Szentgyörgyi Tibor – Filkor Csaba – Borbély Balázs

Modern munkakörnyezet építése Windows Server 2012, Windows 8 és Office 365 alapokon

Microsoft

Windows Server 2012

J.O.S.

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

A könyv nyomtatott verziója megvásárolható a könyvesboltokban,
és a kiadó webáruházában: www.joskiado.hu

Szentgyörgyi Tibor – Filkor Csaba – Borbély Balázs

Modern munkakörnyezet építése

Windows Server 2012, Windows 8 és Office 365

alapokon

Jedlik Oktatási Stúdió
Budapest, 2012

Lektorálta: Szentgyörgyi Tibor

Anyanyelvi lektor: Venczel Katalin

Borító: Varga Tamás

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

Nyomta: LAGrade Kft.
Felelős vezető: Szutter Lénárd

ISBN: 978-615-5012-20-4
Raktári szám: JO-0343

Tartalom

1 Bevezető

Ez a könyv azoknak a kis-és középvállalati rendszergazdáknak szól, akik most ismerkednek a Microsoft alapú hálózatok üzemeltetésével, vagy már üzemeltettek Windows Server 2003 vagy 2008 kiszolgálókat. A fejezetekben végignézzük egy komplett infrastruktúra kialakítását, gyakorlati ötletekkel, tanácsokkal látjuk el, és bemutatjuk a legújabb technológiákat, köztük a magas rendelkezésre állás, a virtualizáció és a PowerShell alapú üzemeltetés újdonságait.

Az utolsó fejezetben bemutatjuk az Office365 termékcsaládot, annak szolgáltatásait, és végigvezetjük Önt a bevezetés, migrálás és üzemeltetési feladatokon.

A könyv fejezetei egymásra épülnek, végigvezetnek minket a telepítés, bevezetés lépésein, az üzemeltetési és hibakeresési feladatokon, hogy a végére egy átfogó képet kapjunk egy optimális, könnyen kezelhető és stabil hálózat működéséről. Minden fejezet végén kitérünk a parancssori üzemeltetésre, ez segíteni fogja Önt a napi feladatok automatizálásában, illetve a speciális feladatok végrehajtásában. Ezen kívül gyakorlati feladatsort is összeállítottunk minden fejezet végén, hogy a megszerzett tudást gyakorolhassa a saját teszt-rendszerén, és kiépíthesse a saját komplett hálózatát.

A Windows Server 2012 alapvető gondolkozásbeli változásokat hoz. Megszűnnek a különálló szerverek, adatok, funkciók, és egységes környezetben kell gondolkoznunk, beleérte a saját telephelyünkön és a felhőben lévő szolgáltatásokat. A kiszolgálók elválnak a hardver elemektől, az adatok a háttértáraktól, így tudjuk biztosítani a rendszer folyamatos működését, skálázhatóságát és biztonságát.

1.1 Privát és Nyilvános felhők

Napjaink informatikai infrastruktúrája átalakulóban van a tradicionálisan üzemeltetett hálózatokról a felhő alapú szolgáltatásokra.

A tradicionális üzemetetési rendszerben különálló számítógépek futnak, magas üzemeltetési költséggel és alacsony kihasználtsággal, általában magas rendelkezésre állási rendszerek nélkül, hiszen az ilyen rendszer kiépítése további költségekkel jár. A rendszer igény szerinti méretezhetősége szintén bonyolult, a szolgáltatás bővítése rendszerint további kiszolgálók üzembe helyezésével valósul meg.

Egy kis- és középvállalat nem mindig engedheti meg magának, hogy további anyagi források segítségével garantálja a különböző rendszerek rendelkezésre állását és itt a jól felkészült üzemeltetői szakemberekkel még nem is számoltunk. Azokról a szakemberekről, akik bevezetik, és később pedig üzemeltetik ezeket a rendszereket.

Amikor felhő alapú szolgáltatásokról beszélünk, az emberek nagy része valami megfoghatatlan, értelmezhetetlen dologra gondol, pedig semmi más, mint a meglévő szolgáltatások megfelelő kombinációja egy egységes, komplex rendszer kialakítására. Beszélhetünk nyilvános felhőről, ahol a kiszolgálókat, szolgáltatásokat egy külső cégnél – akár a Microsoftnál – futtatjuk, illetve a felhő-szolgáltató több ügyfélnek szolgáltat infrastruktúra, platform, vagy szolgáltatás-csomagokat, és beszélhetünk privát felhőről, amikor mi magunk hozzuk létre a megfelelő infrastruktúrát a saját alkalmazásaink futtatásához.

A publikus felhő előnye, hogy nem kell bonyolult infrastruktúrát kiépíteni, sőt, bizonyos esetekben semmiféle infrastruktúrára nincs szükségünk. A számunkra szükséges szolgáltatásokat – pl. levelezés, csoportmunka, vállalatirányítás – béreljük a különböző szolgáltatóktól.

A privát felhő abban az esetben lehet előnyös, ha van megfelelő infrastruktúránk – hardver és szoftver – a rendszer kiépítéséhez, vagy a céges belső információkat nem szeretnénk a felhőben tárolni, vagy nincs megfelelő gyors és stabil sávszélességünk a publikus felhő használatához. Az infrastruktúra nagyjából ugyanaz, a különbség csupán annyi, hogy a publikus felhőt különböző cégek, mint előfizetést használják, a privát felhőt pedig a saját szolgáltatásaink futtatására használjuk.

1.1.1 Hibrid felhő

Bizonyos esetekben szükségünk lehet arra, hogy adataink és szolgáltatásaink egy része a belső infrastruktúrán működjön tovább, bizonyos részét pedig migráljuk a felhőbe. Az ilyen hibrid rendszereknél szükségünk lesz a beállítások – címtár, felhasználók, levelezési beállítások – folyamatos szinkronizálására. Az Office 365-ben lévő Exchange jó példája a hibrid rendszernek, hiszen a felhasználók egy része a helyi hálózaton lévő levelezést használja, másik részük a felhőben lévő Exchange Servert. A két rendszer kapcsolatban van egymással, de egységes egészként tekinthetünk rájuk.

