megfelelő IC komponens és persze a mentő szoftvernek is támogatnia kell a funkciót. De mi a helyzet a Cluster Shared Volume alapú osztott tárterület kezeléssel, ahol egy időben több virtuális gép adatait helyezhetjük el, melyek szétszórva futnak a fürtbe szervezett kiszolgálókon? Ahhoz, hogy az összes hoston futtatott virtuális gépről konzisztens állapotú mentés készülhessen, a mentés idejére a DPM ügynök automatikusan átkapcsolja az osztott lemez elérését redirect módba. Így az összes VM a LUN tulajdonosán keresztül kerül archiválásra. A folyamat végén a LUN elérése visszaáll a normál üzemmódra.



ábra 14: A CSV típusú lemezen elhelyezett VM mentése

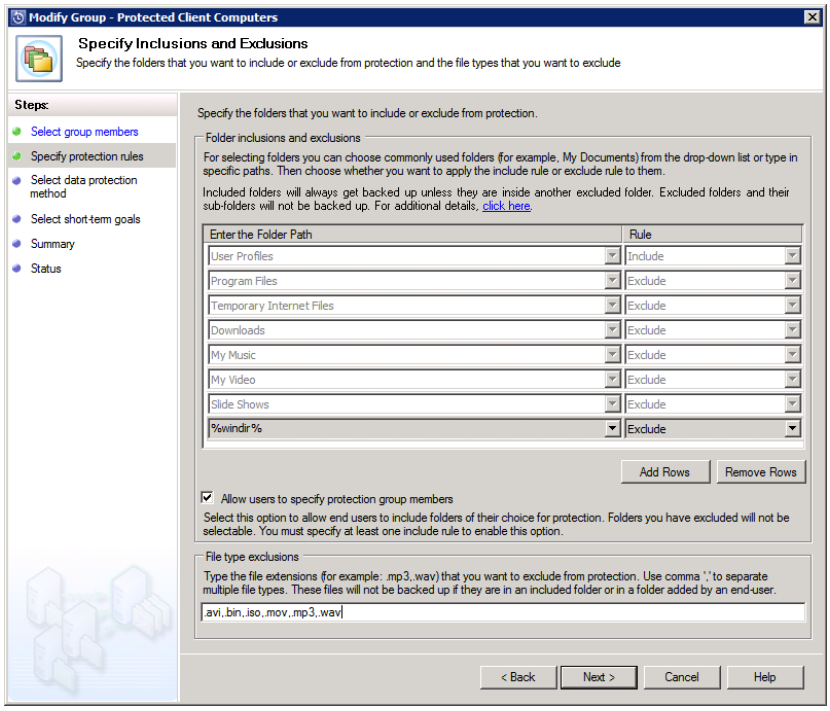
Virtuális gépek és a VHD állományok kezelése

A mentésre kijelölhető elemlistában megtalálható a komplett virtuális gép is, de visszaállítani nem biztos, hogy az egész gépet szeretnénk. Olykor nagyon jól tud jönni az a funkció, amit a DPM VHD elemszintű visszaállítás képességeként tud nyújtani. A kiválasztott időpontban készült VHD mentést képes felcsatlakoztatni, ezáltal tallózható állapotba kerül a virtuális merevlemez tartalma. A többi már egyértelmű: visszaállíthatjuk az eredeti virtuális gépbe, vagy alternatív helyre a szükséges fájlokat. Ha Windows Server 2008 R2 platformra telepítjük a System Center Data Protection Managert, akkor még a Hyper-V szerepkör telepítésére sincs szükség, hiszen ebben az OS-ben már alapértelmezett a natív vhd támogatás.

Végfelhasználói visszaállítás

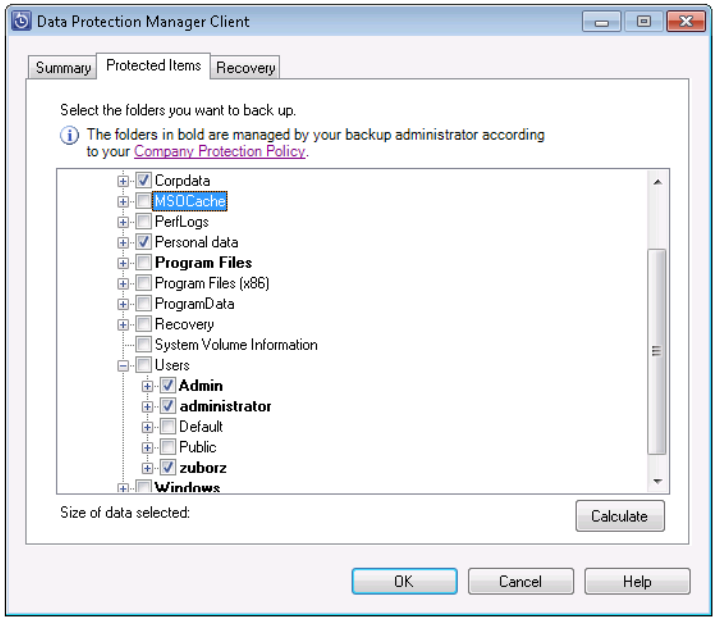
Egy örök dilemma látszik megoldódni az említett funkció bevezetésével. A vállalati üzemeltetés alapértelmezettként nem foglalkozik a munkaállomásokon tárolt adatok mentésével. A lokálisan tárolandó adatok ellen számos szabályozás és technikai korlátozó eszköz született, de úgy tűnik, a felhasználók mindezek ellenére szeretik a gépükön tartani a számukra fontos adatokat. Viszont, ha ez a lehetőség adott, akkor meg kell oldanunk ezen adatok központosított mentését is!

A DPM 2010-ben lehetőségünk van arra, hogy a munkaállomásokon tárolt adatokra egységes mentési szabályozást készítsünk, amit a felhasználó saját szabály elemeivel bővíthet, persze csak akkor, ha ehhez megadtuk számára a megfelelő jogokat.



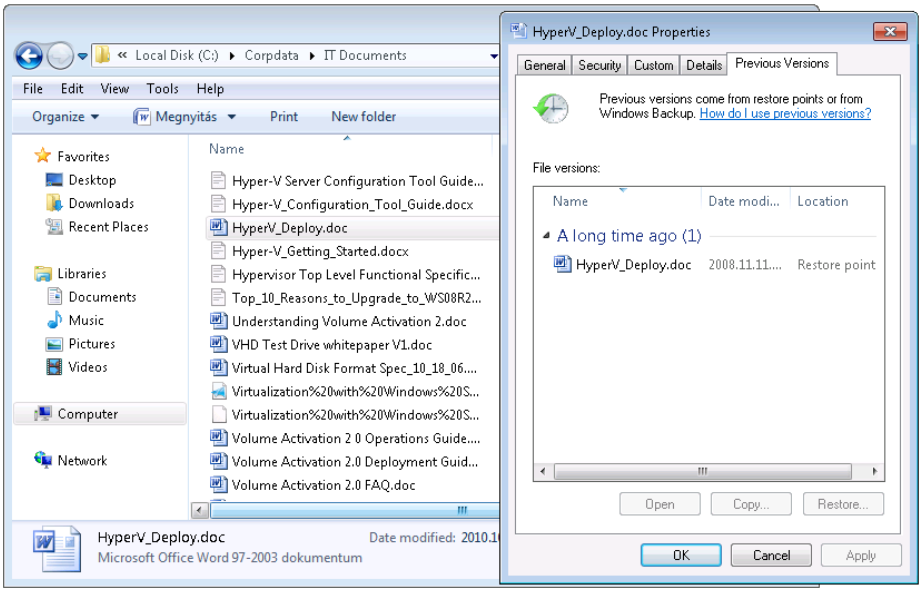
ábra 15: Munkaállomások vállalati mentési szabálya

A funkció igénybevétele előtt a desktop gépekre is telepítenünk kell a DPM ügynök komponenst, majd meg kell fogalmaznunk a védendő erőforrások körét. Miután a munkaállomáson futó ügynök megkapta a szabályokat a folyamat automatizálttá válik. Igény esetén a felhasználó saját igényei alapján kiegészítheti a mentendő adatok körét, de a céges szabályozást nem módosíthatja.



ábra 16: A mentendő adat körét a felhasználó is befolyásolhatja

A visszaállításra a már megszokott előző verziók opció használható:



ábra 17: árnyékmásolatból való visszaállítás

RemoteFX a Windows Server 2008 R2 SP1-ben

Szalay Márton

Rendszermérnök

MCSE, MCITP, MCPD, MCT, CCNA, Security

Napról napra egyre több cég ismeri fel a virtualizációban rejlő előnyöket: a költségcsökkentési lehetőségeket vagy az üzemeltetés egyszerűsödését. A VDI-nek (virtuális desktop infrastruktúra) köszönhetően a korábbi költséges vastag klienseinket olcsóbb vékony kliensekre cserélhetjük anélkül, hogy csökkenne a felhasználói élmény.

A Microsoft több mint két évvel ezelőtt felvásárolta a Calista Technologies nevű, desktop virtualizációval foglalkozó céget. A Calista által kidolgozott technológiákat továbbfejlesztették, majd 2010 márciusában bejelentették a Microsoft RemoteFX-et. Ez nem egy új termék, sokkal inkább az RDP-technológia kibővítése, továbbfejlesztése. A RemoteFX segítségével a távoli asztali kapcsolaton keresztül a felhasználó a megszokott Windows Aero környezetben Silverlight és Flash animációkat nézhet, minden DirectX-re és több, OpenGL-re épülő 3D-alkalmazást futtathat, médialejátszókat és tetszőleges USB-eszközt használhat – pont úgy, mint a saját, helyi számítógépén.

Korábban problémát okozott a 3D-s, illetve a grafikát intenzíven használó alkalmazások (pl. CAD-alkalmazások, animált weboldalak, videók) virtualizálása, pontosabban ezek hálózaton történő átvitele. A RemoteFX ezt a problémát orvosolja.

Képzeljük el azt a szituációt, hogy egy CAD programot használó, 15 fős tervezői csapattal rendelkező tervezőiroda költségcsökkentési céllal konszolidálja a munkaállomásait és a munkatársaknak vékonyklienseket ad. Vesznek egy nagyobb teljesítményű szervert, melyen Hyper-V-ben (akár az ingyenesen elérhető Microsoft Hyper-V Server 2008 R2 SP1-en is) futtatják a 15 db Windows 7 SP1-es virtuális munkaállomást, a szerverbe pedig vesznek 3-4 db támogatott GPU-val rendelkező videokártyát. A RemoteFX akkor jön be a képbe, amikor a tervezők a vékony kliensükről RDP-n keresztül bejelentkeznek a nekik fenntartott Windows 7 SP1-es virtuális gépekre és elindítják a CAD programot. A gyengébb teljesítményű vékony kliensek valószínűleg nem tudnák futtatni a CAD alkalmazást, de nem is kell, ugyanis minden erőforrásigényes műveletet a szerver végez el, a kliensek feladat pedig csak a megjelenítés. E feladatokat a RemoteFX az alábbi szolgáltatásokkal támogatja:

- **Hosztoldali renderelés**: Bár az Aero-felületet már a Windows Vistában lévő 6.0-s RDP is át tudta hozni, azonban valójában csak a 3D-s grafikai utasítások utaztak az RDP-protokollban és a megjelenítést, a kép előállítását a kliens grafikus processzora (GPU-ja) végezte. A RemoteFX esetén a virtuális Windows 7-ben futó 3D-alkalmazás 3D utasításait (DirectX, OpenGL) – egy virtuális videokártya driver közbenjárásával – a virtuális hosztgép (Hyper-V szerver) valamelyik GPU-ja fogja kiszámítani, leképezni, majd a bitképet visszaküldi a virtuális Windows 7-nek, ami továbbítja az RDP-csatornán keresztül erős és adaptív tömörítés mellett a vékony kliensnek. Így a felhasználó – a vékony kliens teljesítményétől függetlenül, kizárólag a szerver CPU-ját és GPU-ját használva – a felhasználói élmény csökkenése nélkül futtathatja a grafikai programokat.
- **GPU virtualizáció**: A RemoteFX egy WDDM driver segítségével elérhetővé teszi a virtuális desktop számára a hosztgép (Hyper-V szerver) GPU-ját, így több virtuális munkaállomás osztozhat egy videokártya GPU-ján, vagyis egy videokártya egyidőben több munkaállomást is kiszolgálhat.

- **Intelligens képernyőrögzítés**: Figyeli az egyes képkockák (frame-ek) között a képernyőt és csak a változásokat küldi kódolásra, továbbá monitorozza a hálózati sebességet és a kódolást, illetve a képfrissítést a rendelkezésre álló sávszélességnek megfelelően állítja be.
- **RemoteFX Encoder**: A kódolást a processzor, a GPU vagy akár dedikált hardvereszköz is végezheti. Amikor a képernyőkép tömörítésre került, az Encoder a keletkezett bitképeket elküldi a virtuális munkaállomásnak, ami pedig továbbítja azokat az RDP kliens felé.
- **RemoteFX Decoder**: Dekódolja a virtuális desktopról az RDP kliensre érkezett bitképeket, amit szintén akár a processzor, akár a kliens GPU-ja vagy akár egy dedikált hardvereszköz elvégezhet.
- **RemoteFX USB átirányítás**: A RemoteFX a klienshez csatlakoztatott USB eszközöket az USB-busz szintjén irányítja át, így a virtuális desktopon anélkül is használhatjuk őket, hogy az RDP kliensen drivert telepítenénk hozzájuk. Ez a megoldás támogatja többek között a hangeszközöket, a tárolókat (pl. pendrive, hordozható merevlemez), a HID-eszközöket (pl. billentyűzet, egér), a nyomtatókat és a szkennereket.

Szoftverkövetelmények:

A RemoteFX-et a Windows Web Server 2008 R2 és a Windows Server 2008 R2 for Itanium-Based Systems kivételével minden, SP1-gyel frissített Windows Server 2008 R2 változaton használhatjuk, még a Microsoft Hyper-V Server 2008 R2-n is! A virtuális desktopon a Windows 7 Enterprise vagy Ultimate kiadás SP1-gyel frissített verziójának kell futnia, ellenben RemoteFX-támogatott RDP kapcsolatot bármilyen számítógépről kezdeményezhetünk, feltéve, hogy Remote Desktop Connection kliensprogram 7.1-es változatát használjuk.

A Windows 7 és a Windows Server 2008 R2 első szervizcsomagjának bétája innen tölthető le.

Hardverkövetelmények:

- SLAT-ot (Second-Level Address Translation, másodszintű címfordítás) támogató processzor, mely virtualizáció során jelentősen javítja a teljesítményt. Az Intel processzoraiban ezt Extended Page Tables (EPT), az AMD-nél Nested Page Tables (NPT) néven találjuk meg.
- A RemoteFX szerverben (virtuális hosztgép) legalább egy, de ajánlott – a használat intenzitásától függően – 4-5 felhasználónként, vagyis 4-5, GPU-t használó virtuális gépenként egy GPU. A GPU driverének támogatnia kell a DirectX 9.0c-t és a DirectX 10-et. Ha a szerverben egynél több GPU van, akkor azoknak egyformának kell lenniük, és megfelelő mennyiségű dedikált – azaz nem a rendszermemóriából leválasztott – videomemóriával kell rendelkezniük. Amennyiben használjuk a Hyper-V Live Migration szolgáltatását, akkor minden RemoteFX szerverben egyforma videokártyákat kell használnunk. Minden, XDDM driverrel rendelkező videoeszközt le kell tiltani – jellemzően ilyenek a szerverek alaplapjára integrált távmenedzsment adapterek.
- A hardveres RemoteFX Encoder opcionális, de jelentősen javítja a RemoteFX szerver skálázhatóságát. A hardveres enkódert egy x4-es vagy gyorsabb PCI-E csatlakozóba kell rakni.
- A szervernek meg kell felelnie a Hyper-V által támasztott követelményeknek.

A RemoteFX szolgáltatást a szerverre a **Server Manager • Kiszolgálókezelő** konzolban a **Roles • Szerepkörök**, **Remote Desktop Services • Távoli asztali szolgátatások** pont alatt telepíthetjük, majd a Hyper-V konzolból adhatunk RemoteFX 3D Video Adaptert az egyes virtuális gépeknek.