Szolgáltatások a felhőben

- Software as a Service (SaaS) – alkalmazás futtatása a felhőben, lehetővé teszi, hogy a felhasználók helytől és eszköztől függetlenül elérjék az adott alkalmazást.
  A rendszergazdáknak nem kell kiépíteni a futtatáshoz szükséges infrastruktúrát. Akkor hasznos, ha általános alkalmazásokat akarunk futtatni, pl. levelezést, csoportmunkát, CRM rendszert. Tipikus példája az Office 365, ahol – szemben a helyi infrastruktúra üzemeltetésével – nincs szükségünk saját kiszolgálóra, nem kell Windows-t, Exchange-et, vírusirtót, tanúsítványt, tűzfalat, stb. telepítenünk, csak egyszerűen létrehozzuk a felhasználóinkat, akik azonnal használhatják az Exchange, SharePoint és a CRM rendszer teljes funkcionalitását. SaaS környezetben minimális üzemeltetési feladatunk, de ezzel szemben kevesebb lehetőségünk is van.
- Platform as a Service (PaaS) Alkalmazásával platformot kapunk a saját rendszerünk üzemeltetéséhez a felhőben. Ez a platform lehet tárterület, adatbázis-hozzáférés, futtatási környezet, stb. PaaS használatával a fejlesztőknek lehetőséget adunk, hogy alkalmazásaikat a felhőben teszteljék és futtassák. Az SQL Azure tipikus példája a PaaS rendszernek, ahol az alap infrastruktúrát, a Windows és SQL Server környezetet béreljük, itt tudunk adatbázisokat futtatni, illetve össze is köthetjük a saját infrastruktúránkon futó alkalmazásainkkal.
- Infrastructure as a Service (IaaS): Ebben az esetben alap infrastruktúrát kapunk, virtuális gépeket, tárterületet és hálózati hozzáférést, így lehetőségünk van egyéni feladatokat megvalósítani, vagy meglévő hálózatunkat beköltöztetni a felhőbe. Nincs szükségünk saját hardverre vagy internet-kapcsolatra az infrastruktúránk futtatásához. Az IaaS rendszerek biztosítják a folyamatos elérhetőséget, a magas rendelkezésre állást, a mentési folyamatokat, mi pedig használat után fizetünk, illetve bármikor, rugalmasan bővíthetjük gépeinket vagy igényelhetünk újabbakat. A Microsoft Azure IaaS alapja a Hyper-V technológia és a System Center család.

1.1.2 A Microsoft felhő

A Microsoft régóta futtat különböző felhő alapú szolgáltatásokat, mint a Windows Live Messenger 500 millió felhasználóval, BPOS és CRM online szolgáltatások 40 millió előfizetővel, vagy akár a Windows Update szolgáltatások, ahonnan havonta több mint 1 petabájt frissítést töltenek le a világ több százmillió számítógépére. Magyarországon is régóta elérhető az iskolák számára a Microsoft Live@Edu szolgáltatás, ahol az Exchange Online szolgáltatást használhatják ingyenesen, de az Office 365 felhasználása is rohamosan terjed a kis-és középvállalati szektorban.

2 Verziók, újdonságok

Az új operációs rendszer számos újdonságot és jelentős különbséget is jelent a Windows Server 2008 R2-höz képest. Frissítés illetve a telepítés előtt ki kell választanunk azt a kiadást, amely alkalmazások igényeit illetve rendelkezésre állási, virtualizációs szándékainkat tökéletesen lefedik. Emellett figyelembe kell vennünk a felhasználói létszámot, amely csatlakozni fog a kiszolgálóhoz.

A Windows Server 2012 következő kiadásokban érhető el:

Verzió	**Ajánlott**	**Funkciók**	**Licenc**
Datacenter	Magas rendelkezésreállású privát és hibrid virtualizációs környezetbe	Teljes funkcionalitású kiszolgáló környezet, korlátlan számú virtuális kiszolgálóval.	Processzor x 2 + CAL
Standard	Kevésbé vagy nem virtualizált környezetbe	Teljes funkcionalitású kiszolgáló környezet, maximum 2 virtuális kiszolgálóval.	Processzor x 2 + CAL
Essentials	Kisvállalkozások számára.	Előre konfigurált hálózati beállítások a felhőbe való integrációhoz, virtualizációs lehetőségek nélkül. Ez lecseréli a Small Business Essential kiadást.	Szerver (25 fő felhasználói limit)
Foundation	Olcsó megoldás, pár fős cégeknek.	Általános funkcionalitású célszerver megoldás, virtualizációs lehetőségek nélkül.	Szerver (15 fő felhasználói limit)

A kiadások árai a következőképpen alakulnak:

Verzió	**Ár**
Datacenter	$4.809
Standard	$882
Essentials	$425
Foundation	csak OEM-ként

2.1 Standard és Datacenter verzió

A licencigény alapján kijelenthető, hogy ha például van 2 db fájlszerverünk 1-1 CPU-val, amelyen Windows Server 2008 R2 Standard fut, akkor ezt a két szervert konszolidálhatjuk 1 db 2 processzoros Windows Server 2012 Standard vagy Datacenter-re. A Microsoft a Windows Server 2012 licenceknél figyelembe vette, hogy legalább 2 magos processzorok vannak a forgalomban.

Az Datacenter és Standard változat a szerepkörökben és szolgáltatásokban tökéletesen megegyezik.

A Windows 2008 R2-höz képest változás, hogy teljesen eltünik a Web, az Enterprise és a HPC verzió. Az Enterprise verzióból a következő funkciók immár a Standard változatnak is részei:

- Windows Server Failover Clustering
- BranchCache Hosted Cache Server
- Active Directory Federated Services
- Additional Active Directory Certificate Services capabilities
- Distributed File Services (támogat 1 DFS root-nál többet is)
- DFS-R Cross-File Replication

Az Datacenter és Standard változata tehát szerepkörökben és szolgáltatásokban tökéletesen megegyezik. További változás a Windows Server 2008 R2-hoz képest, hogy az új Standard verzióban már nincs memória és CPU korlát, azaz a korábbi maximum 32 GB memória és 4 db CPU korlát eltűnik. Tehát a Standard ebből a szempontból is megegyezik a Datacenter kiadással. Az új Windows Server verzió immár nem támogatja az Itanium processzort.

2.2 Virtualizáció

A Datacenter és Standard közötti alapvető különbség a virtualizálható gépek száma. A Datacenter változatban a szerver erőforrása határozza meg a virtualizálható gépek számát, a Standard változatnál összesen 2 db virtuális gépet telepíthetünk. Ha szeretnénk több mint két virtuális gépet telepíteni és nem szeretnénk Datacenter verzióra frissíteni, akkor további licenceket kell vásárolnunk:

Standard Edition licencek	Virtuális gépek száma
1	2
2	4
3	6
4	8

Természetesen a virtuális gépekre nem szükséges további licenceket vásárolnunk, legyen az Standard vagy akár Datacenter.

2.3 RDS és RMS licencek

A Remote Desktop Services és Rights Management Service licencek továbbra is változatlanok, azaz az operációs rendszer licencén kívül további RDS és AD RMS CAL-t kell vásárolnunk.

2.4 Windows Server Essentials 2012

A Windows Server Essential vonal tovább él, a főbb újdonságok a következők:

- Windows Server 2012 operációs rendszer
- Adatvédelem
- Hozzáférés „bárhonnan”
- Egészségi monitorozás
- Rugalmas terhelhetőség
- Bővíthetőség
- Kiegészítők további kisvállalati megoldásokhoz, többek között az Office 365-höz

A Windows Small Business Edition változat megszűnik, ehelyett ajánlják a Windows Server Essentials-t, a felhő alapú szolgáltatásokkal kiegészítve (e-mail, csoportmunka támogatás, online mentési szolgáltatás stb.)

2.5 Frissítési jogok

A Windows Server 2008-ról és Windows Server 2008 R2-ről indíthatjuk a frissítést, az ez előtti verziók nem támogatottak. A frissítést csak ugyanarra a kiadásra tehetjük meg.

Windows Server 2008 (R2) Standard → Windows Server 2012 Standard
Windows Server 2008 (R2) Enterprise → Windows Server 2012 Standard
Windows Server 2008 (R2) Datacenter → Windows Server 2012 Datacenter

2.6 „Downgrade” jogok

Ha esetleg mégis úgy döntünk, hogy visszaállunk Windows Server 2008 R2 operációs rendszerre (pl. alkalmazás kompatibilitási szempontból), ezt is megtehetjük. Egy Windows Server 2012 Standard verzióról lefokozhatjuk a kiszolgálónkat egy Windows Server 2008 R2 Standard-ra vagy egy Enterpise-ra, egy Windows Server 2012 Datacenter-ről bármelyik Windows Server 2008 R2 verzióra.

3 Windows Server 2012 telepítése

Ebben a fejezetben megnézzük a Windows Server 2012 telepítéséhez szükséges hardver feltételeket, a telepítési módokat, és a grafikus verzió telepítését.

Fizikai vagy virtuális gép
Első lépésben el kell döntenünk, hogy új szerverünket fizikai vagy virtuális gépre szeretnénk telepíteni. Ehhez a döntéshez fontos tudnunk, hogy a kiszolgáló milyen feladatokat fog ellátni, mert bizonyos funkciók nem telepíthetők virtuális környezetbe.

Virtuális gépet érdemes telepítenünk, ha:

- A futtatandó szerepkör nem igényli egy teljes értékű számítógép teljesítményét
- Fontos a magas rendelkezésre állás
- Könnyen skálázható rendszert szeretnénk (pl. memória-, processzorbővítés)

Fizikai gépet érdemes telepítenünk, ha:

- A gépnek nagyobb erőforrásra van szüksége
- Közvetlen hozzáféréssel kell rendelkeznie bizonyos hardver erőforrásokhoz
- A rajta futó szolgáltatás nem támogatja a virtualizációt

Ebbe az utolsó részbe tartozott régen az Active Directory is, de a Windows Server 2012-ben már telepíthetünk tartományvezérlőt virtuális gépre is.

Fontos átgondolni a licencelési kérdést is, hiszen a Windows Server 2012 Standard verzió licence egy fizikai és két virtuális gép használatára jogosít, tehát ugyanazon a vason egyszerre három példányban futtathatunk Windows Servert, és telepíthetünk különböző szolgáltatásokat a gépekre.

Hardver feltételek:

A Windows Server 2012 telepítéséhez a következő minimális hardver-feltételeknek kell megfelelnie a szerverünknek:

- 64 bites CPU
- Processzor sebesség: 1.4 gigahertz
- 512 megabyte RAM
- 32 GB lemezterület, ha a szerverben nincs több, mint 16 GB RAM

A Datacenter verzióban támogatott maximális hardver:

- 640 logikai processzor
- 4 TB RAM
- 63 tagból álló feladatátvevő fürt

A telepítés forrása lehet DVD lemez, USB pendrive, hálózati megosztás vagy központi telepítési kiszolgáló (WDS), System Center használata esetén pedig használhatunk SCCM Zero Touch telepítést, vagy System Center Virtual Machine Manager (SCVMM) környezetben Virtuális gép sablonokat is.

Amennyiben DVD-ről telepítjük az operációs rendszert, a gépben kell, hogy legyen DVD olvasó, ez virtuális környezetben további konfigurálást igényel. A telepítő DVD-re nincs lehetőségünk frissítéseket elhelyezni, és egyszerre csak egy gépre telepíthetünk vele.

Az USB alapú telepítés jelentősen gyorsabb, és Windows frissítéseket, drivereket is el tudunk helyezni a telepítési médiumon. A számítógépek jelentős része képes USB-ről bootolni. Az USB eszközön előre elkészített válaszfájlt is elhelyezhetünk, ezzel automatizálhatjuk a telepítést. Elkészítéséhez szükségünk lesz a Windows USB DVD Download Tool-ra mely kicsomagolja az ISO vagy DVD tartalmát az USB eszközre. A program letölthető a Microsoft Store-ból:
http://www.microsoftstore.com/store/msstore/html/pbPage.Help_Win7_usbdvd_dwnTool

Virtuális környezetben legegyszerűbben ISO fájlból tudunk telepíteni, amennyiben a virtualizációs hoszton elérhető a telepítő ISO fájl.

A Windows Deployment Services alapú telepítésnél a számítógép hálózatról indul PXE protokoll segítségével, ilyenkor nincs szükségünk külön DVD lemezre vagy USB eszközre, és akár egyszerre több gépre is telepíthetünk operációs rendszert.