További olvasnivalók angolul:

- A RemoteFX röviden (videó): http://technet.microsoft.com/en-us/edge/remotefx-in-server-2008-r2-sp1-with-michael-kleefe.aspx?query=1
- A támogatott GPU-k listája: http://go.microsoft.com/fwlink/?LinkID=197416
- RemoteFX bevezetése lépésről lépésre: http://technet.microsoft.com/en-us/library/ff817611(WS.10).aspx
- USB átirányítás beállítása RemoteFX-en lépésről lépésre: http://go.microsoft.com/fwlink/?LinkId=192431
- NVIDIA és a RemoteFX: http://blogs.nvidia.com/ntersect/2010/07/nvidia-and-microsoft-enhancing-the-virtual-desktop-user-experience-with-microsoft-remotefx.html

Extended Events kezdőknek

Bitemo Erik

Disney Interactive Media Group, DBA Expert

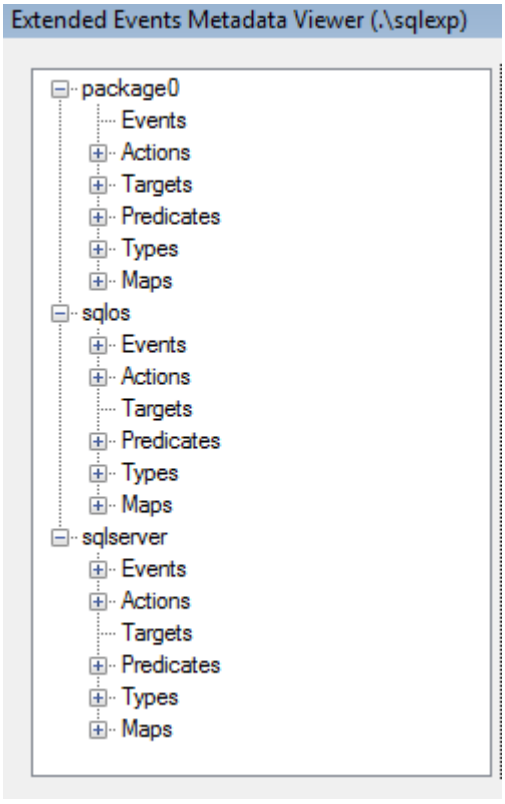
MCDBA, MCTS

SQL Server MVP

Az SQL 2008 jónéhány újdonságot hozott, ezek közül az egyik legalacsonyabb marketing/hasznosság aránnyal rendelkező az Extended Events (magyarul kiterjesztett események, de még egyszer nem írom le). Ez egy alacsonyszintű eseménykezelő rendszer, ami tulajdonképpen egy alapos debug lehetőség SQL Serverhez. Az esemény itt egy meghatározott pont a kódban (mármint az SQL Server mint alkalmazás kódjában, és persze nem egy, hanem sok meghatározott pont van, de valószínűleg nem érdekel minket minden egyszerre), ami érdeklődésünkre számot tarthat. Tehát igazi debug lehetőség, csak éppen nem Visual Studio, hanem Transact-SQL kell hozzá.

Az események sokfélék lehetnek, fájl hozzáféréstől lockok kezelésén át T-SQL utasítások végrehajtásáig bármi beleférhet. A megfigyelhető események köre némileg átfedésben van a Profiler vagy SQL Trace által figyelhető adatokkal, de az Extended Events sokkal mélyebb betekintést enged az SQL Serverben zajló dolgokba, és sok olyan dolgot is meg tud mondani, amit a Profiler soha (például mennyi idő volt egy latch megszerzése). És ami igazán lényeges: olyan áron mondja meg, hogy a Profiler/SQL Trace elsápad az irigységtől. Egy 2 GHz-es processzoron 2 µs alatt dolgoz fel egy eseményt. Ez érezhetően elég kicsi, másodpercenként 500,000 eseményt dolgozhatna fel főállásban egy processzormag. Itt azért megkérdezheti az olvasó, hogy „jó, jó, de akkor miért nem ezt használja mindenki a világon?”.

Az első és sokaknak legfájdalmasabb válasz, hogy talán azért, mert nincs hozzá grafikus felület. Mindent Transact-SQL-ben kell összedobálni hozzá, és ebben az esetben a Books Online is kevesebb példát hoz, mint szeretnénk.



ábra 18: Extended Events Metadata Viewer

Ezt a problémát kiválóan orvosolja Jonathan Kehayias open source és ingyenes Management Studio add-inje, az Extended Events Manager, amit a CodePlexről lehet letölteni. Ez egy kicsit áttekinthetőbbé teszi a dolgokat, sőt, akár össze is rakhatunk egy eseményfeldolgozó szeánszot, azaz **event session**t a segítségével, illetve megnézhetjük azokat, amik már futnak. Az 1. ábrán láthatjuk az Extended Events objektumait, illetve a fastruktúra tetejét, ami felvázolja a második választ az olvasó kérdésére: kissé összetett a dolog.

Az Extended Events a hatékonyság érdekében két részre van vágva az elejétől: az **engine**, azaz az eseményfeldolgozó, és a **metaadatok**, vagyis az, hogy milyen események elérhetőek, azoknak milyen tulajdonságaik vannak, milyen módokon lehet gyűjteni az adatokat, stb. A metaadatokat **package**-ek (csomagok) tartalmazzák, amiket be lehet tölteni futásidőben is, így akár saját diagnosztikai csomagot is gyárthatnak azok, akik akarnak. Egy package a következő kategóriákba tartalmazó objektumokat tartalmazhat:

- **Events** / események: ezeket akarjuk gyűjteni, megfigyelni. A tevékenységekhez tartoznak bizonyos saját mezők, amik a rá jellemző információkat tartalmazzák. Pl. lock esetén a tranzakció id.
- **Actions** / tevékenységek: Itt tudunk további gyűjtendő mezőket megadni, tipikusan a sysprocesses tábla (akarom mondani sys.dm_exec_sessions és sys.dm_exec_requests DMV-k) tartalmait innen tudjuk hozzáadni, mivel azok az események nagyobb részénél érdekesek lehetnek.
- **Targets** / gyűjtők: Ide kerülnek a gyűjtött események. Az Extended Events elég egyedi gyűjtési lehetőségeket ajánl. Ilyen például a párosítás, ahol eseménypárokat lehet gyűjtögetni (pl. lock adása-elengedése), és páratlan események keresésére kiváló. Ott van a bucketizer is (szinkron vagy aszinkron), ami megadott számú dobozba (az angol szerint vödörbe) dobja szét a beérkező eseményeket, maximum eseményszám per vödör paraméterrel. Mellesleg fájlba is tud gyűjteni, meg ETW (**Event Tracing for Windows**) targetet is tud produkálni.
- **Predicates** / tulajdonságok: Ezekkel előszűrhetjük az eseményeket, például csak bizonyos CPU használatot elért taskoknál gyűjtünk adatot.
- **Types** / típusok: Ezeket az adattípusokat fogja ismerni az Extended Events engine.
- **Maps** / térképek: ezek felsorolások, amelyek tartalmazzák pl. a lockok típusait, a különféle várakozás típusokat, stb.

Ezek után ránézve a metaadat fára, azt látjuk, hogy három package van betöltve: a package0, az sqlserver és az sqlos. És azt is kibökhetjük, hogy a package0 egyáltalán semmiféle eseményt nem tartalmaz, szóval akkor mi értelme a létezésének? Nos, az Extended Events igen fifikás szerkezet, a betöltött package-ek egy nagy dobozba kerülnek, és az egyik package-ben definiált eseményt a másik package-ben definiált target segítségével gyűjthetjük, akár a harmadik csomagban definiált kiegészítő tevékenységek megadásával.

Ezzel az új tudással felvértezve mindent kikövetkeztetünk: a package0 az általános és az ETW-hez szükséges metaadatokat tartalmazza: itt található az összes target például. A sqlos az SQL Server operációs rendszerével kapcsolatos adatokat szolgáltatja. (Igen, az SQL Serverben van egy operációs rendszer, mert kell neki, mivel sok olyan feladatot, amit egy processznek általában az operációs rendszer kezel, az SQL Server maga szeret megoldani. Két tipikus példa a feladatütemezés és a memóriakezelés.) Az sqlserver nevű csomag meg minden mást, amit még kitaláltak.

Illetve... van egy negyedik csomag is, a SecAudit nevű. Erről azt kell tudni, hogy egy private (magyarul privát) csomag, aminek az objektumait nem használhatjuk fel saját event session létrehozása során, és ő

csak az Enterprise Editionben (pontosabban Enterprise engine-ben, azaz a developer és az evaluation is tartalmazza) található. A művelt és Millenárist megjárt olvasó itt már bólogat: igen, az **SQL Server Audit** saját kis csomagja ez, hiszen az is Extended Events alapú.

Most, hogy ennyit beszéltünk, nézzünk egy egyszerű event sessiont:

```
IF EXISTS(SELECT * FROM sys.server_event_sessions WHERE name='TechnetDemo')
    DROP EVENT SESSION [TechnetDemo] ON SERVER;
CREATE EVENT SESSION [TechnetDemo]
ON SERVER
ADD EVENT sqlserver.error_reported(
     ACTION (sqlserver.session_id, sqlserver.sql_text, sqlserver.tsql_stack,
sqlserver.username)
     WHERE ([sqlserver].[database_id]=(7)))
ADD TARGET package0.ring_buffer(
     SET max_memory=4096)
WITH (MAX_MEMORY = 4096KB, EVENT_RETENTION_MODE = ALLOW_SINGLE_EVENT_LOSS,
MAX_DISPATCH_LATENCY = 1 SECONDS, TRACK_CAUSALITY = OFF, STARTUP_STATE = OFF)

ALTER EVENT SESSION [TechnetDemo] ON SERVER STATE = START
```

Ez elég randának tűnik, de ezt Jonathan kis kütyüjével egyszerűen összedobhatjuk, aztán meg már könnyű kézzel piszkálni. Nézzük végig sorban: csináltunk egy új event sessiont, és hozzáadtuk a sqlserver package-ből az error_reported eseményt. A standard mezői mellé még a session_id, sql_text, tsql_stack és username infót gyűjtjük, szűrőfeltételünk pedig annyi, hogy a database_id (ami egy sqlserverből vett predicate) legyen 7, mert nekem az az AdventureWorks. Kell még egy target is, most egy ring buffert választottam (természetesen package0-ból), ami pont az, aminek látszik: egy meghatározott méretű memóriadarab, amibe tömjük be az adatot, és ha megtelik, a túloldalán kiesik a legrégebbi. A session viselkedését befolyásolhatjuk néhány WITH opcióval, ezek közül az egyik legérdekesebb az event retention mód, vagyis esemény megőrzés módja. Lehet egy vagy több veszteséget megengedni, vagy mondhatjuk, hogy nem lehet eseményvesztés. Ez utóbbi jó ötletnek tűnik, de ha valami nagyon sokszor bekövetkező dolgot választunk sok adattal, akkor még a könnyűsúlyú Extended Events is belerúghat a szerverünkbe. A track_causality állítja be, hogy a kauzalitást, azaz az ok-okozati összefüggéseket gyűjtse-e a session. Ez akkor lehet hasznos, ha több helyről származó adatot szeretnénk összevetni. A startup_state pedig magától értetődően azt határozza meg, hogy ha elindul az SQL Server, akkor vele induljon-e a session.
Ennyi tudás után generáljunk forgalmat:

```
USE AdventureWorks
SELECT * from AdventureWorks.HumanResources.Department d
where d.ModifiedDate > -34656456565656
-------------
Msg 8115, Level 16, State 2, Line 1
Arithmetic overflow error converting expression to data type datetime.
```

Majd nézzük meg, hogy mit fogtunk, azaz milyen események vannak a ring bufferben:

```
SELECT CAST(xet.target_data AS xml)
FROM sys.dm_xe_session_targets xet
       INNER JOIN sys.dm_xe_sessions xe
              ON (xe.address = xet.event_session_address)
WHERE xe.name = 'TechnetDemo'
```

Láthatjuk, hogy nem is egy, hanem két eseményt is elkaptunk: az első a USE AdventureWorksre adott válasz, a *Changed database context to 'AdventureWorks'*. Hm. Ez is egy message, csak olyan alacsony

severity szinttel, hogy nem is tekintjük hibának. Elég a 10 feletti severity-ket figyelni, nosza, adjuk is hozzá a scripthez ezt a feltételt is:

```
IF EXISTS(SELECT * FROM sys.server_event_sessions WHERE name='TechnetDemo')
    DROP EVENT SESSION [TechnetDemo] ON SERVER;
CREATE EVENT SESSION [TechnetDemo]
ON SERVER
ADD EVENT sqlserver.error_reported(
     ACTION (sqlserver.session_id, sqlserver.sql_text, sqlserver.tsql_stack,
sqlserver.username)
     WHERE ([sqlserver].[database_id]=(7) and severity > 10))
ADD TARGET package0.ring_buffer(
     SET max_memory=4096)
WITH (MAX_MEMORY = 4096KB, EVENT_RETENTION_MODE = ALLOW_SINGLE_EVENT_LOSS,
MAX_DISPATCH_LATENCY = 1 SECONDS, TRACK_CAUSALITY = OFF, STARTUP_STATE = OFF)
ALTER EVENT SESSION [TechnetDemo] ON SERVER STATE = START
```

Most már csak a tényleges hibát kapjuk el, úgyhogy nézzünk bele a kiváló XML kimenetbe: láthatjuk benne a tsql_stack actiont is.

```
    <action name="tsql_stack" package="sqlserver">
      <type name="unicode_string" package="package0" />
      <value>&lt;frame                                                level='1'
handle='0x0200000052DA6E07EB81796A32995BE22ED68BBCE433D912'          line='3'
offsetStart='36' offsetEnd='-1'/&gt;
&lt;frame                                                           level='2'
handle='0x020000000A9A43160C5A6FDF101DC8F793CEDA4AFC7F00A9'          line='3'
offsetStart='8' offsetEnd='-1'/&gt;</value>
      <text />
    </action>
```

Vastaggal kiemeltem a stack trace lényegét: a két handle segítségével kiszedhetjük az SQL utasításokat, a sys.dm_exec_sql_text DMF segítségével – ez legyen házi feladat mindenkinek (a megoldást majd megírom a blogomon :).

Remélem mostanra azok, akiknek a Profiler már unalmas, megtalálták következő játszótársukat az Extended Events személyében. Zárásul még egy érdekes adalék, ami SQLKlubon jött fel: SQL Expresshez nincs Profiler – viszont az Extended Events elérhető abban is, és megadja a szükséges információkat. Még egy okkal több amellett, hogy megbarátkozzunk vele!

Windows Intune – Felügyelet a felhőből

Gál Tamás

Microsoft Magyarország

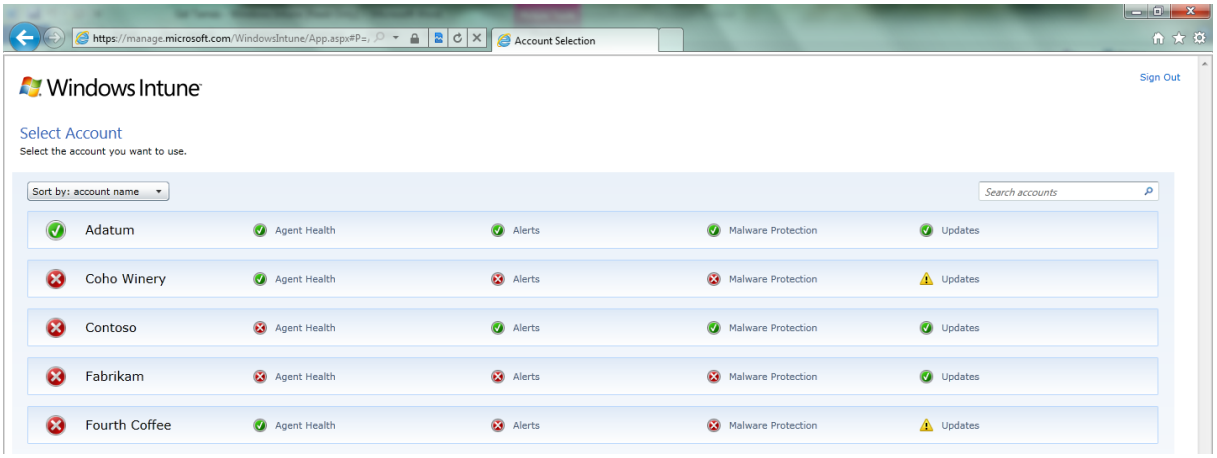
IT üzemeltetési szakértő

Forefront MVP

2010 őszére már kis hazánkban is minden a felhőről szól, Azure, AppFabric, Windows Live, ADFS, Service Bus, BPOS ezek a hívószavak - persze a teljesség igénye nélkül. Mit tehet egy ilyen helyzetben egy alapból szkeptikus és konzervatív, viszont sokat látott üzemeltetési szakember? Elkezdi megismerni a lehetőségeket, amit lehet kipróbál, és a saját tapasztalata alapján óhajt megyőződni arról, hogy van-e élet a felhőben, és ha van milyen is az?

Mi a Windows Intune?