Telepítési opciók

Az operációs rendszer telepítésekor a következő módszerek közül választhatunk

- **Friss telepítés:** Új operációs rendszer telepítése új lemezre. Ez a leggyakrabban használt módszer
- **Frissítés:** a felhasználói dokumentumok, adatok és programok megtartásával, egy meglévő operációs rendszer frissítése. A frissítési alap lehet Windows Server 2003, R2, Windows 2008 vagy R2, de mindenképpen 64 bites verzió. Frissítés nem lehetséges 32 bitről 64 bitre illetve különböző nyelvi verzióra. A frissítés a telepítő lemezen lévő SETUP.EXE futtatásával indítható a meglévő operációs rendszerről.
- **Migráció:** meglévő operációs rendszer áttelepítése Windows Server 2012-re, új számítógépre, a Windows Server Migration Tools segítségével. Ebben az esetben a beállítások és fájlok átkerülnek az új operációs rendszerre.

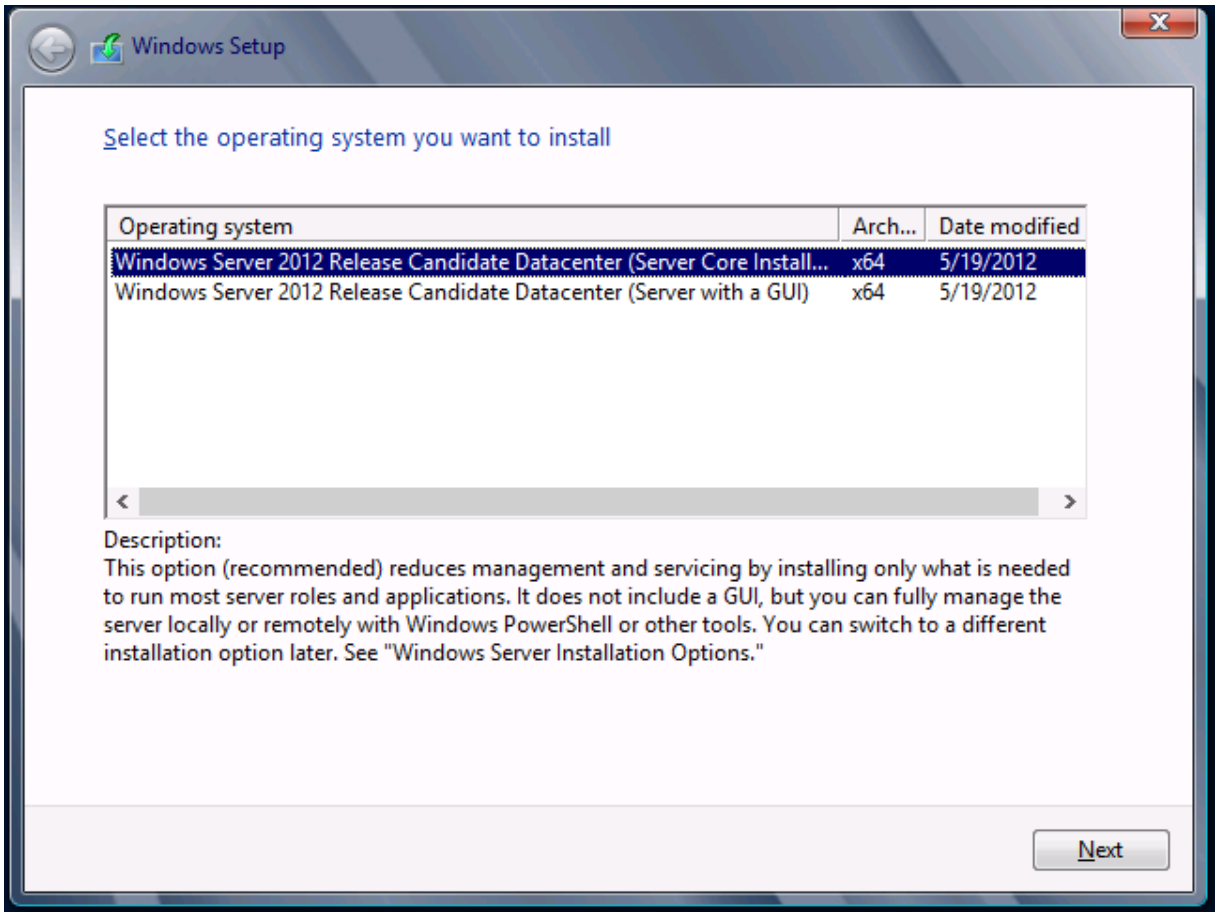
3.1 Telepítés

Windows Server 2008 óta a telepítés két jól elkülöníthető részre osztható: telepítés és testre szabás. Maga a telepítési folyamat kizárólag partícionálást és fájlmásolást végez. A telepítés után a számítógépnév, IP cím, és minden egyéb beállítás megadása a kezdeti konfigurációs varázslóban történik.

A Windows Server telepítő lemezének két legfontosabb állománya a boot.wim és az install.wim. A Windows Server telepítése az ún. boot.wim állomány betöltésével indul. Ez egy Windows PE alapú grafikus rendszer, amely a megfelelő hálózati és lemezkezelő illesztőprogramok betöltése után elindítja a telepítőt. (ez a wim állomány bővíthető további driverekkel, működésével a WDS fejezetben fogunk részletesen foglalkozni.)

A területi és billentyűzet beállítások után meg kell adnunk, milyen változatot szeretnénk telepíteni: grafikus vagy Server Core felületet. Ez az előző Windows Server verziókkal ellentétben telepítés után is bármikor változtatható: a grafikus felület egy ki-, és bekapcsolható szol-

gáltatás, így bármikor válthatunk a két felület között, bár ehhez szükségünk lesz a telepítő lemezre.



A telepítésnél választhatunk a frissítés és az egyéni (új) telepítés közül. A frissítés indításához azonban a telepítőt a frissítendő operációs rendszerből kell futtatni, így ennek a menüpontnak itt nincs nagy jelentősége.

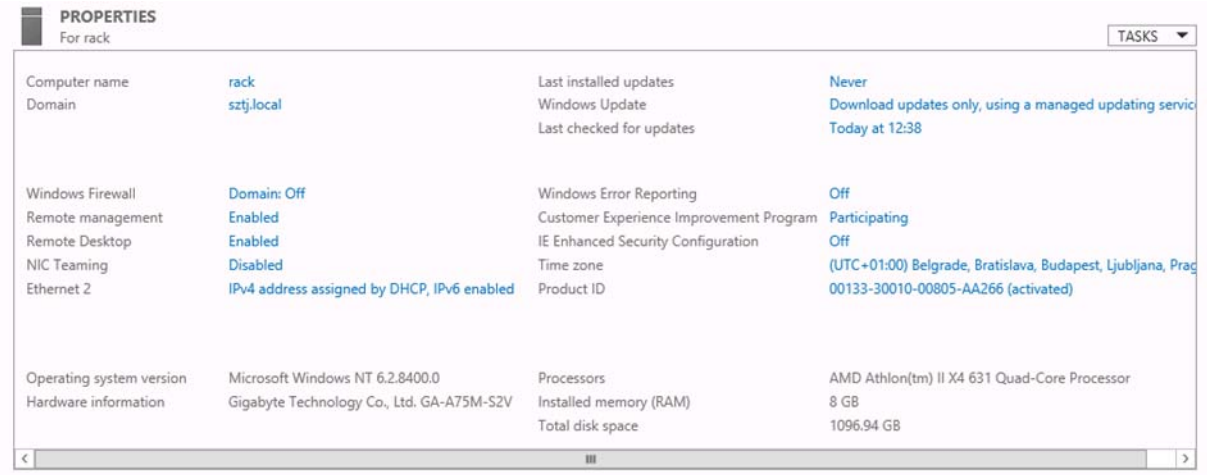
Az új telepítés kiválasztása után meg kell adnunk a lemezt vagy a felcsatolt VHD fájlt, ahová az operációs rendszert szeretnénk telepíteni, utána pedig már semmi dolgunk nincs, a telepítő megformázza a lemezt, kicsomagolja az install.wim állományt, generál egy véletlenszerű nevet és biztonsági azonosítót (SID) a számítógépnek, és beállítja a hálózati kártyát DHCP kliensként.

Fontos, hogy a telepítés közben bármikor előhívhatjuk a parancssort a SHIFT-F10 billentyűkombináció segítségével, akár IP konfiguráció lekérdezéshez, akár lemezkezeléshez a diskpart.exe segítségével.

Telepítés utáni teendők

A telepítés után a kiszolgáló újraindul, majd grafikus verziónál bejelentkezés után elindul az új kiszolgálókezelő.

A helyi kiszolgáló konfigurálását választva elérhetjük kezdeti beállítás képernyőt:



A kezdeti konfigurációs képernyőn a következő beállításokat tudjuk elvégezni: (lehetőleg ebben a sorrendben)

- IP cím(ek) megadása
- Számítógépnév
- Csatlakozás tartományhoz
- Időzóna beállítása
- Automatikus frissítések engedélyezése
- Szerepkörök és szolgáltatások telepítése
- Távoli asztal engedélyezése
- Windows Tűzfal beállítása

Nem elhanyagolható, hogy itt tudjuk kikapcsolni az internet Explorer Fokozott Biztonsági Funkcióit (IE ESC) a rendszergazdák és a felhasználók számára, kizárólag ezen a gépen.

IP cím beállítása

Itt adhatjuk meg a különböző hálózati kártyáink nevét (pl. LAN, DMZ, stb.), az IPv4-es IP címüket, átjárót és DNS kiszolgálót. Ha a gépet szeretnénk AD tartományba léptetni, az elsődleges DNS kiszolgálónak mindenképpen valamelyik tartományvezérlőt érdemes beállítani.

Az IPv4 cím megadása történhet parancssorból is:

```
Netsh interface ipv4 set address “Local Area Connection” static 10.1.1.1
        255.0.0.0
```

NIC Teaming

Újdonságként jelenik meg a Windows Server 2012-ben a NIC Teaming, ami segítségével több hálózati kártyát tudunk összefűzni, ezzel nagyobb sávszélességet és rendelkezésre állást tudunk elérni. A NIC Teaming használatához nem kötelező ugyanattól a gyártótól származó hálózati kártyákat használnunk, de csak azonos sebességű kártyákat használhatunk. Amennyiben az egyik hálózati kártya elromlik, vagy megszűnik a kapcsolata, a többi kártyán tovább folyik az adatátvitel. Ez a funkció különösen hasznos, ha iSCSI rendszerrel dolgozunk, vagy ha több virtuális gépek futtatunk, és szeretnénk nagyobb sávszélességet használni.

Offline Domain Join

Ez a funkció azoknak lehet hasznos, akiknek több telephelyük van, és a telephelyeken nem rendelkeznek folyamatos Internet-kapcsolattal. Ebben az esetben lehetőségünk van előkészíteni egy számítógép-fiókot az Active Directoryban, majd a távoli számítógépet beléptetni a tartományba kapcsolat nélküli módban.

Első lépésben elő kell készítenünk a számítógépfiókot. A tartományvezérlőn, rendszergazdai jogosultságokkal hozzunk létre egy fájlt:

```
djoin.exe /provision /domain sztj.local /machine tavoligep /savefile
        c:\tavoligep.txt
```

Ezután a távoli gépen futtassuk le a kapott fájlt, szintén a djoin.exe segítségével:

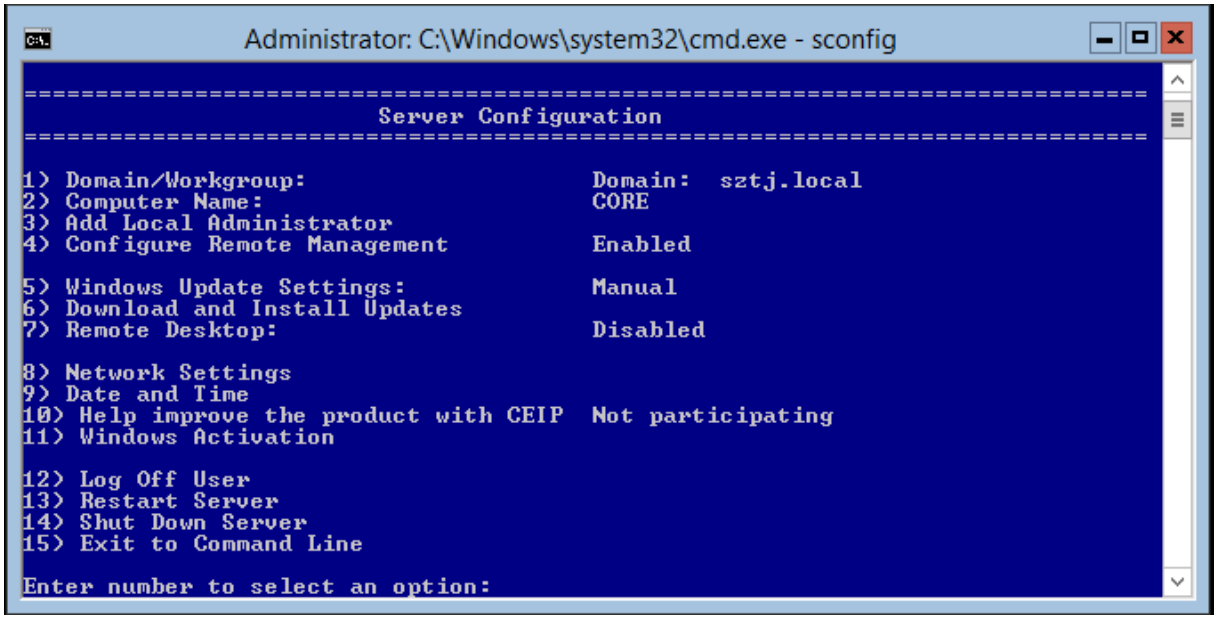
```
djoin.exe /requestODJ /loadfile tavoligep.txt /windowspath %systemroot%
        /localos
```