- Röviden: egy webalapú, Silverlight-os kliens PC felügyeleti megoldás.
- Vizuálisan: egy light-os SCE (System Center Essentials) konzol, amiben van egy alapszintű, de proaktív gépfiók felügyelet, kicsi Group Policy (de nem az!), kicsi WSUS, szoftver/hardver leltár, antimalware szoftver (Forefront Endpoint Protection), és egy Remote Assistance a teljes távvezérléshez.
- Felépítés, stuktúra szintjén: a kliensek bárhol lehetnek, bent az irodában, a telephelyen, vagy akár mozgásban (pl. egy notebook).
- Konfigurálás, üzemeltetés: 95% a webes felületen, 5% a kliens gépen (igazából a felhasználó bevatkozása csak a vezérlés átvétele apropóján szükséges).
- Költség: erről nincsenek (még nem is lehetnek) pontos és végleges információim, azonban az tuti, hogy a Windows 7 Enterprise és a Forefront Client licenc benne lesz az árban, sőt egyúttal az MDOP-ra (Microsoft Desktop Optimization Pack) is előfizethetünk, és ez így együtt már igencsak kedvezményesnek tűnik.



ábra 19 Lehet több gépparkunk (szervezetünk) is a felhőben, és ezek között kapcsolgatni is teljesen egyszerű

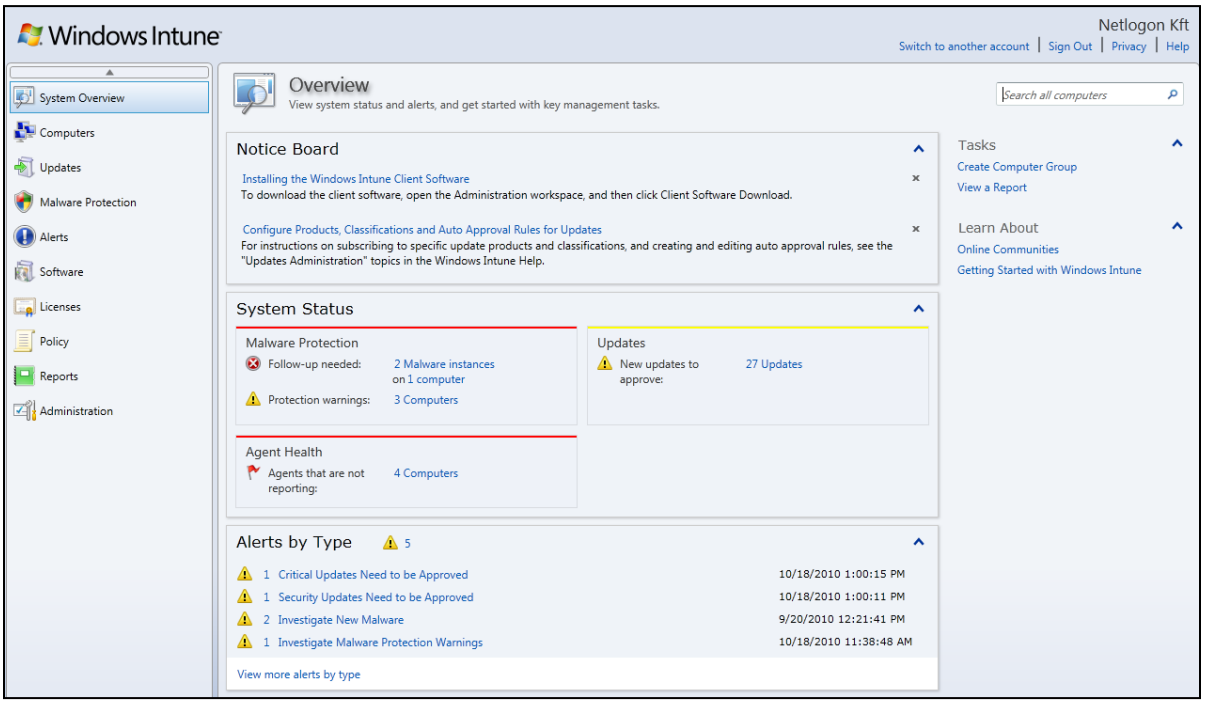
A bétáról

A cuccról bármi véglegeset mondani egyelőre nem tudok, jelenleg béta állapotban van, annyira, hogy Magyarországról nem is lehet elérni. Nekem is csak azért sikerül, mert egy speciális teszt hozzáférésem van, amely viszont szépen működik már vagy 2 hónapja. Öt gépet tartok „benne”, 4 XP SP2-öt és egy Windows 7-et (ebben a konstrukcióban 25 lenne a maximum). Mind az öt egyébként fizikailag egy

helyen van, egy klasszikus Windows tartományban, azaz egy 110 kliens gépes, 6 szerveres infrastruktúra részeként működik, ergo nem gond ha egy másik névtérnek is tagja a gép, rendeltetésszerűen használható ilyen körülmények között is.

Telepítés, üzembe helyezés

Nem mondhatni hogy megizzadtam volna a beüzemeléssel és a telepítéssel, hiszen a dolog pofonegyszerű volt. Miután kész lett a hozzáférésem beléptem a Live ID-mal a https://manage.microsoft.com oldalon keresztül az Intune-ba, majd a cégek közül kiválasztottam azt amelyikbe be akartam terelni a klienseimet (a felügyeleti gépen minimum Silverlight 3.0 kell összesen ehhez).



ábra 20: Mondom, hogy egy mini SCE

Az *Administration* pont alól letölthetőek a kliens telepítő csomagok (x86, és x64 egyaránt, de nem univerzális, hanem egyedi, azaz egy csomag az adott szervezethez van összeállítva), amelyeket le is szedtem, és irány a leendő Intune kliensek. Mely gépek lehetnek kliensek? Nincs komoly megszorítás, nézzük csak:

- Windows 7 Enterprise, Ultimate, és Professional.
- Windows Vista Enterprise, Ultimate, és Business.
- Windows XP Professional (SP 2; SP3 ajánlott)

Hardveres megszorítás sincs, amin elfut az adott OS, az jó lesz. Admin jogosultság kell, és szoftveres követelmény is van, de csak az XP SP2 esetén (Forefront Client Security Filter Manager QFE for Windows XP SP2 illetve MSXML 6.0 szükséges).

Ezek után felraktam az kliens telepítő csomagokat az öt gépre, restart, és nagyon hamar (> 5 perc) már be is jelentkeztek és a konzolon is láttam a gépeket.

Mit lehet csinálni a konzolon?

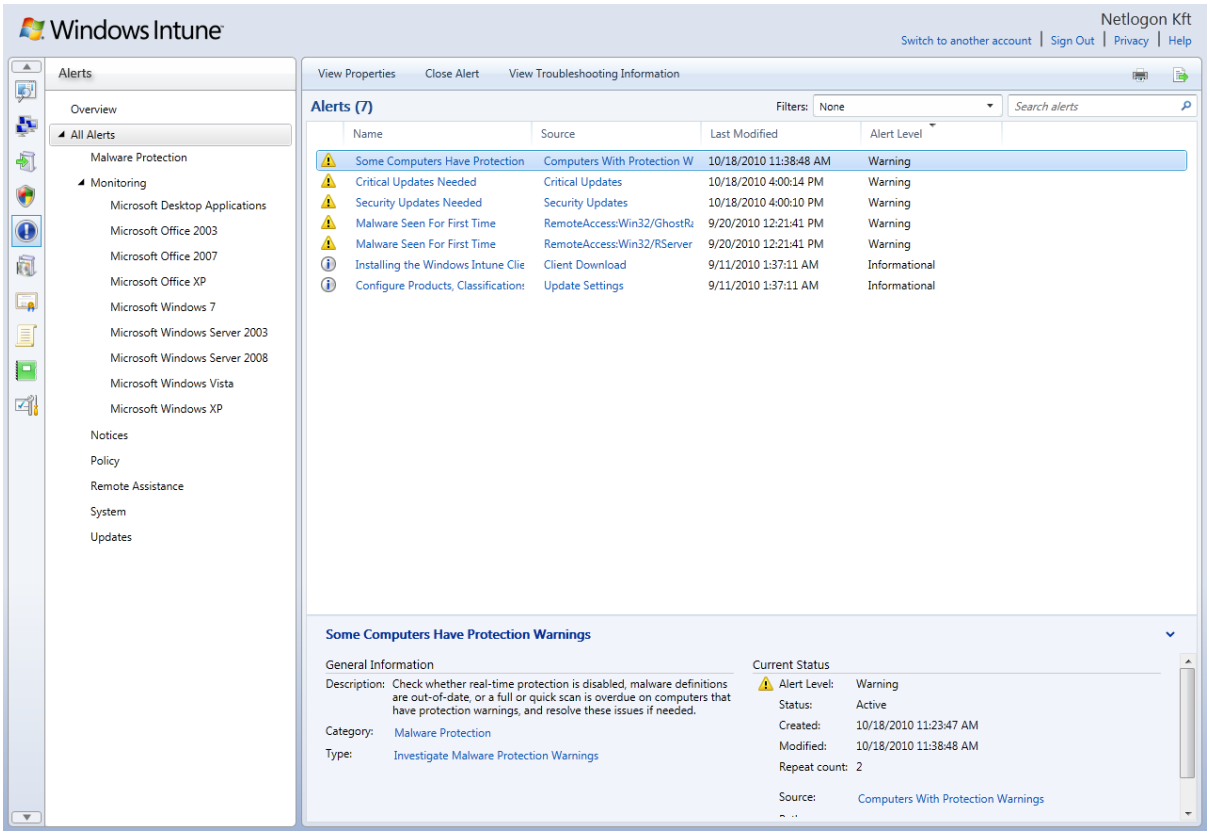
Az áttekintő képernyőről (*Overview*) már egy csomó információ és feladat elérhető (lásd a második ábrát), mint például a képernyő alján a Malware Protection alatti figyelmeztetések, vagy éppen a frissítésekre vonatkozó riasztások, vagy a tetején a kliens szoftverre utaló link, illetve a mini WSUS kezdeti konfigurációs táncára felhívó hivatkozás.

A *Computers* alatt csoportokat hozhatunk létre a WSUS-ból ismert módon. Amely gép nincs csoporthoz rendelve az a szintén ismerős *Unassigned Computers* gyűjtőbe kerül. A csoportok egymásba ágyazhatóak, és egy gép több csoportnak is lehet tagja. Itt lehet megtalálni az igazán részletes hardver leltárt is, az adott gépfiók tulajdonságai között.

Az *Updates* alatt megkapjuk a mini WSUS-t, a szokásos lehetőségekkel, illetve kissé szűkítve, merthogy nyilván nincs meg minden (pl. minek a lemezkarbantartás, vagy a proxy beállítás, ez nem a mi gondunk többé) komponens.

Malware Protection viszont nincs az SCE-ben, de itt igen. Viszont ez csak a riasztások és a statisztika formájában létezik per pillanat, mivel innen semmilyen művelet nem indítható (vagy csak én nem találtam meg.)

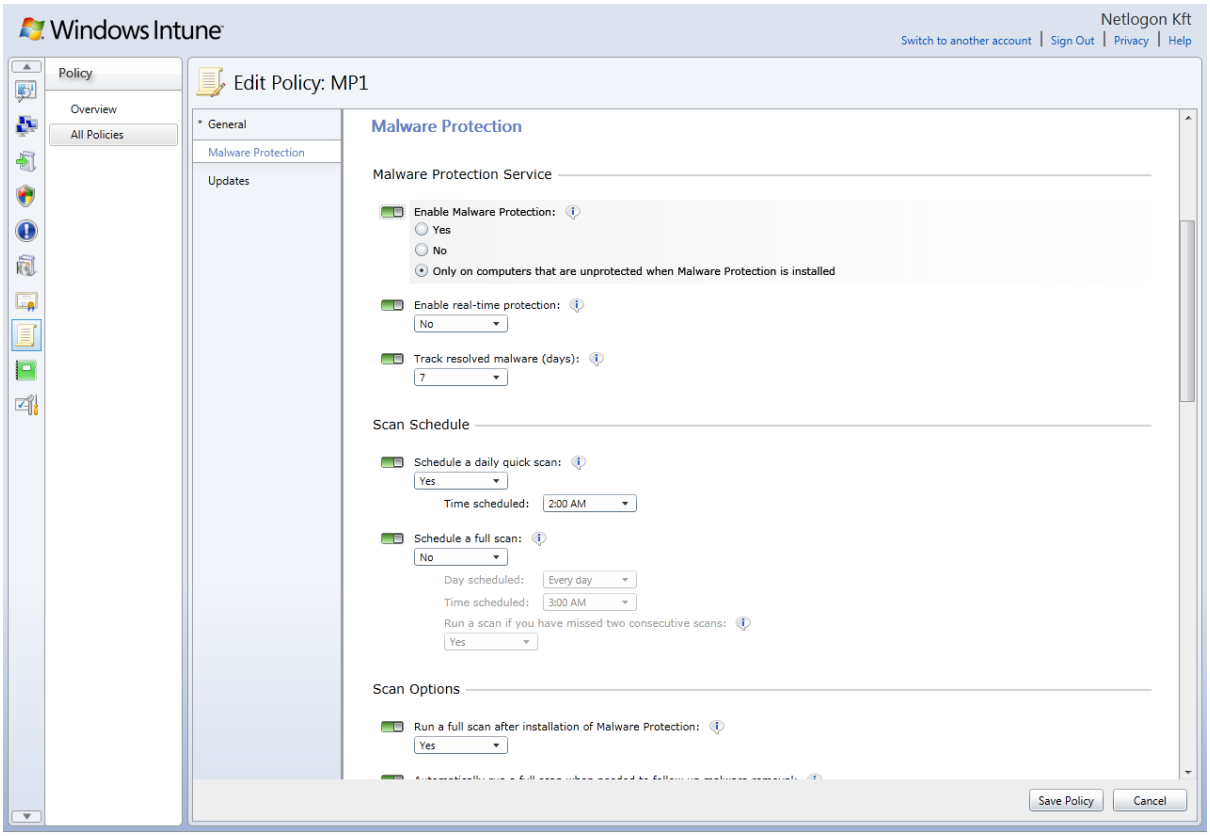
Az *Alerts* szintén ismerős lesz, az összes létező beépített szolgáltatáshoz és megoldáshoz a Malware Protection-tól kezdve a Remote Assistance-on keresztül a hardveres problémákig mindenhez kaphatunk riasztást (összesen 379 riasztási típus van), hozzárendelhetünk értesítéseket, és egyebek.



ábra 21 A riasztások szakasz

Megdöbbentő módon a *Software* pont alatt találjuk a szoftverleltárt, akár egy csoportban vagy gépenként is láthatjuk a feltelepített szoftvereket.

Ha a *Licenses* részen átugrunk, akkor jöhet a *Policy* szakasz, ahol egyelőre 3 féle házirend sablonból válogathatunk, azaz konfigurálhatjuk az Intune Agent-et, az Intune Center-t, valamint készíthetünk Windows Firewall házirendeket. Mindezeket röptében, a beállítások megtétele után, azonnal le is küldhetjük a kliensekre, a korábban említett csoportok szintjén akár eltérő módon is. Azonban jó ha tudjuk, hogy ha a gépek a földön is egy tartományban vannak, akkor a klasszikus házirendek felülírják ezeket. Nyilván ezért érdemes lenne ezeket a gépeket egy külön OU-ba tenni és a klasszikus GPO-kat blokkolni, vagy WMI-vel szűrni, vagy bármi más módszerrel izolálni - már persze ha ez a célunk. Egyébként a klasszikus házirendek és ezen házirendek között semmilyen kapcsolat nincs.

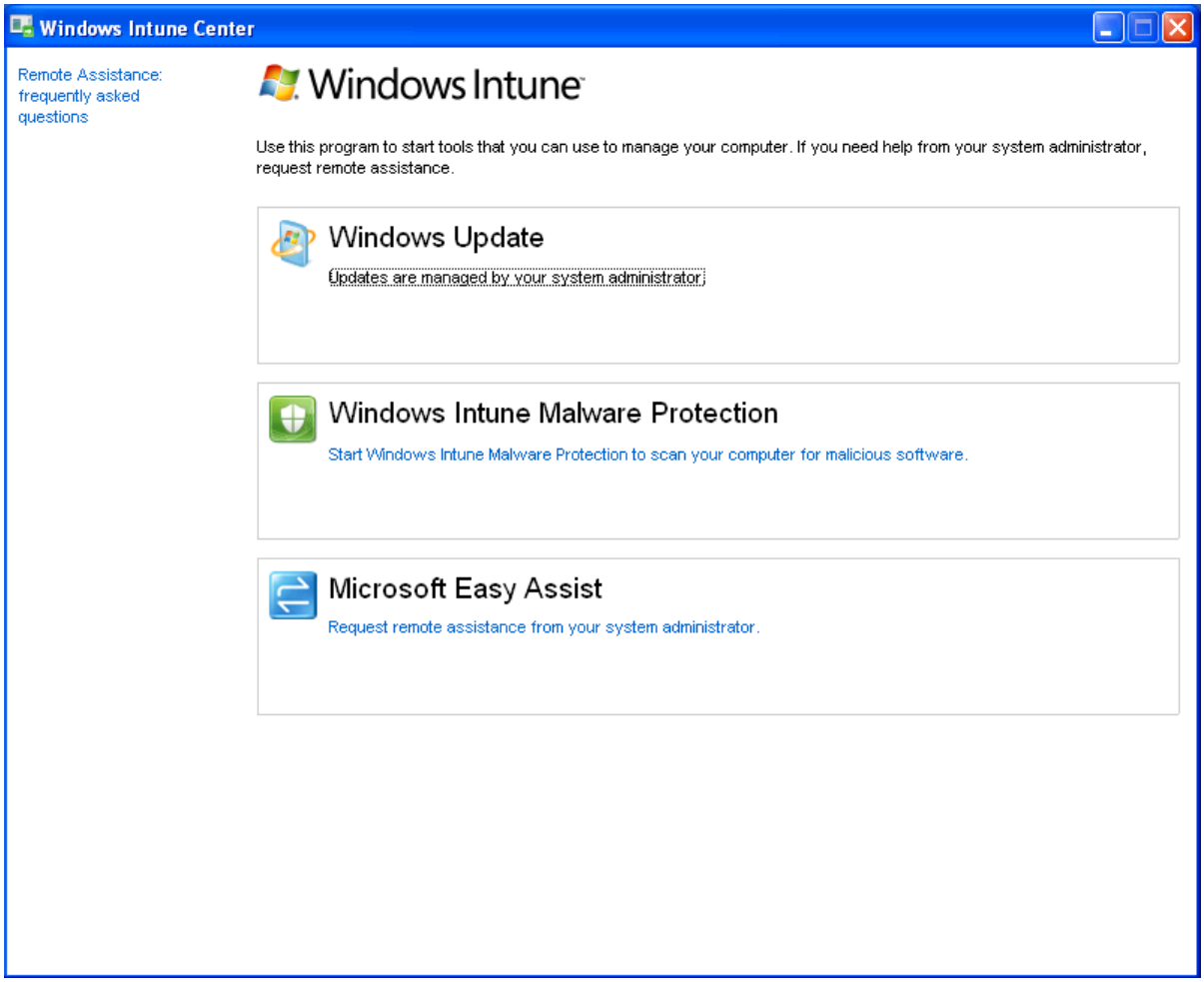


ábra 22 A Malware Protection rész egy Intune Client típusú policy.

Már csak két elem maradt az eszköztárból, a *Reports* (frissítések, licencek és szoftverek) és az *Administration*. Az utóbbi alatt a szokásos beállítások, a jogosultságok (egy szintén Live ID-val rendelkező e-mail címet kell megadnunk egy *Service Administration* szinthez, ami elvileg kissé gyengébb mint az eredeti ún. *Tenant Administrator*, de erről még nem sikerült kideríteni sokkal többet), illetve a riasztások és a frissítések opciói találhatóak meg.

Mit lehet csinálni a kliens alkalmazásból?

Ugorjunk a kliensre, ahol a kliens szoftver telepítése után egy Windows Intune Center parancsikont találunk a Windows Asztalán. Ha ezt elindítjuk, akkor a következő képet látjuk.



ábra 23 A Microsoft Easy Assist gyakorlatilag a Remote Assistance

Itt a legérdekesebb dolog az Easy Assist, amelyre ha egy felhasználó kattint, akkor az admin felületen egy *Alert* aktivizálódik, amely elvezeti az üzemeltetőt az ő gépen egy Easy Assist kliens (EASetup.exe) telepítéséig. Ha ez fent van a gépünkön, akkor elfogadhatjuk a kérést és a LiveMeeting szervereken keresztül megnézhetjük a kliens képernyőjét, a felhasználó megoszthatja velünk az Asztalát, az alkalmazásait, stb., hogy be is avatkozhassunk, de közben cseveghetünk is vele, és még van pár egyéb opció is. Mindent a felhasználó kontrollál, tehát garázdálkodni nehéz, ellenben az látszik, hogy fontos volt, hogy a felhasználó tudja kezelni (plusz az egész kliens alkalmazás már most is magyarul van).

Mikor készül el a Windows Intune?

Elvileg a jövő év (2011) közepe a cél, ergo ez egy abszolút korai bemutatkozás, ezért újra jelzem, hogy még sok-sok minden változhat Intune ügyben, de ami van, az nekem per pillanat ígéretesnek tűnik. Jópár leírás és videó viszont elérhető már most is, a http://www.windowsintune.com címen.

System Center Configuration Manager 2007 R3

Horváth Ottó

Grepton Informatikai Zrt., Support Engineer

Group Policy MVP

Lassan több mint 16 év telt el az első Microsoft alapú rendszerfelügyeleti megoldás megjelenése óta, bár kétlem, hogy túl sokan emlékeznének az akkor még Systems Management Server (SMS) 1.0 néven futó csodára. Annyira régi a termék, hogy még az interneten kutakodva is meglehetősen nehéz információkhoz jutni vele kapcsolatban. Az azért mindenképpen látszik, hogy a központi menedzsment infrastruktúra ötlete nem egy új keletű dolog. Az évek során persze rengeteget változott a termék, de azt hiszem az SCCM 2007-ben ért el olyan formát, amelyről már bizton állíthatjuk, hogy egy kiválóan hatékony és skálázható konfigurációmenedzsment eszköz. Természetesen az SCCM 2007 is folyamatosan fejlődik, az elmúlt három év alatt kettő javítócsomag és egy kiegészítő csomag jelent meg a termékhez. Jelen cikk apropója nem más, mint a második kiegészítő csomag megjelenése, amely az R3 jelölést kapta.

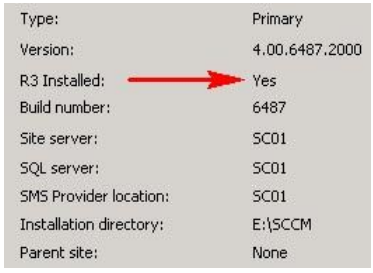
Minek is nevezzelek?

A kérdés nem csupán költői, ugyanis még sokat látott rendszermérnökök számára is elég megtévesztőek tudnak lenni az SCCM 2007-hez kiadott kiegészítések, frissítések elnevezései, főleg ha azt is megnézzük időben miként követték egymást a megjelenések.

Az R3-ról tudni kell, hogy hasonlóan elődjéhez, nem egy javítócsomagról inkább egy kiegészítőről van szó, amely új szolgáltatásokat ad az SCCM képességeihez. A kiegészítő csomagok, tehát az R széria telepítése úgymond opcionális, azaz csak akkor szükséges telepítenünk őket, ha a bennük rejlő új szolgáltatásokat szeretnénk használni.

Ettől szinte teljesen független a szervizcsomagok megjelenése, melyek nagy lélegzetvételű főként (de nem kizárólag) javításokat tartalmazó csomagok. Telepítésük az erősen ajánlott kategóriába tartozik.

Mivel a kivétel erősíti a szabályt, az R3 csak SP2-vel ellátott SCCM szerverekre telepíthető, tehát itt mégis összekapcsolódik a két dolog. Az ok nagyon egyszerű, az R3 új funkcióit kliens oldalon csak az SP2-vel frissített kliens ügynökök tudják kezelni.



ábra 24: R3 telepítve

Összefoglalva, a legfrissebb SCCM 2007 verzió jelenleg az SP2-vel frissített, a legtöbb szolgáltatást tartalmazó pedig az SCCM 2007 SP2 R3. Természetesen az R3 tartalmazza az R2 minden szolgáltatását is, így nem szükséges azokat külön telepítenünk.

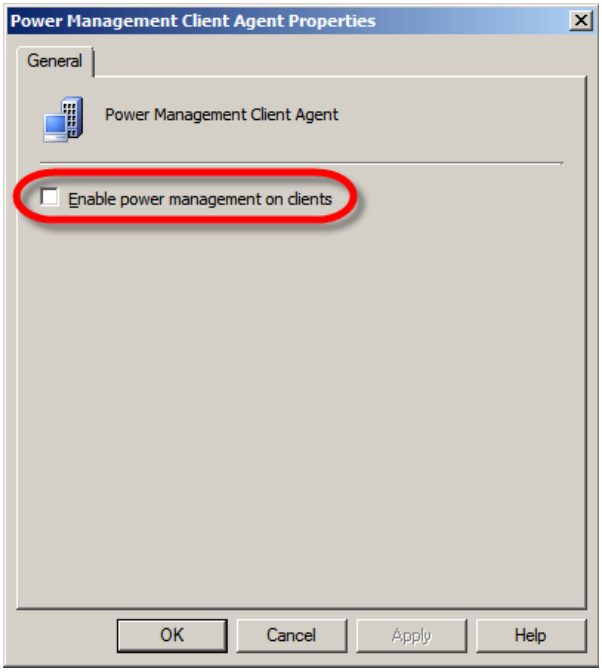
Az R3 eszközkészlete

Energiagazdálkodás

Az SCCM 2007 R3 segítségével képesek vagyunk teljes körűen szabályozni az SCCM felügyelete alá vont klienseink energiagazdálkodási beállításait, ezen felül kimutatásokat is készíthetünk szervezetünk energiahasználatáról.

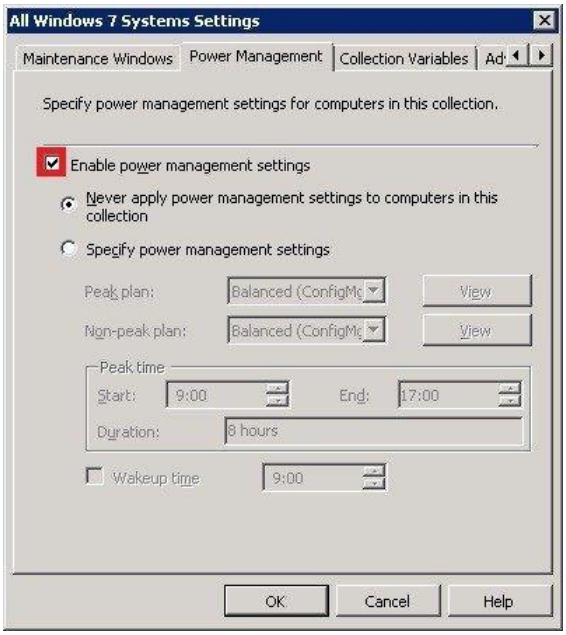
Hogyan működik?

Alapjában véve az energiagazdálkodási funkció az SCCM hardverleltárára épül, ezért ennek engedélyezése és megfelelő konfigurációja elengedhetetlen a szolgáltatás használatához. A telepítés során az R3 kibővíti az SMS_DEF.mof tartalmát az újonnan érkező osztályokkal, a fájlokat viszont nem cseréli le, így a mof fájl egyedi beállításai nem vesznek el. Ennek ellenére érdemes a mof fájlokat elmenteni a telepítés előtt. A funkció használatát két komponens teszi lehetővé, a kliens ügynök illetve a definiált energiagazdálkodási beállítások. Először magát az ügynököt kell engedélyeznünk a szokásos módon:



ábra 25: Az ügynök engedélyezése

Ezek után kezdhetünk hozzá a kívánt beállítások testre szabásához, melyeket a kollekciók tulajdonságait módosítva érhetünk el. Mindenképpen érdemes új kollekciókat létrehozni az energiasémák menedzseléséhez, legalább egy engedélyező és egy tiltó szabályt tartalmazót.

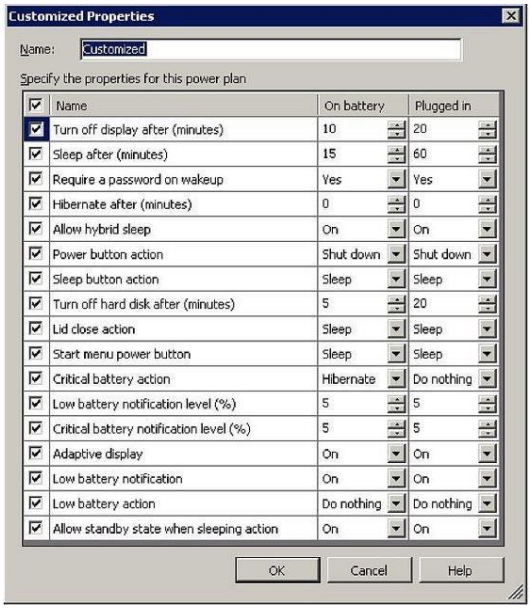


ábra 26: Energiagazdálkodás

A tiltó szabályt alkalmazó kollekcióra azért lehet szükség, mert amennyiben egy számítógép esetleg több olyan kollekciónak is tagja, amely energiasémát szabályoz, a „never apply” beállítás minden esetben megtiltja az energiasémák központi szabályozását.

Amint a képen is látható, lehetőségünk van megadni mely időszak jelenti számunkra a *munkaidőt* és ennek megfelelően különböző sémákat definiálhatunk. Ezen felül meghatározhatjuk mikor ébredjen fel a számítógép, amennyiben mondjuk éjszakai frissítést, programtelepítést vagy egyéb karbantartási műveletet szeretnénk végezni a számítógépeken. Felmerülhet a kérdés szükséges-e a WOL a gépek felélesztéséhez. Szerencsére nem, az itt beállított idő a BIOS időzítőjén alapul, amelynek segítségével például a BIOS-ban beállított időben is felébred a számítógép. Az időzítő mindaddig működik, amíg a számítógép tápellátást kap.

Érdemes egy pillantást vetni a sémák részletes beállításaira is, mivel szerencsére a lehetőség tárháza meglehetősen széles.



ábra 27: A sémák részletes beállításai

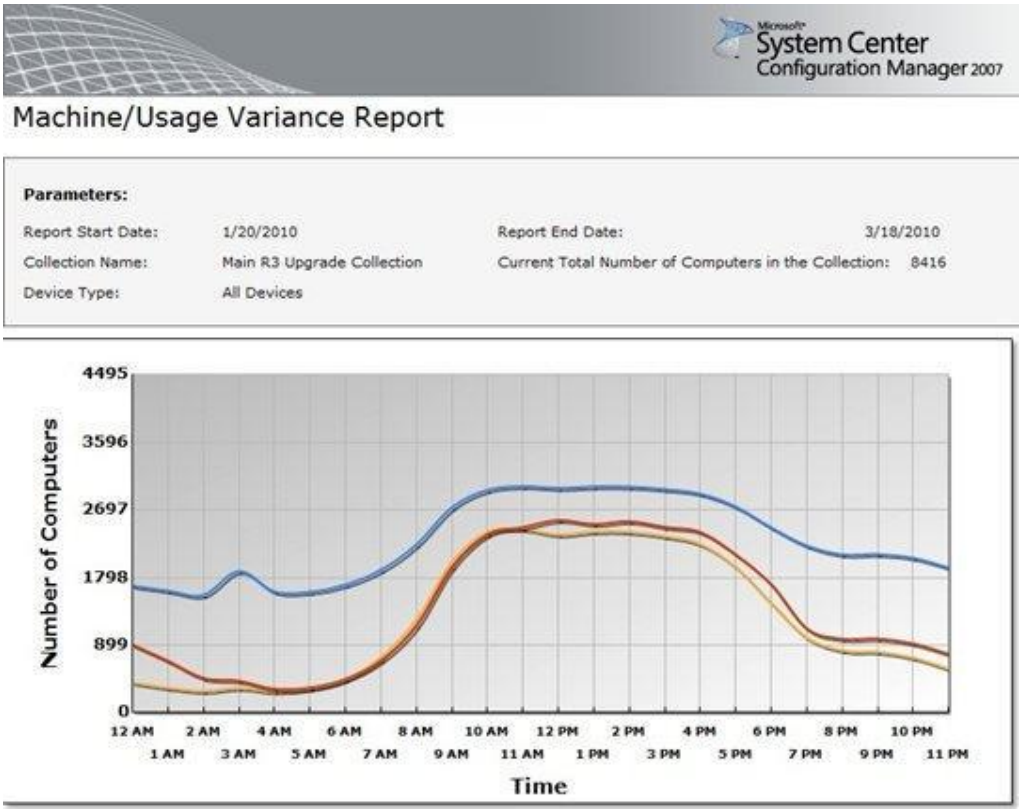
Fontos megjegyezni, hogy minden egyes kollekciónál beállított séma egyedi az adott kollekcióra vonatkozóan, tehát hiába ugyanazt a nevet látjuk a sémánál, az mindig csak az adott kollekcióra érvényes, nem pedig az összesre ahol energiagazdálkodást szabályozunk.

Érdekesség, hogy míg Windows 7 kliensek esetében a felhasználó tudja módosítani a beállításokat, Windows XP esetében erre nincsen lehetőség. Egyelőre nem derült ki, hogy programhibáról vagy tervezett működésről van-e szó. Természetesen Windows 7 kliensek esetében is csak addig maradnak érvényben a változtatások, amíg nem frissül a központi konfiguráció az SCCM szerverről. A megszokottól eltérően a művelet minden 24 órában egyszer történik meg, nem pedig minden házirend frissítéskor.