Remote Management

Itt engedélyezhetjük a kiszolgáló távoli kezelését Kiszolgálókezelőből, WMI vagy PowerShell segítségével. Ha engedélyezzük, a kliens gépünkre telepített Remote Server Administration Toolkit (RSAT) segítségével központi helyről kezelhetjük az összes kiszolgálónkat, vagy akár kiszolgálócsoportokat hozhatunk létre a könnyebb kezeléshez.

Server Core

A grafikus felület nélküli verzióban, a telepítés utáni első lépéseket az sconfig.cmd program segítségével tudjuk elvégezni. A Server Core-ral a 22. fejezetben foglalkozunk részletesebben.



GYAKORLATI FELADATSOR

1) Az Ön által használt virtuális környezetben hozzon létre egy új virtuális gépet DC1 néven.
2) Hardver paraméterek: 1 CPU, 1GB RAM, 60GB HDD, 2 hálózati kártya

3) Indítsa el a Windows Server 2012 telepítőjét
4) Válassza ki a telepítési nyelvet, billentyűzet-kiosztást magyarra, amennyiben lehetséges
5) Telepítse a Windows Server 2012 (Server with a GUI) verziót
6) Válassza az egyéni telepítést
7) Hozzon létre egy 40GB-os kötetet.
8) Állítsa be a jelszót: **Pa$$w0rd**
9) A kiszolgálókezelőből válassza a helyi gép beállítását
10) Nevezze át a számítógépet DC1 névre
11) Állítsa be az időzónát
12) Engedélyezze a NIC Teaming funkciót, adja hozzá mindkét hálózati kártyát.
13) Állítsa be az IP címet:
    a) IP cím: 172.16.0.1
    b) alhálózati maszk: 255.255.0.0.
    c) átjáró: 172.16.0.254
    d) DNS kiszolgáló: 172.16.0.1,172.16.0.254
14) A szerepkörök közül telepítse fel a DNS kiszolgálót

3.2 Windows Server 2012 szerepkörök és szolgáltatások.

A Windows Server 2012-ben, csakúgy, mint a Windows Server 2008-ban, a kiszolgáló a telepítés után – főleg biztonsági okokból - semmilyen funkciót nem lát el. Az operációs rendszer telepítése után a kezdeti konfigurációs varázslóval tudjuk testre szabni a kiszolgálónkat, gépnevet, IP-címet és tartomány tagságot állítani. A kezdeti beállítások után pedig különböző funkciókat telepíthetünk, melyeket alapvetően két részre oszthatunk:

Szerepkörök

- Olyan funkciók gyűjteménye, ami hálózati szolgáltatást nyújt a felhasználók és számítógépek számára. pl. fájlkiszolgáló, tartományi szolgáltatások, stb.
- A szerepkörök rendszerint további rész-szerepköröket tartalmazhatnak.
- A Kiszolgálókezelő feltelepíti a szerepkörhöz szükséges további funkciókat is.
- A 2012-es Kiszolgálókezelővel egyszerre több kiszolgálót is kezelhetünk, szerepkörönként csoportosítva.
- A szolgáltatásokhoz szükséges tűzfal-szabályok automatikusan létrejönnek azok telepítésekor.
- Akár PowerShellből is telepíthetünk az **Add-WindowsFeatures** parancs segítségével. Ez különösen hasznos, ha Server Core verzión dolgozunk.

Szerepkör	**Funkció**
Active Directory Certificate Services (AD CS)	Tanúsítványok létrehozására, kezelésére használható.

AD DS	Tartományszolgáltatás a felhasználók, számítógépek és egyéb hálózati objektumok központi kezelésére, hitelesítésre és azonosításra.
AD FS	Federációs szolgáltatás webes egyszeri bejelentkezésre (SSO) és azonosságkezelésre.
Active Directory Lightweight Directory Services (AD LDS)	Egyszerűsített címtárszolgáltatás, ami nem tartalmaz jelszavakat és bizalmas információkat, de felhasználókat, csoportokat, e-mail címeket igen, így felhasználhatjuk pl. telefonkönyvként vagy egyéb eszközökhöz, ahol felhasználói adatokra van szükség. (hálózati scan, VoIP telefonközpont, stb.)
Active Directory Rights Management Services (AD RMS)	RMS házirendek segítségével védhetjük a hálózaton lévő dokumentumainkat, szabályozhatjuk, kinek milyen hozzáférése legyen. (pl továbbküldés, nyomtatás, szerkesztés)
Application Server	Microsoft .NET Framework 4.5, és .NET Enterprise szolgáltatások központi kezelésére
DHCP Server	Kliens számítógépek IP cím-kiosztására.
DNS Server	Névfeloldás TCP/IP hálózatokon.
Fax Server	Faxok küldésére és fogadására, faxok hálózaton keresztüli kezelésére
File and Storage Services	Megosztott mappák, elosztott fájlrendszer és hálózati tároló funkciók támogatása.
Hyper-V®	Virtuális gépek futtatására.
Network Policy and Access Services	Hitelesítési szolgáltatás távelérési ügyfeleknek, tartalmazza a HRA és NAP szolgáltatásokat.
Print and Document Services	Hálózati nyomtatók, scannerek és dokumentumok központi kezelése.
Remote Access	A DirectAccess funkcióval folyamatos hálózati hozzáférést biztosít az ügyfélgépeknek, melyek így mindig elérhetőek és menedzselhetőek lesznek. Emellett támogatja a VPN technológiákat és betárcsázási rendszereket.
Remote Desktop	Távoli asztal szolgáltatás, RemoteApp alkalmazások futtatása.

Services (RDS)	
Volume Activation Services	Újdonság a Windows Server 2012-ben, a mennyiségi licenc kulcsok központi kezelésére és aktiválására szolgál. Segítségével a VLK kulcsos számítógépeket AD alapokon, automatikusan aktiválhatjuk domain tagság alapján.
Web Server (IIS)	A Windows Server 2012 webkiszolgáló komponense
Windows DS	Windows operációs rendszerek hálózaton keresztüli központi telepítésére.
Windows Server Update Services (WSUS)	Microsoft frissítések központ telepítésére.

Szolgáltatások

A szolgáltatások kiegészítő funkciókat látnak el a Windows Serveren, és általában nem nyújtanak hálózati szolgáltatást a kliensek felé. Ilyen például a feladatfürt-átvevőszolgáltatás, vagy a Windows Biztonsági Mentés. A szerepkörök függőségei között szerepelhetnek bizonyos szolgáltatások, amelyeket a kiszolgálókezelő automatikusan feltelepít.

Néhány szolgáltatást kiemeltünk, a teljesség igénye nélkül:

Szolgáltatás	**Leírás**
Background Intelligent Transfer Service (BITS)	Háttérben futó aszinkron letöltés, akár Windows frissítések letöltésére, akár BranchCache használatára. Ha a felhasználó éppen használja a hálózatot, a BITS szolgáltatás leállítja a háttérbeli letöltést
Windows BitLocker® Drive Encryption	Teljes lemez vagy kötet titkosítása
BitLocker network unlock	Segítségével a BitLockerrel titkosított lemezeket tudjuk visszafejteni a tartományi gépeken, AD-ban tárolt információk segítségével.
Windows BranchCache®	Telephelyeken használható file-cache lehetőség, fájlok, Windows frissítések letöltésére
Failover Clustering	Magas rendelkezésre állású rendszereket építhetünk

Group Policy Management	Vállalati csoportházirend-szerkesztési lehetőség
IP Address Management (IPAM) Server	Új szolgáltatás a Windows Server 2012-ben, az IP címek központi kezelését, adminisztrálását segíti elő
Remote Server Administration Tools	Felügyeleti konzol, segítségével további kiszolgálókon futó szolgáltatásokat tudunk felügyelni
Remote Procedure Call (RPC) over HTTP Proxy	Belső RPC forgalmat csomagol HTTP(S) alagútba.
Simple Mail Transfer Protocol (SMTP) Server	Egyszerű levélküldési protokoll
Telnet Client	Telnet kliens program, alapértelmezésben nincs feltelepítve
User Interfaces and Infrastructure	Grafikus felhasználói felület, a 2012-ben már kikapcsolható képesség, így menet közben tudunk váltani GUI és core operációs rendszer között.
Windows Internal Database	Beépített SQL Express, amit csak a Windows szolgáltatások és a WSUS kiszolgáló használhat.
Windows Server Backup	Biztonsági mentés és visszaállítás program
Windows Server Migration Tools	PowerShell parancsok gyűjteménye, amik segítenek szerepkörök, rendszerfájlok, adatok migrálásában, a Windows Server előző verzióiról.

PowerShell parancsok:

- Get-WindowsFeature: szerepkörök és szolgáltatások lekérdezése
- Install-WindowsFeature: szerepkör hozzáadás
- Remove-WindowsFeature: szerepkör eltávolítása
- Get-WindowsFeature | Where-Object {$_.InstallState -eq “Installed”} telepített szerepkörök lekérdezése
- Uninstall-WindowsFeature User-Interfaces-Infra grafikus felület eltávolítása

4 Kiszolgálókezelő

A Server Manager (Kiszolgálókezelő) szerepet tölthet be a kis- és középvállalatoknál, nagyobb szervezeteknél a Microsoft a System Center családot ajánlja.

A Windows Server 2008 és a Windows 2008 R2-ben megjelent Server Managert a Microsoft teljesen újraírta és számos üzemeltetői tevékenységet segítő újdonsággal egészítette ki.

Az előző Windows Server verzióknál többnyire a lokális szerveren lévő Server Managert használtuk, távoli kiszolgálóknál körülményes volt csatlakoztatás, amely azt jelentette, hogy engedélyezni kellett a távoli kiszolgálónál a Server Managert, majd ezután tudtunk kapcsolódni a szerverhez. Ezen kívül egy időben csak egy gépre tudtunk csatlakozni.

Régi Server Manager felület

A Windows Server 2012-nél jóval könnyebb dolgunk van. A Server Managerrel egyszerre több kiszolgálóhoz csatlakozhatunk, a kiszolgálókat csoportokba szervezhetjük és a távoli Windows Server 2012-es szervereknél már alapértelmezetten be van kapcsolva a távoli kapcsolódás lehetősége. Lehetőségünk van arra is, hogy egy szerveren használva az összes általunk üzemeltetett Windows Server operációs rendszerű gépet menedzseljük, de arra is, hogy a Windows 8 munkaállomásunkon a Remote Server Administation Tools-t telepítve kezeljük a szerverparkunkat, mivel az új RSAT is tartalmazza a Server Managert.

Letölthető itt: http://www.microsoft.com/en-us/download/details.aspx?id=28972

Az új Server Manager-rel a következő operációs rendszerekkel ellátott gépekre csatlakozhatunk:

Operációs rendszer	Funkcionalitás
Windows Server 2012	Teljes
Windows Server 2012 with Minimal Server Graphical Interface	Teljes
Windows Server 2008 R2	Teljes, de szerepköröket és szolgáltatásokat nem telepíthetünk
Windows Server 2008 (x32 és x64)	Teljes, de szerepköröket és szolgáltatásokat nem telepíthetünk
Windows 2003 R2 Server	Erősen korlátozott, csak a szerverek bekapcsolt illetve leállított állapotát láthatjuk.