Jelentések:

Amennyiben elvégeztük a szükséges konfigurációt, bizonyára szeretnénk kimutatások formájában látni milyen megtakarítást érhetünk el az egyes konfigurációkkal, jelenleg mennyi energiát emésztenek fel a klienseink. Természetesen az SCCM riportjai biztosítják mindezen információkat, azonban pár dologra nem árt figyelnünk.

Az SCCM 2007 R3 riportjai csak és kizárólag az SQL Reporting Services funkciójával érhetőek el, a klasszikus beépített kimutatásokkal nem tudjuk megjeleníteni őket. Amennyiben tehát szeretnék az újonnan megjelent funkciókat is használni mindenképpen engedélyeznünk kell a „Reporting Services” használatát, azonban egyébként is ajánlott az SQL-es megoldás használata, mivel a következő verziókban mindenképpen ez lesz az egyetlen elérhető megoldás. Amennyiben engedélyeztük a „Reporting Services” támogatást, egyetlen dolgunk, hogy importáljuk az SCCM R3 riportjait. A szükséges .cab állomány a telepítőkészlet „Reports\Power Management” könyvtárában található. Amint megtörtént az importálás, máris elérhetjük az energiagazdálkodással kapcsolatos jelentéseket.



ábra 28: Jelentések

Utolsó megjegyzés az energiagazdálkodással kapcsolatban, hogy csak kliens operációs rendszerek esetében érhető el, a szerverek energiagazdálkodásának szabályozása jelenleg nem lehetséges, de azt hiszem nem is ez a funkció célja, ami persze nem zárja ki azt, hogy a jövőben esetleg megjelenik ez a lehetőség is.

Egyéb újdonságok:

Delta AD Discovery

A már jól ismert AD System Discovery feladat kiegészítéseként megjelent a Delta AD Discovery, melynek segítségével egy korábbi teljes felderítés óta bekövetkezett változásokat kérdezhetjük le. Előnye, hogy jóval gyakrabban futtatható a címtárban történt változások keresése céljából, mivel kevésbé terheli az AD infrastruktúránkat, mint a teljes szinkronizáció, hiszen nem szükséges minden objektum minden paraméterének lekérdezése.

Dyanamic Collection Updating

A kollekciók tartalmának frissítése normál esetben szintén 24 óránként történik meg, amely főként az operációs rendszer telepítési folyamata, illetve az első ügynöktelepítés után okozhat sok fejfájást az SCCM-t üzemeltető rendszergazdáknak. Ennek következtében akár az is előfordulhat, hogy egy dinamikus kollekcióra kihirdetett program csak egy nappal az ügynök telepítése után kerül ki a célcsoport klienseire. Ezt a problémát igyekszik orvosolni a dinamikus kollekció frissítés, mely az alábbi négy esetben használható:

- Első alkalommal felderített rendszerek esetén
- OSD eljárással telepített kliensek első felderítésekor
- Első hardverleltár készítése során
- SCCM kliensek verziójának frissítése után

A fentiektől eltérő esetekben a normál kollekciófrissítési metódus érvényes.

PreStaged Media

Az SCCM szoftvertelepítési képességét használók számára biztosan ismerős már a PreStaged vagy más néven OEM média fogalma, hiszen az MDT integrációval már elég régóta elérhető ez a típusú telepítés eljárás az SCCM-ben. Az R3-ban viszont már natív SCCM képességgé vált az OEM telepítőkészletek készítése, azaz létrehozhatunk egy olyan telepítőkészletet amelyet előtelepíthetünk a kiszemelt klienseinken, majd a telephelyre szállítva erről az állapotról folytatódhat a telepítés a különböző szekvenciák futtatásával. Azaz megspóroljuk magának az alap lemezképnek (WIM fájlnak) a hálózaton át történő telepítéséhez szükséges időt.

Előfeltételek

Az R3 telepítéséhez minimum SCCM 2007 SP2-re van szükségünk ugyanis az új képességek használatához az SP2-es verziójú kliens szükséges. Továbbá szükségünk lesz a KB977384 jelzésű javításra, mind a szerveren mind az összes felügyelni kívánt kliensen. A javítócsomag telepítésekor a varázsló segítségével automatikusan létrehozhatjuk a javítás terítéséhez szükséges csomagot és programot is. A hirdetmények létrehozása és kollekciókhoz rendelése a mi feladatunk marad.

Operációs rendszer telepítés SCCM használatával – 1.rész

Horváth Ottó

Grepton Informatikai Zrt., Support Engineer

Group Policy MVP

Az operációs rendszer telepítésről általában

Amint a címből is kitűnik a következő rövid leírásban az operációs rendszer telepítésről lesz szó, természetesen nem a hagyományos értelemben vett Windows telepítőlemezes „kattintgatós” telepítést fogom részletezni.

Milyen telepítési metódusokat is ismerünk?

Az otthoni felhasználók esetében megszokott az úgynevezett telepítőlemezes telepítési eljárás, amikor a Windows lemezünket használva a varázsló segítségével telepítjük az operációs rendszert. Természetesen egy vállalati, főleg nagyvállalati környezetben nem alkalmazható több okból sem.

Telepíthetjük az operációs rendszert előre elkészített lemezképeket felhasználva is, néhány évvel ezelőtt erre egy elfogadott módszer volt például a Symantec Ghost és hasonló alkalmazások használata. A megoldás előnye, hogy a lemezkép tartalmaz minden szükséges beállítást és alkalmazást, de a testreszabhatóság és a dinamikus telepítőkészlet készítés nagyon korlátozott. Másrészt ezen módszerek egyáltalán nem támogatottak illetve Windows Vista utáni rendszerek esetében rengeteg kompatibilitási problémát okozhatnak, ezért nem is ajánlottak.

A harmadik típusú eljárás az automatizált telepítés, melynek megkülönböztetjük két válfaját, melyeket LTI és ZTI betűszavakkal szokás jelölni. Az LTI (Lite Touch Installation) típusú megoldásokkal kis emberi beavatkozással tudjuk nagyszámú kliensre telepíteni az operációs rendszert, ZTI (Zero Touch Installation) metódus esetében egyáltalán nem szükséges emberi beavatkozás a telepítési folyamat közben, azon kívül, hogy távolról elindítjuk az eljárást.

A Microsoft rendszerek világában a LTI eszköze az MDT (Microsoft Deployment Toolkit) amely egy dokumentációkat, automatizmusokat, menedzsment eszközöket magában foglaló csomag, mely a WAIK-re, WDS-re épülve lehetővé teszi az operációs rendszerek tömeges telepítését.

A ZTI eszköze, mely a cikk témája is lesz, elsősorban a SCCM, amely magában is képes a ZTI típusú telepítések elvégzésére. Azt viszont mindenképpen tudni kell, hogy a maximális testreszabhatóság és a legszélesebb funkciókészlet használatához a SCCM és a MDT együttes alkalmazása javasolt. Ugyanis az MDT nem csak az LTI, de a ZTI módszerhez is tartalmaz eszközöket, viszont ezek mindegyike a SCCM-re épül.

Milyen feladatokat valósít meg az automatizált operációs rendszer telepítési képesség?

Az SCCM és MDT integrációja a következőket teszi lehetővé számunkra:

- Telepítőkészlet elkészítése és testre szabása beavatkozás nélkül
- Alkalmazások integrálása a telepítőkészletbe meghatározott szabályok alapján
- Operációs rendszer telepítése és teljes körű testre szabása meghatározott szabályok alapján
- Operációs rendszerek migrációja, felhasználói adatok mentése és visszatöltése

- A migrációt megelőzően biztonsági mentések készítése
- A korábbi operációs rendszer virtuális géppé konvertálása és azonnali csatlakoztatása Windows VPC-vel
- Aktuális frissítések integrálása a telepítési folyamat közben
- Automatikus driver telepítés

Amennyiben egyszer elkészítettük a telepítési eljárást, minden automatikusan történik további emberi beavatkozás nélkül. Leszámítva persze a hibakezelést. ☺

A gyakorlat - Első lépesek

Ugyan rendelkezem már egy éles infrastruktúrával ahol a következőkben ismertetésre kerülő eljárás tökéletesen működik és több éles bevetésen is bizonyított már, a hitelesség és a demó kedvéért kiépítettem virtuális környezetet ahol lépésről lépésre bemutatom az OSD képességhez szükséges eszközök telepítését és konfigurálását. Így remélhetőleg egyetlen lépés sem fog kimaradni, hiszen én is lépésről lépésre a leírtakat követem.

Ahonnan elindulunk:

A kezdéshez kialakítottam egy nagyon egyszerű SCCM infrastruktúrát, amely mindössze egyetlen központi szerverből és néhány kliensből áll. Az operációs rendszer Windows Server 2008R2, melyre egy SQL Server 2008R2 került.

Megjegyzés, éles környezetben is ajánlott az SCCM szerveren elhelyezni az SQL adatbázist, akármennyire is furcsán hangzik. Az SCCM rengeteg adatbázis műveletet végez működése során, ezért kiemelten fontos, hogy az SQL adatbázis elérése minél nagyobb sebességű legyen. Viszont azt kell mondanom, ez hálózaton keresztül az esetek nagy többségében lassabb, mint a helyi szervert használva ahol a memórián keresztül tudnak kommunikálni a komponensek. Ezt a sebességet semmilyen hálózati adapter nem tudja biztosítani. A Microsoft ajánlása alapján a dedikált szerveren üzemeltetett SQL nagyobb teljesítményt biztosít, de valójában csak 100k számítógép felett válik erősen ajánlott konfigurációvá a szeparálás. Természetesen ebben az esetben dedikált minimum gigabites kapcsolat szükséges. Tapasztalataim alapján még a magyar viszonylatban nagyvállalatok esetében is gyorsabb a site szerveren futó SQL-es megoldás, mint a különválasztott infrastruktúra, természetesen a Site szerver számítógépnek megfelelő erőforrásokkal kell rendelkezni, ami SQL esetében főleg nagyon sok memóriát jelent. 8GB alatt nem érdemes próbálkozni a legkisebb környezetekben sem. ☺

Szóval vissza a demó környezethez. Az operációs rendszer és adatbázis telepítése után felkerült a SCCM 2007 SP2-es verziója majd az R2 is. A Windows 7 terítéséhez mindenképpen szükséges mind az SP2 mind az R2, előbbi a Windows 7 támogatáshoz, utóbbi az ismeretlen számítógépek támogatásához. A telepítést követően csak a legfontosabb dolgokat konfiguráltam, úgy mint felderítési módok, „Network Access Account”, kliens terítés, „boundaries”, Egy korábbi cikkemben már említettem, milyen problémákba ütközhet az ember, ha figyelmetlen a telepítés közben:

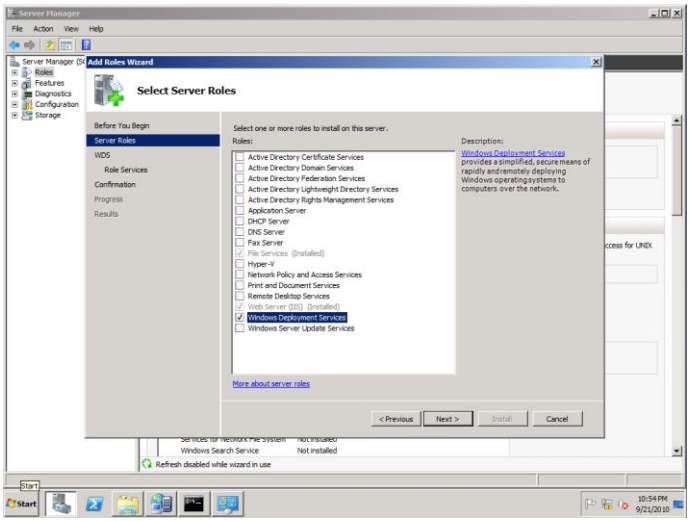
SCCM 2007 telepítés, ahol a varázsló kevés

Ha minden rendben, az SCCM működik, a kliensekre települt az ügynök, kommunikálnak is egymással, jöhet az OSD környezet előkészítése.

Komponensek telepítése

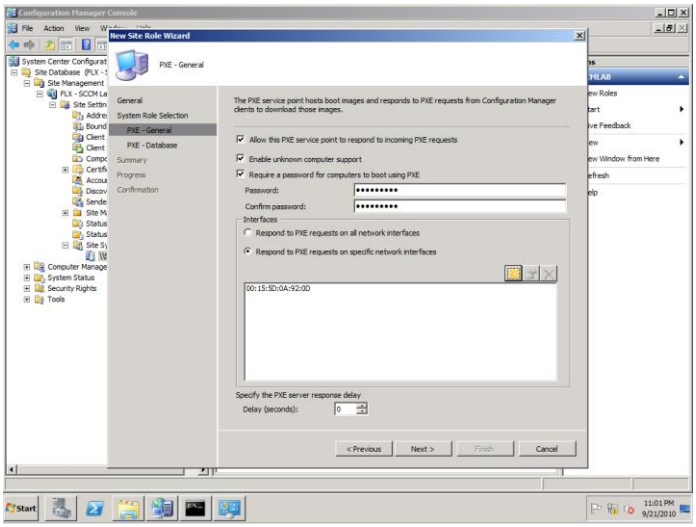
Az első és legfontosabb teendőnk a PXE Service Point telepítése, mely gyakorlatilag egy normál PXE szolgáltatás kombinálva egy kis WDS-sel. Nagyon fontos, hogy a lépéseket pontosan kövessük, mert amennyire egyszerűnek látszik a dolog annyi hibát tud okozni a későbbiek során, ha az elején elrontjuk a telepítést és az alapbeállításokat.

Első lépésben telepítsük a WDS szolgáltatatást a szerverünkre. A telepítés után ne konfiguráljuk be a WDS szolgáltatást, ne próbáljuk meg elindítani a services.msc-ből, csak hagyjuk abban az állapotban, ahogy a varázsló konfigurálta.



ábra 29: WDS telepítés

Jöhet a PXE service Point telepítése



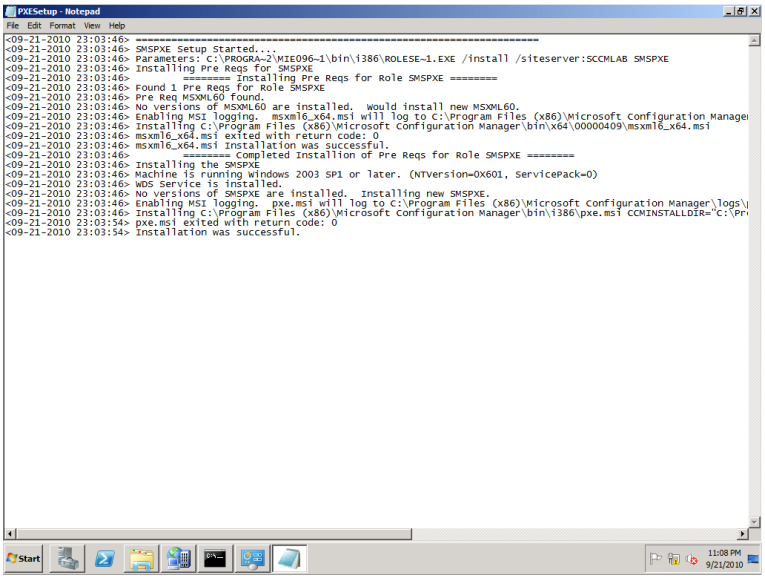
ábra 30: PXE service point telepítés

- *Allow the PXE service point to respond to incoming PXE requests*
  Ez a beállítás engedélyezi, hogy a PXE szerepkör egyáltalán válaszoljon a hálózati kliensek felől érkező PXE kérésekre, tehát mindenképpen szükséges beállítanunk.

- *Enable unknown computer support*
  Az ismeretlen számítógépek támogatása abban az esetben jöhet jól, ha nem szeretnénk az újonnan vásárolt, SCCM-et még soha nem látott gépeink MAC vagy GUID számát felvinni az SCCM-be a telepítés megkezdése előtt. Az opció bekapcsolásával minden ismeretlen számítógépen elindul a PXE boot és megfelelő konfiguráció esetén a telepítés is.

- *Require a password for computers to boot using PXE*
  Amennyiben az ismeretlen számítógépek támogatását engedélyeztük, nagyon fontos ennek a korlátozásnak a használata is, mivel nem szeretnénk ha egy véletlen hálózati boot után a klienseink magukra rántanának egy új Windows verziót, ezért követeljük meg a felhasználónévhez és jelszóhoz kötött telepítést.

A telepítés sikerességét a pxesetup.log fájlban ellenőrizhetjük. Sajnos a varázsló sok esetben akkor is sikeres telepítést jelez, ha bizonyos részfeladatok vakvágányra futottak a telepítés közben.



ábra 31: Pxesetup.log

Az így elkészült infrastruktúra alapjában már használható lenne az operációs rendszer telepítési képesség használatára, azonban a magasabb fokú testreszabhatóság és az egyszerűbb kezelhetőség miatt néhány további kiegészítő telepítése ajánlott.

MDT 2010

Az OSD képesség teljes kiaknázásához kimondottan ajánlott az MDT telepítése, amely önmagában is használható operációs rendszerek telepítésére, azonban csak LTI módszerrel. Mi viszont ZTI megoldást szeretnénk, hiszen ezért is használjuk az SCCM-t, így az SCCM - MDT páros a barátunk. A telepítés

meglehetősen egyszerű, amit nem szabad elfelejteni az a telepítés végén az integrációs varázsló futtatása, ugyanis ezzel regisztráljuk be a szükséges komponenseket az SCCM-be.

A folytatás…

Ezen a ponton el is érkeztünk oda, hogy rendelkezésünkre áll az OSD képesség használatához szükséges infrastruktúra, de természetesen még rengeteg lépés van hátra ahhoz, hogy csak hátradőlve várjuk a Windows telepítések elkészültét. A telepítési folyamatot az SCCM-ben és az MDT 2010-ben is egy úgynevezett Task Sequence írja le, amely gyakorlatilag nem más, mint a telepítési folyamat egymást követő lépéseinek meghatározása, egy folyamatábra, ha úgy tetszik. A cikk következő részében ezen folyamatleírások készítését és alkalmazását fogom bemutatni.

SCCM v.Next

Horváth Ottó

Grepton Informatikai Zrt., Support Engineer

Group Policy MVP

Azt hiszem a System Center termékcsalád és annak konfigurációmenedzsmentért felelős tagját senkinek nem kell bemutatnom. Ha nem is üzemeltetünk mindannyian SCCM-et napi szinten, de legalább előadások, cikkek révén biztosan mindenki kapcsolatba került már vele. A termék régóta jelen van a piacon, nagyon sok változáson és komoly átalakításon ment keresztül és ez a jövőben sem lesz másként. A napokban jelent meg a SCCM 2007 R3-as kiegészítő csomagja, és már javában készül a következő generáció is, mely jelenleg v.Next kódnévre hallgat. A következőkben ezen verzió újdonságairól lesz szó, nagyrészt csak elméleti síkon, mivel az első béta verzió csak az újdonságok kis részét tartalmazza, ezért a gyakorlati bemutatás még nehézkes lenne.

Mi változott?

A jelenlegi információk alapján úgy tűnik, hasonló léptékű változásnak lehetünk szemtanúi, mint korábban az SMS 2003-ról SCCM 2007-re történő váltás során. Természetesen a termék alapvető felépítése most sem változik lényegesen, az viszont már most nagyon jól látszik, hogy a terméket egy új szemléletmód mentén próbálták kialakítani.

Felhasználó központú menedzsment

A V.Next-ben a kliens központú menedzsment szemléletmódot egy sokkal inkább felhasználó központú szemléletmód váltja fel, azaz minden menedzsment eszköznek és eljárásnak az alapja maga a felhasználó lesz, ellentétben a korábbi inkább számítógép központú felfogással. Ez segíti mind a felhasználókat mind az üzemeltetőket, előbbieket abban hogy az alkalmazásokat és konfigurációs beállításokat egyszerűen és hatékonyan eljuttassák a célfelhasználókhoz, utóbbiakat pedig abban hogy ezen konfigurációs paraméterek, alkalmazások minden esetben kövessék őket attól függetlenül, hogy pontosan milyen földrajzi helyről vagy milyen eszközről dolgoznak éppen.

Rugalmas alkalmazás terítés

Az előzőekben említett felhasználó központú menedzsment megvalósításának egyik eszköze az úgynevezett rugalmas alkalmazásterítés, amely képessé teszi a rendszert arra, hogy intelligens módon különböző rendszerállapotokra reagálva különböző módokon juttassa el a felhasználókhoz a nekik szükséges konfigurációs paramétereket, elsősorban alkalmazásokat. Mindezt egy új alkalmazásmodell használatával valósítja meg, melyben minden alkalmazást csak egyetlen alkalommal szükséges definiálni, majd azokat különböző csatornákon keresztül tudjuk telepíteni, például virtuálisan, prezentációs szerverek felé, vagy a hagyományos alkalmazásterítési eljáráson keresztül. A folyamat során megkülönböztetésre kerülnek a felhasználók elsődleges illetve másodlagos eszközei, melyek a számukra megfelelő módon kaphatják meg az adott alkalmazásokat. Egyszerűbben mondva, a szerver képes eldönteni, hogy az adott eszközünk számára milyen módon juttatható el az adott alkalmazás és a lehetőségek közül a legoptimálisabb módot fogja választani. Amennyiben az adott eszközre például nem telepíthető egy alkalmazás, azt eljuttatja virtuálisan vagy akár streaming segítségével.

Igény szerinti alkalmazás elérés

Szintén a felhasználó alapú megközelítés ismérve, hogy a végfelhasználók számára elérhetővé tehetünk egy önkiszolgáló felületet, melyen kiválaszthatják a publikált alkalmazások közül azokat melyek számukra szükségesek, majd elindíthatják annak telepítését. Ezzel jelentősen csökkenthető az alkalmazásigénylések miatt keletkezett helpdesk bejelentések száma és ezáltal az üzemeltetők ráfordításai is.

Egységes menedzsment felület

A jövőben a Configuration Manager felülete lesz az a felület ahonnan minden menedzsmenttel kapcsolatos terméket és funkciót koordinálhatunk, és itt most nem kizárólagosan az SCCM képességeire kell gondolnunk. A központi menedzsment infrastruktúra jelenleg a következő termékek konfigurációját képes megvalósítani:

- APP-V
- Med-V
- Citrix Xen App

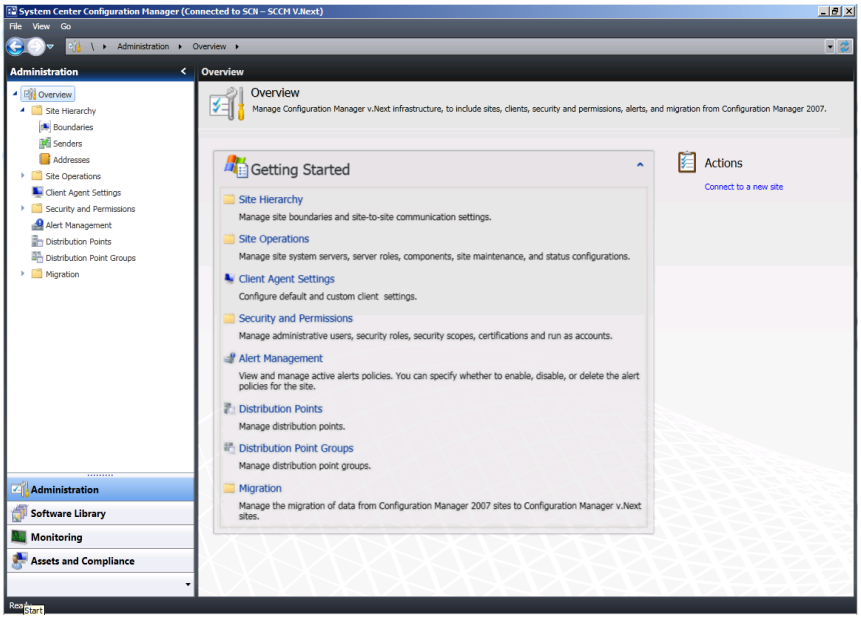
Továbbá az sem titok, hogy a korábban Mobile Device Manager néven ismert szintén a System Center család részét képező mobil eszközök kezeléséért felelős termék teljes egészében beolvad az SCCM alá, illetve a Forefront Endpoint Protection 2010 is kizárólag az SCCM-en keresztül lesz használható.

Megfelelőség

A V.next-től kezdődően a kliens oldalon is megjelent a megfelelőség ellenőrzésének lehetősége, azaz meghatározhatunk klienseink számára egy olyan kívánt állapotot melytől való eltérést monitorozhatunk illetve automatikusan korrigálhatjuk azt. A szolgáltatás kísértetiesen hasonlít a Windows Server 2008-ban megjelent NAP lehetőségre, ahol a kliensek állapotától tehettük függővé a hálózati hozzáférésüket. Ezzel együtt megjelenik az úgynevezett öngyógyító kliens fogalma is, melynek használatával klienseink egészségi állapota akkor is korrigálható, amennyiben magát a kliens ügynököt már eltávolították az adott eszközről. Egyelőre nem teljesen tisztázott miként fog működni ez a funkció, de nagyon érdekesnek hangzik, remélem egy következő béta verzióban már több részletet is megtudhatunk.

Adminisztráció

Ha ránézünk a következő képre, látható, hogy radikálisan megváltozott az SCCM menedzsment felülete és azt is elárulhatom, ez még nem a végleges megjelenése a konzolnak. Például a második béta verzióban máris másként fest. Ahogy megfigyelhető, különböző kategóriákba szedve és funkciók szerint csoportosítva érhetőek el a különböző opciók, nem a korábban megszokott ömlesztett fa struktúrában. Azt hiszem, mondhatjuk, hogy a funkciók bővülése során egyre inkább átláthatatlanná vált az SCCM kezelőfelülete, tehát éppen ideje volt a váltásnak.



ábra 32: Az SCCM konzol

Természetesen a felület nem minden. Olyan újdonságok jelentek meg az adminisztráció terén, mint például a RBAC (Role Based Access Control), amelynek segítségével a különböző szerepkörrel rendelkező kollegák számára szabhatjuk testre a megjelenő funkciókat, és mindenki csak ahhoz fér hozzá amire a munkájához feltétlenül szüksége van. Jelenleg összesen 13 ilyen szerepkör található beépítve a termékben.

(Icon)	Name	Type
	Application Administrator role	Built-In Role
	Application Deployment role	Built-In Role
	Application Editor role	Built-In Role
	Asset Analyst role	Built-In Role
	Asset Management role	Built-In Role
	Compliance Settings Management role	Built-In Role
	ConfigMgr Administration role	Built-In Role
	Hierarchy Administrator	Built-In Role
	Mobile Device Analyst role	Built-In Role
	Operating System Deployment Management role	Built-In Role
	Read-only role	Built-In Role
	Remote Tools role	Built-In Role
	Software Updates Management role	Built-In Role

ábra 33: Szerepkörök

Integrált platform

Az SCCM fő célja minden esetben a kliensek teljes életciklusának követése, támogatása. Az SCCM lefedi a teljes folyamatot melynek részei az OS és alkalmazások telepítése, frissítések terítése, konfigurációkezelés, majd a kliensek nyugdíjazása. Ezen felül a platform egy integrált megoldást kíván nyújtani, amely egyéb Microsoft alapú megoldásokkal közösen együttműködve tudja még hatékonyabbá tenni az infrastruktúra üzemeltetést és támogatást. A teljesség igénye nélkül ilyenek például a

BranchCache, DirectAccess, USMT, ACT. Természetesen nagyon fontos a többi System Center termékcsalád többi szereplőjével történő szoros együttműködés is, ezek közül talán leginkább kiemelendő a sokak számára valószínűleg még ismeretlen System Center Service Manager mellyel együttműködve megvalósítható az automatikus incidens- és változáskezelés.

Kompatibilitás

Úgy gondolom a cikk vége felé közeledve egyre inkább érezhető, hogy az új verzióban várható változások és az üzemeltetéshez szükséges szemléletmód váltás miatt az átállás nem lesz feltétlenül egyszerű folyamat , ezért mindenképpen érdemes néhány szót szólni a kompatibilitási kérdésekről. Gondolok itt arra, hogy vajon mi lesz a már meglévő SCCM2007 vagy akár SMS2003-as infrastruktúrák sorsa a jövőben.

Természetesen a megjelenéskor már rendelkezésre fognak állni azon eszközök melyekkel megtehetjük a korábbi rendszereink direkt migrációját, ideértve az alkalmazásokat, klienseket, riportokat stb. Valószínűleg azon vállalatok lesznek kevesebben, akik egyik napról a másikra direkt migrációval cserélik le már meglévő SCCM infrastruktúrájukat, és úgy gondolom a fejlesztők sem voltak más véleményen. Lehetőség lesz ugyanis arra, hogy szép apró lépésekben térjünk át az új felhasználó központú szemléletmódra, miközben még a régi kliens centrikus módszereket is használjuk a rendszereink menedzselésére. Azt hogy ezt pontosan milyen formában fogják biztosítani sajnos még nem ismert, de a megjelenésig még majd egy év van hátra, így nyugodtak lehetünk, hogy van idő ezt is részletesen kidolgozni.

Összefoglalás

A cikk zárásaként csak annyit, hogy mindenképpen ajánlatos figyelni a következőkben megjelenő béta verziókat főleg a 2011 év elején megjelenő második béta lehet majd érdekes, mert minél előbb elkezdjük tanulni az új eszközöket és szemléletmódot annál egyszerűbb lesz az átállás megtervezése és kivitelezése. Természetesen a Technetklub és a magazin hasábjain is rengeteget fogunk még foglalkozni a V.Next képességeivel, amint újabb és pontosabb információk állnak rendelkezésünkre.

Utószó

Muszáj megjegyeznem itt is, hogy nagyon korai fázisban van a fejlesztés, egyelőre publikusan csak Béta1-es verzió érhető el, és csak 2011 első felében várható a Béta 2 megjelenése, ezért minden itt leírt információ a jelenlegi terveket és állapotot tükrözi, azok bármikor változhatnak. Abban azért biztos vagyok, hogy az alapvető koncepció nem fog lényegesen módosulni a megjelenés napjáig.

A Felhő felületén

Varga Gábor

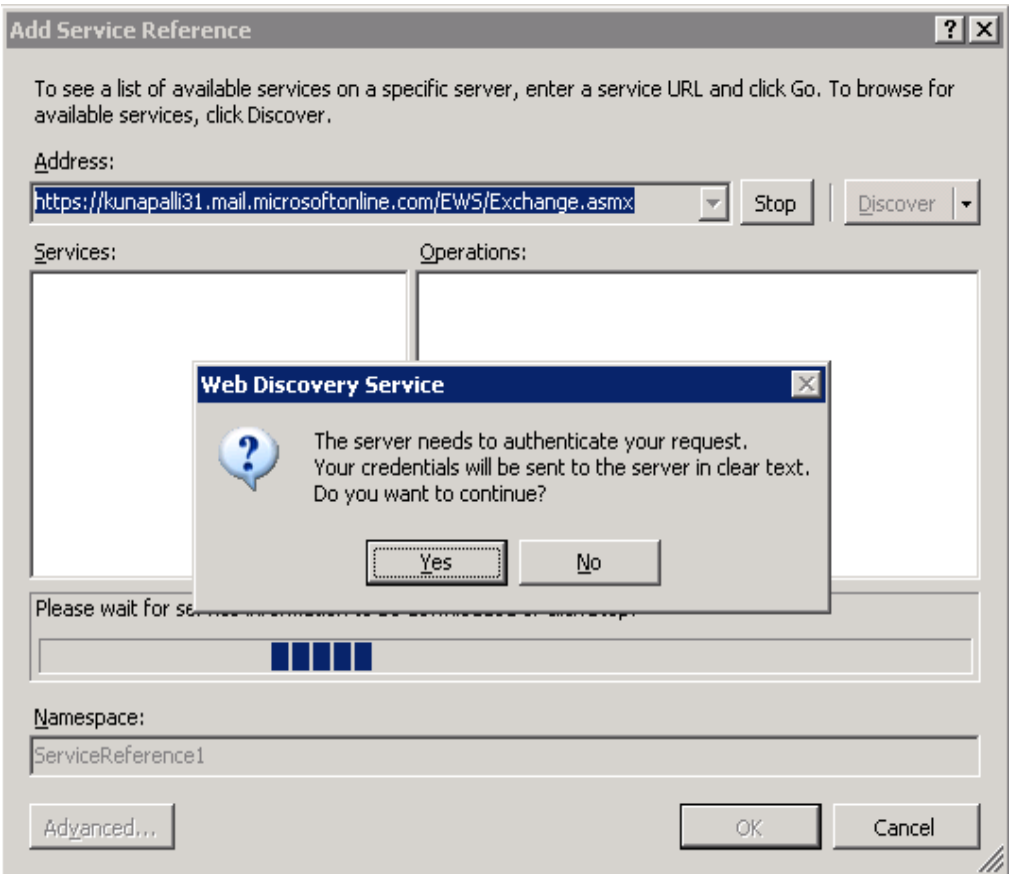
Microsoft Magyarország kft.,

Megoldásértékesítési tanácsadó

A Microsoft Online Services, közkeletű néven a BPOS (Business Productivity Online Services) a Microsoft jól ismert vállalati alkalmazásainak új megjelenési formája: ahelyett, hogy például a Microsoft Exchange-et telepítenünk kellene saját szervereinkre a felhasználás helyén, a Microsoft már adatközpontjában telepítette, és a felhasználóknak hozzáférést nyújt az Exchange funkcióihoz. A felhasználók ugyanazokat a funkciókat használhatják, mint a jól ismert és megszokott, helyben telepített (on-premise) esetben, mégsem kell a rendszerek telepítésével járó manuális munkát elvégeznünk. Más szóval az informatikai erőforrást kihelyeztük a Felhőbe, de továbbra is helyben vesszük igénybe azt.

Mindez azonban nem jelenti azt, hogy egy megközelíthetetlen, fekete dobozt használnánk, amelybe még az értő szemű adminisztrátor sem pillanthat bele. A Felhőben lévő fekete dobozon a Microsoft nemcsak a felhasználóknak, hanem az adminisztrátoroknak, sőt a fejlesztőknek is nyitott ablakot.

Jó hír: Mivel a Microsoft a korábban már jól ismert termékeit helyezte át a Felhőbe, sok technikai felület megegyezik a megszokott Microsoft termék által nyújtott felülettel. Aki járatos például az Exchange Web Services (EWS) programozási felület használatában, ugyanezt az API-t meg fogja találni az Exchange Online szolgáltatáson is, néhány korlátozással.



ábra 34: Visual Studioban pontosan úgy hivatkozhatunk az Exchange Online EWS felületére, mint egy helyben telepített Exchange 2007 vagy Exchange 2010 EWS felületére

Természetesen a felhő modellből következik néhány specialitás. A felhő modell előnyeinek egy legfontosabb forrása a megosztott használat, hiszen tudjuk, hogy minél nagyobb egy rendszer, annál kisebb az üzemeltetési költség egységenként. A megosztott használat ellenére az Exchange-ben megtaláljuk a Global Address List funkciót, de ez természetesen nem az Exchange Online rendszeren lévő több millió felhasználót tartalmazza, hanem csak azokat, akik az adott előfizető vállalathoz tartoznak. Emiatt érezheti úgy a felhasználó, hogy saját Exchange-en dolgozik — ezt nevezzük multitenant működésnek. Általánosságban elmondható, hogy azok a programozási technikák nem, vagy csak korlátozottan működnek, amelyek a szerverre feltöltendő programkódot feltételeznek, mert a Microsoft Online szolgáltatásnak biztosítania kell a felhasználók védelmét egymás futtatható kódjától. Nincs azonban akadálya annak, hogy a Microsoft Online-ra ráfejlesszünk a nyilvános felületeken keresztül.

A Felhő néhány további ponton is más megközelítést követel, mint a hagyományos informatika. Példaként vegyük az Excel távolról futtatható változatát, az Excel Web Applicationt, amelyet a Microsoft az Office 365 szolgáltatás keretében is elérhetővé tesz 2011 tavaszán, igazi Felhő szolgáltatásként. Itt az helyi gépen beállított alapértelmezett mappát visszadó INFO() makrófüggvényt értelemszerűen nem használhatjuk, hibát ad vissza. Másik példa az időt visszadó MOST() — angol Excelben NOW() — függvény, amely nem a helyi PC, hanem a szerver idejét fogja visszaadni. Mindezen természetes

különbségek ellenére azt mondhatjuk, hogy az Excel Web Application a makrók futtatása tekintetében is közel ugyanazzal a tudással rendelkezik, mint a jól megszokott helyi Excelünk.

Adminisztártorok számára fontos, hogy az Exchange Online Powershell parancsokkal menedzselhető, tehát itt sem kell egy új eszközt kezünkhöz idomítani. Ezeket a parancsokat a Microsoft Online Services Directory Synchronization eszközzel lehet telepíteni. A legfontosabb parancsokról itt olvashatunk:

Bulk User Account Activation and Password Reset http://technet.microsoft.com/en-us/library/ee662252.aspx

Migration Cmdlet Reference http://technet.microsoft.com/en-us/library/cc742577.aspx

Ha valamilyen feladatot korábban programkód írásával oldottunk meg, amelyet Exchange-hez fejlesztettünk, és az nem a régebbi API-k valamelyikét (pl. régebbi Exchange verziók DAV vagy szerver oldali CDO felületét) használja, akkor jó eséllyel könnyen tudjuk portolni a Felhőbe. A kliensre épülő megoldások természetesen szintén működnek, ilyenre példa lehet az Outlook Add-In, vagy az Outlook MAPI módszer használata. Működik továbbá az OWA Web Part technika is, ahogyan azt megszoktuk a helyi Exchange-nél, hiszen ezek is tulajdonképpen kliensre épülő programozási módok, még ha az OWA kiens a böngészőben fut is.

A Sharepoint Online esetében egyelőre szűkebb az arzenál, de a Web Services felület jelentős része ott is meghívható, sőt a beágyazott Data Form Web Part akár külső adatforrásokat is képes megjeleníteni. Programozói szempontból az Office 365 hoz majd nagy előrelépést, amely bizonyos esetekben programkód feltöltését is lehetővé fogja tenni.

Amennyiben a feladat megköveteli az Exchange Online-t vagy a Sharepoint Online-t kiegészítő programlogika írását, akkor erre a legjobb módszer, hogy azt nem az Exchange Online-on, illetve a Sharepoint Online-on belül helyezzük el, hanem egy Windows Azure alkalmazásban, hiszen onnan is hívhatjuk az Exchange Online-t, illetve Sharepoint Online-t. Erre egy konkrét példát tartalmaz az Exchange Online Developer Guide.

A programozók számára több technikai dokumentumot is készített a Microsoft, amelyeknek a címe is igen beszédes:

Az Exchange Online Developer Guide itt érhető el:
http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=0ffa787d-79cd-43fd-b528-b47d45c7ea0d

A Microsoft SharePoint Online Standard Developer Guide pedig itt:
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d007f35e-375c-4b11-bc40-bc9082bb224a&displaylang=en

Exchange 2010 Service Pack #1

Petrényi József

SRI Kft, senior technikai tanácsadó

Exchange Server MVP

Erősen tartja magát az a vélemény, miszerint az Exchange kifejezetten az a termék, melyet csak az SP1 után szabad komolyan venni. Szívem szerint küzdenék ellene, de a tapasztalat azt mutatja, hogy a legendának van egy halvány alapja, legalábbis az Exchange 2007 bevezetése megtépázta némileg ennek a patinás szoftvertermékneknek a jóhírét.

A 2010-es verziónál azért ennyire nem rossz a helyzet. A szoftver kibocsátási hibáit a Rollup Pack-ek folyamatosan javítgatták (4 jelent meg a szervizcsomag előtt), a funkcionalitási hiányosságok pedig messze nem voltak annyira ordítóak, mint a 2007-es RTM verzió esetén. Hogy akkor milyenek voltak? Pont erről fog szólni a cikk: milyen funkcionalitásbeli pluszt hozott nekünk az SP1?

A telepítéssel kapcsolatos újdonságok

Mint közismert (hogy mondta, Safranek?), az Exchange alkalmazás telepítése előtt a számítógépet preparálni kell. Magyarul a Windows Server operációs rendszer változatától és a telepítendő Exchange szerepköröktől függően több-kevesebb képességet fel kellett ugrasztanunk a számítógépre. Nem volt ez olyan nagy ördöngősség, a Technet Library megfelelő fejezetéből kitúrtuk az adott helyzetben szükséges képességeket, ezeket beleírtuk az implementációs tervbe, aztán már jöhetett is a servermanagercmd vagy a Powershell, utána pedig reménykedhettünk a prerequisit check hosszú percei alatt, hogy jó fejezetet találtunk meg, és nem felejtettünk ki semmit. Nem meglepetés, hogy a folyamat ilyetén menetével a rendszergazdák nem volt igazán elégedettek, hiszen magánál az Exchange telepítőprogramjánál jobban senki nem tudhatta, milyen képességre is lesz még szüksége az alkalmazásnak - akkor miért is nem ő teszi fel ezeket a hiányzókat?

Nos, az SP1-be ez a funkcionalitás már belekerült. Nem kell vacakolni a szükséges képességek telepítésével, elég csak bekattintani egy checkbox-ot és hajrá. (Felügyelet nélküli telepítésnél meg kell adni a */InstallWindowsComponents* paramétert.) Rossz hír, hogy a telnet klienst ez sem teszi fel, márpedig anélkül egy Hub/Edge szerver olyan, mint Shrek szamár nélkül.

(Amennyiben olyan képesség is szerepel a listán, amelyhez újraindítás szükséges, semmi gond, a restart után újra el kell indítani a telepítőt és az onnan fogja folytatni, ahol kihúzták alóla a delejt.)

A Client Access Server szerepkör újdonságai

ActiveSync

Az Activesync funkció menedzselési lehetőségei szépen bővültek.

Az Exchange Control Panel-ből a következő funkciók érhetőek el:

- Beállíthatjuk az alapértelmezett hozzáférési szinteket mindenféle mobileszköz számára.
- E-mail figyelmeztetést állíthatunk be arra az esetre, ha a mobil eszköz karanténba kerülne.
- Lekérhetjük a karanténba zárt mobileszközök listáját.

- Eszközszintű szabályokat hozhatunk létre.
- Konkrét felhasználók konkrét mobil eszközeit engedélyezhetjük, illetve tilthatjuk.

Ezeken kívül a felhasználók tulajdonságlapján is bővült az eszköztár:

- Kilistázhatjuk egy konkrét felhasználó mobil eszközeit.
- Távoli önmegsemmisítést kezdeményezhetünk konkrét mobil készülékekre. (Nem robban, csak törlődik a tartalma.)
- Törölhetjük a használaton kívüli mobil eszközök partneri kapcsolatait.
- Szabályokat hozhatunk létre, melyek egy konkrét mobil eszközt használó összes felhasználóra vonatkoznak.
- Végül innen is engedélyezhetjük, illetve tilthatjuk konkrét felhasználók konkrét mobil eszközeit.

Eddig lehetőségünk volt engedélyezni a CAS szerveren az IRM integrációt. Jó is volt ez, abban az esetben, ha a mobil eszközökön is Windows operációs rendszer futott. A mobil világ többi része meg csak pislogott. Az SP1 lehetővé teszi - ActiveSync mailbox policy segítségével - hogy maga a CAS szerver hámozza ki az IRM-védett levél tartalmát és adja oda majdnem tisztán a mobil kliensnek. Ezzel már el tudnak bánni a nem Windows termékek is. (A majdnem tisztán azt jelenti, hogy azért egy jelzés kimegy arról, hogy ez eredetileg egy védett szöveg.)

Outlook Web App

Hah, a legfontosabb: skinek húzhatók a webes felületre. Jelenleg 27 elemű a készlet.

Az Office Communication Server és az Outlook Web App együttműködésére szolgáló információk mostantól az Active Directoryban tárolódnak a web.config file helyett, ezáltal jóval könnyebben kezelhetőek.

Annyira lehet, hogy nem közismert, de az owa virtuális könyvtáron a csatolásokra vonatkozóan nem csak block/allow kategóriák vonatkoznak, hanem létezik egy force save kategória is. Az ide tartozó csatolásokat meg lehet ugyan nyitni, de csak úgy, hogy megnyitás előtt a csatolás lementődik a kliens gépre. SP1 előtt ezek a fájlok kihagyták az XML/HTML forgalomra vonatkozó biztonsági ellenőrzést. Az SP1 után a *ForceSaveAttachmentFilteringEnabled* kapcsoló magasra állításával parancssorból (*set-owamailboxpolicy*, vagy *set-owavirtualdirectory*) beállítható hogy az ellenőrzés ezekre a kiterjesztésekre is vonatkozzon.

Egy újabb ütős újdonság: az SP1 után már az OWA-ból is tudjuk módosítani a tartományi jelszavunkat. (Ehhez a registry-t kell megpiszkálni a CAS szerveren.)

Vegyes

Federation Trust esetén már használhatjuk az Exchange szerver saját maga által aláírt tanúsítványát is, nem szükséges lecserélni egy CA szerver által kibocsátottra.

Megjelent a Reset Client Access Virtual Directory varázsló. A magam részéről láttam már olyat, hogy félrement egy telepítés és már rögtön az elején szanaszét állítódtak a CAS szerver virtuális könyvtárain a jogosultságok. És akkor még nem is beszéltünk azokról, akik bátortalan jogosultságmódosításokkal elindultak a Sötét Oldal felé, aztán váratlanul egy vulkán lávafolyamában találták magukat. Az

alapértelmezett könyvtárjogosultságokat végülis össze lehetett vadászni a netről és vissza is lehetett mindent állítgatni... de ez meglehetősen Hamupipőke jellegű munka volt. Ennek vége, itt van a Jótündér... akarom mondani, a varázsló. (Resetelés előtt azért elmenti egy logfájlba az aktuális jogosultságokat.)

Történtek változások Client Throttling Policies téren is. Ezek olyan házirendek, melyek a klienshozzáférések okozta terhelést próbálják elviselhető értéken tartani. Az SP1 előtt csak azok a házirendek voltak alapértelmezésben bekapcsolva, melyek a hozzáférések számát korlátozták. Az SP1 után már mindegyik működik helyből. Újítás az a viselkedés is, hogy mi történjen, ha egy válaszidő jellegű mennyiségre kihegyezett házirendben lépjük túl a beállított küszöbértéket? Az SP1 előtt ilyenkor négylábas megadás következett, azaz a CAS szerver bontotta a kapcsolatot. Az SP1 után valamivel már finomabb a reakció, a kapcsolat kivár, de nem bontódik fel. Emellett bejött két új cmdlet, melyekkel ezeket a terhelésszabályozó házirendeket tudjuk kezelgetni. (*get/set-ThrottlingPolicyAssociation*)

A levéltovábbítás (Hub/Edge szerepkörök) újdonságai

Nem tudom, mennyire ismert a MailTips funkció. Nagyon röviden arról van szó, hogy már a levél írásakor, de legkésőbb az elküldés előtt a szerver megvizsgálja, hogy számíthatunk-e levéltovábbítási hibára? (Túl nagy levél, nem létező címzett, meg ilyenek.) Az SP1 ezt a funkciót azzal bővítette, hogy immár az előzetes vizsgálat működhet federációs kapcsolaton, illetve Exchange Online-on keresztül is. Emellett némileg bőbeszédűbb lett a funkció, azaz jobban követhetjük az eventlogban, mit is csinál. Jöttek új alert, illetve performance counter változók is.

A Message Tracking is főleg monitorozási funkciók terén javult, értsd eventlog, alert és perfcount bővülések. Illetve bejött egy felhasználói élményt növelő újítás is: ha a levél feladója delivery report-ot kért az elküldött leveléről, de az még nem állt össze, mert a Message Tracking még nem végzett, akkor a felhasználó az SP1 után egy udvarias és részletes magyarázó levelet kap arról, miért nem lehetett teljesíteni a kérését.

Az SP1-es Transport szerverek mondhatni rajta tartják a kezüket a levelezés ütőerén. Az egyik trükkjük, hogy folyamatosan minősítgetik a feladott leveleket: lesznek alacsony és lesznek magas költségű levelek. Az utóbbin értünk olyanokat, amelyeknek túl sok a címzettje, túl nagy a belerakott csatolt fájl, és hasonlók. Ezeket a leveleket a Transport szerverek hátrébb sorolják és csak akkor küldik el, ha éppen ráérnek. Hasonló trükk az is, hogy a Transport szerverek figyelik a Mailbox szerverek RPC terheltségét, és amennyiben az túl nagy, akkor visszavesznek a lendületből.

Bekerült a rendszerbe egy érdekes viselkedési mód, melyet Shadow Redundancy Promotion névvel illettek. Hogy ezt megértsük, kicsit mélyre kell fúrnunk. (Aztán legfeljebb a chilei bányászoknál visszafordulunk.)

Maga a Shadow Redundancy a magas rendelkezésreállású rendszerek egyik építőeleme. Addig oké, hogy az adatbázisokból annyi másolatot üzemeltetünk, hogy minden elképzelhető katasztrófa esetén maradjon valahol egy belőlük... de mi történik azokkal a levelekkel, amelyek már bekerültek ugyan az Exchange organizációnkba, de még nem érkeztek meg az adatbázisba - és ekkor éppen lehal a Transport szerver? Ehhez a Microsoft némileg kibővítette az SMTP protokoll utasításkészletét, bevezetve ezzel a Shadow Redundancy fogalmát. Nagyon röviden arról van szó, hogy a Transport szerver továbbítja a

levelet, de emellett berakja egy Shadow Queue-ba is, ahol addig őrzi, amíg meg nem győződik arról, hogy a következő Transport szerver át nem vette. (Ehhez a plusz kommunikációhoz kellenek a plusz parancsok.)

A gondok akkor kezdődnek, amikor az Exchange 2010 Transport szerver olyan SMTP szervertől vesz át levelet, mely nem ismeri a Shadow Redundancy technikát. (Azaz gyakorlatilag a külvilágból, illetve a korábbi Exchange szerverektől.) A Transport szerver, illetve ekkor inkább Edge szerver, ilyenkor nem igazolja vissza egyből a levél megkapását, hanem vár arra, hogy a levél ténylegesen is eljusson a címzett Mailbox szerveréig. De mi van akkor, ha mondjuk egy hálózati hiba miatt a belső levelezési lánc ideiglenesen megszakad? A külső levelező szerver egyre türelmetlenebbül vár, a levél végülis megérkezett hozzánk... valamit csinálni kell. Az Exchange 2010 RTM ilyenkor a timeout előtt pár pillanattal nagy bátran visszaküldött egy igazolást, hogy minden rendben, aztán reménykedett, hogy tényleg rendben is lesz. Az SP1 viszont bevezette a Shadow Redundancy Promotion viselkedést: az Edge szerver keres odabent akárhol egy működő Transport szervert és elküldi neki a levelet. Ez már SR kompatibilis módban megy, tehát a levél átkerül a következő szerverre, belekerül az Edge szerver Shadow Queue-jába... azaz egészen biztosan elszállításra kerül valamikor, valahogyan. Nyugodtan lehet értesíteni a feladót, hogy a levelét megkaptuk, és az garantáltan el fog jutni a felhasználó postafiókjába.

Tudjuk, hogy a Transport szerverek beépítetten tudják a terheléselosztást, amennyiben több is található belőlük egy organizáción belül. Az SP1 ezen az algoritmuson is módosított egy kicsit: korábban ugyanis, ha kiesett egy Transport szerver, a terhelés nem egyenletesen oszlott meg a maradék szervereken. Innentől viszont igen.

Le lettek cserélve a receive konnektorok. Az új verzió már támogatja SMTP esetén az Extended Protection for Authentication-t, mely gyakorlatilag TLS csatornába bújtatott Integrated Windows autentikációt jelent.

A nagy változtatásokból a send konnektorok sem maradtak ki. Az SP1-ben definiálhatunk úgynevezett betonbiztos levelezési útvonalakat, melyek akkor is működnek, amikor nem. Hülyén hangzik, pedig nem az. Tipikusan ilyen útvonal a felhőbe, azaz az Exchange Online felé mutató konnektor. Elképzelhető, hogy pillanatnyilag nem érhető el - mert pont akkor vált elérhetetlenné egy kapcsolat - de a következő másodpercben már a helyére is állt egy másik. Felesleges lenne, ha ilyenkor a levelek NDR-rel pattannának vissza. (Az Exchange Online kapcsolat egyébként is furán működik egy kicsit, normál üzemmódban is kaphatunk olyan hibaüzeneteket, melyek más kapcsolatnál bontást eredményeznek. Itt nem.)

Érdemes megemlíteni, hogy az SP1 nem csak hozott, hanem vitt is. Amennyiben Edge szervert használunk, melyen beüzemeltük a gyári spamszűrést, akkor az SP1 telepítése után kellemetlen meglepetésben lesz részünk: az SCL meghatározásához szükséges spamminta adatbázis a továbbiakban nem fog frissülni. A Microsoft hivatalos álláspontja szerint a spamminta adatbázis frissítését összekötötték a vírusminta adatbázis frissítésével, erre a kunsztra viszont csak a Forefront Protection for Exchange Server 2010 lesz képes.

Jogosultságbeli változások

Az RBAC-ba (Role-based Access Control) bekerült egy új hatókör, a database szkóp.

Egy újabb szemléletbeli váltás történt a jogosultsági rendszerben. SP1 előtt az Exchange adminisztrátorok képesek voltak felhasználókat létrehozni, törölni a címtárban, illetve hozzáfértek nem egészen Exchange jellegű tulajdonságokhoz is. Ennek most vége.

Mostantól az RBAC-hoz tartozó elemek (management role groups, managment role assignment policies) elérhetők Exchange Control Panel-en keresztül is, grafikusan. (Hiphiphurrá.)

Adattárolást érintő változások

Az Exchange 2010 RTM lekorlátozta a felhasználónkénti hozzáférések számát az adatbázisokhoz. Az SP1 ezen belül megnövelte az adminisztrátori hozzáférések limitjét 64000 session/server értékre.

Az egyik kedvencem. A 2010 SP1 előtti bármelyik Exchange verzió esetében ha megsérült egy, vagy több postafiók, akkor le kellett csatolni az adatbázist, majd offline állapotban ráküldeni az *Isinteg* parancsot. Az SP1-ben bejött egy új cmdlet (*new-mailboxrepairrequest*), mely képes megvizsgálni egy-egy postafiókot és kijavítani az esetleges sérüléseket. Mindezt online módban.

Ez se rossz. Kapunk egy szkriptet (*troubleshoot-databasespace.ps1*), mely negyedóránként lefut és figyeli, mennyi az üres hely az adatbázisok és logok alatti merevlemezeken. Ha ez az érték 25% alá esik, akkor megvizsgálja, hogy nem a logfájlok hirtelen megugrott szaporodása vitte-e el a helyet? Ha igen, akkor a szkript megvizsgálja az adatbázis 25 legjobban pörgő postafiókját és a legnagyobb forgalmúakat karanténba vágja. (Hat órán keresztül a postafiókok elérhetetlenné válnak.) Amennyiben ezzel sem tudja lecsökkenteni a növekedést, akkor egyrészt riaszt, másrészt kiveszi az illető adatbázist az ún. Provisioning adatbázisok közül. (Az Exchange 2010 esetében nem kell konkrétan megmondanunk, melyik adatbázisba szeretnénk, hogy kerüljön egy új postafiók. Elég csak megadnunk egy listát - provisioning list - és az ebben szereplő adatbázisokból választ a szerver egyet, load balance alapján.) Amennyiben a szkript tíznél több postafiók esetében talál túl intenzív használatot, rendszerhibát jelez.

Kapunk egy hasonló szkriptet arra az esetre, ha egy adatbázis válaszideje durván megnőne. (*troubleshoot-databaselatency.ps1*)

Radír. Az SP1 hozott egy új cmdletet: *remove-storemailbox*. Ez gyakorlatilag kipurgálja a megnevezett postafiókokat. Aktív postafiókra nem működik, csak valamilyen módon törölt postafiókokra. Konkrétabban:

- Soft-deleted postafiókok: Amikor egy postafiókot átmozgatunk egy másik adatbázisba, nem törlődik egyből a régiből, hanem ún. soft-deleted állapotba kerül. (Arra az esetre, ha vissza akarnánk csinálni az átmozgatást.)
- Removed, vagy disabled pstafiókok: Amikor egy postafiókot vagy kitöröltünk, vagy lecsatoltunk egy felhasználóról.

Alaphelyzetben mindkét kategória esetén a törlés csak a retention time lejárta után történik meg. A *remove-storemailbox* parancs ezt gyorsítja fel.

A public folderek is kaptak néhány új szkriptet. Ezek elsősorban a replikációkra vonatkozó statisztikákra, illetve hibajavításokra vonatkoznak. Ezenkívül bekerült a grafikus konzolba a kliens szintű jogosultságok állítgatása a foldereken.

Végül egy figyelmeztetés. Az SP1-ben megváltozott az adatbázis séma, azaz RTM szerverről lecsatolt adatbázist - 'database portability' ide, vagy oda - nem tudunk felcsatolni SP1-es szerveren. Na meg fordítva sem.

Postafiókokat érintő változások

Elismerem, nem ez a legnagyobb horderejű változás, de azért említsük meg: létre tudunk hozni csoportnév-konvenció házirendet, azaz innentől csak a névkonvenciónknak megfelelő nevű levelezési csoportokat leszünk képesek kreálni.

Megjelent egy csomó új cmdlet, melyek segítségével aszinkron módon tudunk közvetlenül pst-be exportálni, illetve pst-ből importálni.

A lágytörlésről (khmm) már esett szó, említsük meg egy másik aspektusból is. Ha egy postafiók mozgatása behal, akkor az SP1 után nem kell aggódni, az eredeti helyéről nem törlődött a tartalom, visszaállítható.

Az egyik legnagyobb durranás: az SP1-ben már elválasztható egymástól a felhasználó éles postafiókja és a személyes archív postafiókja. Eddig ezt a hiányosságot okoltam leginkább azért, hogy annyira még nem terjedt el a Personal Archive. Innentől a személyes archívum külön adatbázisban és külön szerveren is tárolható, a kezelése teljesen különválik a felhasználó tényleges postafiókjától. (Ha nem lelkendeznél még kellően, gondolj bele az ESE adattárolási mechanizmusába.)

A következő újdonság bejelentésekor játszódik némi mosoly a szám szélén. Azon ember mosolya, aki már egész varjúsereget is látott már karókra tűzve. Arról van szó, hogy az SP1-es verzióban már létre tudunk hozni hierarchikus címlistákat is. Ha visszaemlékszünk, ezzel a képességgel a 12 évvel ezelőtt regnáló Exchange 5.5 is rendelkezett. Igaz, akkor még saját Directory Service szolgáltatása volt. Aztán kihúzták alóla és elnevezték Active Directory-nak. A címlisták pedig eleinte (v2000/2003) ldap lekérdezések, később pedig (v2007/2010) opath filterek alapján álltak össze, kemény, egy dimenziós lista formájába. Ez változott meg, mostantól simán le tudjuk képezni a címlistákba a cégünk belső hierarchiáját, ami mindenképpen egy kellemesebb felhasználói élmény.

A magas rendelkezésreállást érintő változások

Continuous Replication - blokk módban. Emésszük egy kicsit. Eddig ugye úgy ment a logreplikáció, hogy amint "elkészült" egy logfájl, fájlszinten át lett másolva a másik/többi node-ra. Habár a logfájlok mérete pont az adatvesztés minimalizálása miatt 2007-ben 5 MB-ról 1 MB-ra csökkent, de azért egy elveszett 1 MB-os logfájl is rendes galibákat tudott okozni. A blokk mód megértéséhez megint fúrjunk egy kicsit. Általánosságban bármilyen változás történik, maga a változás nem közvetlenül a logfájlba íródik, hanem egy ún. logbufferbe. Amikor ez megtelik, akkor megy ki az infó magába az 1 MB-os logfájlba. Blokk mód esetén *már az elemi változás* íródik bele párhuzamosan minden node logbufferébe. Azaz ekkor már nem kell várni arra, hogy maguk a logfájlok replikálódjanak.

Enhanced Datacenter Activation Coordination (DAC) támogatás. Itt már átlépünk a Site Resiliency, azaz telephely szintű forró redundancia világába. Maga a DAC egy Site Resilience üzemmód, melyben cmdletek segítségével valósítjuk meg az átállást. A 2010 RTM verzióban a DAC mode csak akkor volt használható, ha legalább 3 node-ból álló DAG rendszerünk volt. Az SP1 ebben is lazított, immár 2 node-

os DAG esetében is működik a DAC mode. (Mielőtt legyintenénk, gondoljunk bele, mi is van akkor, ha az a telephely dől le, ahol az egyik node mellett a witness is van?)

Ezen a területen is kaptunk egy szakajtó segédszkriptet:

- *CheckDatabaseRedundancy.ps1*: Mint a neve is mutatja, leellenőrzi, hogy adatbázis-redundancia téren minden rendben van-e?
- *Start/StopDagServerMaintenance.ps1*: Az első parancs előkészíti a DAG node-ot karbantartásra. (Elmozgat róla minden aktív adatbázist és DAG funkcionalitást. illetve blokkolja, hogy a szerver részt vegyen a DAG működésében.) A második meg visszacsinálja mindezt.
- *CollectOverMetrics.ps1*: Ez a szkript már létezett korábban is, de most ki lett bővítve. Ha lefuttatjuk, összegyűjti az összes rendelkezésére álló adatot a switchover, illetve failover esetekről. (A bővítés gyakorlatilag azt jelenti, hogy már ismeri a blokk módot.)
- *CollectreplicationMetrics.ps1*: Szintén már létező szkript kibővítése. Az a trükkje, hogy real time képes monitorozni az éppen zajló logreplikációt.

Emellett néhány funkcionalitás feljutott az EMS-ből az EMC-be, illetve jelentősen felgyorsult a switchover/failover folyamat is.

Házirend és megfelelőség az SP1-ben

Erről a területről csak szemezgetnék, mert a rengeteg apró változást inkább nem sorolnám fel.

Retention Policy

Az SP1-ben már a Calendar, illetve a Tasks default folderekre is tudunk retention policy jelölést rakni.

A felhasználók az Exchange Control Panelből be tudják jelölni azokat a leveleket, melyekre nem szeretnék, hogy ráessen a retention policy.

Discovery

Mielőtt az adminisztrátorok ráküldenék a tényleges tömeges keresést a postafiókokra, visszajelzést kapnak, hogy mekkora eredményhalmazt kapnának. Ez anélkül segítheti őket a keresőkifejezés finomításában, hogy meg kellene várniuk a tényleges keresés eredményét.

Az adminisztrátorok megjegyzésekkel láthatják el a talált leveleket.

A keresés kiszűri az eredményhalmazból a duplikátumokat.

Information Rights Management (IRM)

OWA-ból anélkül is megtekinthetjük az IRM védett csatolt fájlokat (WebReady document viewing), hogy azokat a hozzájuk tartozó alkalmazásokkal megnyitnánk. (Természetesen ez nem minden fájltipusra igaz, csak bizonyos támogatottakra.)

Az IRM már cross-organization környezetben is támogatva lett.

Exchange szerepkörönként logolhatjuk az IRM-mel kapcsolatos eseményeket.

Az Unified Messaging szerepkör változásai

Tekintve, hogy ez a szerepkör a legritkábban előforduló szerepkör a vadonban, inkább csak röviden felsorolok néhány változást, a teljesség igénye nélkül.

- Az ECP-ben is megjelenik a felhasználó hívási statisztikája, illetve a hívási logja.
- ECP-ből is lehet menedzselni az UM funkciókat.
- Immár tudunk organizációk között is mozgatni UM-enabled postafiókot.
- Caller Name Display támogatás.
- Test-ExchangeUMCallFlow cmdlet: tesztelhetjük az UM kapcsolatot és magának a hívásnak a menetét.
- Támogatja a Lync Server 2010-et. (Az OCS 2007 utódját.)
- 11 új nyelvi csomag, ebből négy támogatja a felolvasást (Voice Mail Preview) is. Az utóbbiak: kanadai angol (I'm a lumberjack, and I'm okay), lengyel, portugál és spanyol. A magyar a fasorban sincs.

Auditálás

Az auditálás mindig is egy kényes feladat. Ha túl kevés információt gyűjtök, akkor pont az nem lesz benne, amire kíváncsi vagyok. Ha túl sokat, akkor benne lesz ugyan, de nem találom meg. Az SP1 úgy próbálja feloldani az ellentmondást, hogy rágyúr a keresésre. Ez konkrétan azt jelenti, hogy az EMS-ből indíthatunk tetszőleges részletességű keresést, a parancs kimenetele lehet egyszerűen a képernyő, egy xml fájl, vagy email egy tetszőleges címre.

Jó, de mi is az, amiben kereshetünk, azaz mit is auditálunk? Az adminkodást. Azaz minden művelet, mely az Exchange rendszer konfigurációját érinti, rögzítésre kerül. (Konkrétan maga a keresés is, hiszen az is parancs kiadása.)

Az SP1 emellett bevezeti a postafiók auditálást. Minden megmozdulás auditálható, mely érinti a postafiókot, függetlenül attól, hogy egy adminisztrátor, egy delegált személy, vagy maga a tulajdonos követte el. Mit értünk megmozdulás alatt? Gyakorlatilag mindent: kapcsolódás postafiókhoz, levelek mozgatása, törlése vagy egyszerűen csak a megnyitása. Durva, nem? Ha belegondolunk, mennyi adat kerül rögzítésre, rögtön örülni fogunk a keresés feljavításának.

A log eredménye nem az eventlogba kerül, hanem magába a vizsgált postafiókba. Engedélyezése a set-mailbox paranccsal történik - azaz postafiókonként szabályozható.

Zárszó

Nagyjából ennyi. Habár nem minden változást soroltam fel, de a lényegeseket igen. Első ránézésre ijesztően hosszúnak tűnhet a lista, de vizsgáljuk meg alaposan a változásokat: egyik sem olyan, melynek hiánya nagyon megnehezítené a rendszer használatát. Okos dolgok, jobb lett tőlük a termék... de ezek nélkül sem rossz. Azaz Exchange téren a kizökkent világ kezd valóban helyreállni: a szervízcsomag plusz igényeket elégít ki, nem pedig alapfunkciókat.