4.1 Telepítés

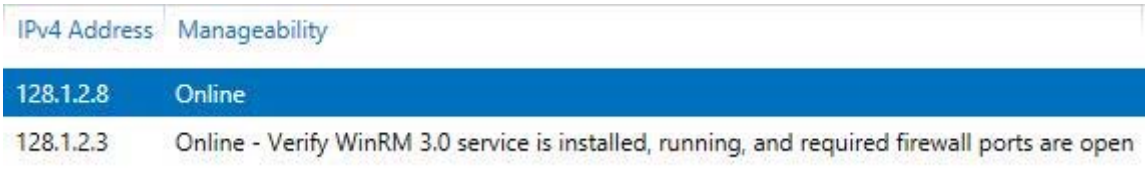
Az új Server Managerrel a következő operációs rendszerű gépekről kezelhetjük a kiszolgálóinkat:

- Windows Server 2012 Standard
- Windows Server 2012 Datacenter
- Windows Server 2012 with Minimal Server Interface (Graphical Management Tools and Infrastructure)
  Az új Windows Server Kiszolgálókezelő automatikusan elindul. Helyi illetve távoli bejelentkezéshez sem szükséges engedélyezés, ha helyi rendszergazdák vagyunk a szerveren. Telepítés és egyéb konfiguráció nem szükséges.
  A következő előfeltételek szükségesek ahhoz, hogy a Server Managerrel a Windows Server 2008-as és Windows Server 2008 R2 alapú kiszolgálókhoz csatlakozni tudjunk:
- Legfrissebb Service Pack-kel ellátott kiszolgálók
- .NET Framework 4.0
  Letölthető: http://www.microsoft.com/en-us/download/details.aspx?id=17851
  Windows Update segítségével tegyük fel a legfrissebb hozzá kapcsolódó frissítéseket is (újraindítás szükséges).
- Windows Management Framework 3.0 (újraindítás szükséges)
  Letölthető: http://www.microsoft.com/en-us/download/details.aspx?id=29939
- A Windows Server 2012 egyelőre nem tudja megjeleníteni a Windows Server 2008 és a 2008R2-ben lévő teljesítmény adatokat. A kiszolgáló mellett a következő jelenik meg: „Online – cannot get performance counter data”, ehhez kiadott a Microsoft egy javítást, ami letölthető itt: http://support.microsoft.com/kb/2682011 (újraindítás szükséges).

Ha a telepítésekkel megvagyunk, lépjünk be és indítsunk rendszergazdai jogosultsággal egy PowerShell-t, majd írjuk be a következőt:

```
winrm quickconfig
```

A parancs beállítja a WinRM-et távoli elérésre és a hozzá szükséges porthoz felvesz egy tűzfalszabályt.



Felkészített és egy felkészítetlen Windows Server 2008-as kiszolgáló

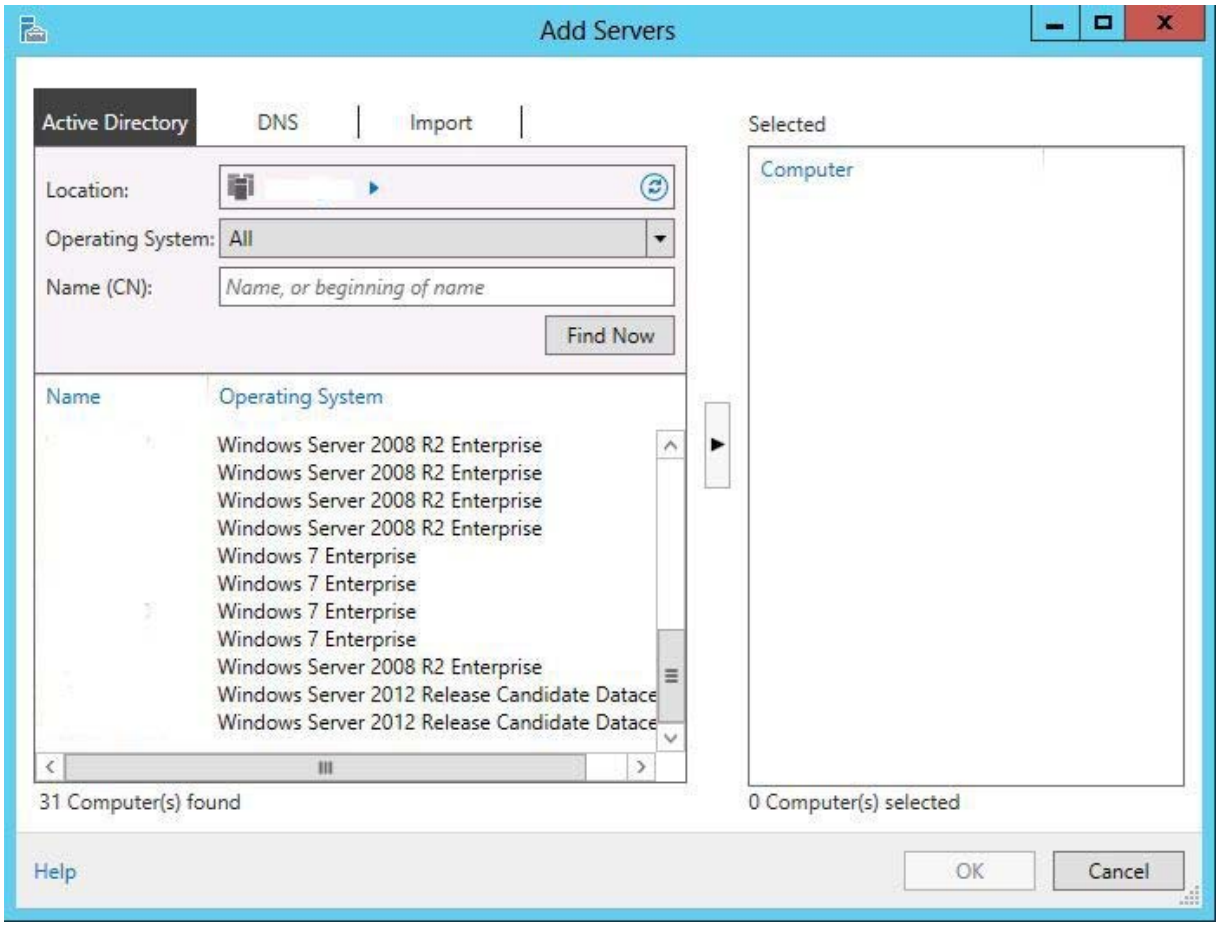
A Windows Server 2003 R2 kiszolgálókra nem szükséges egyéb komponenst telepíteni, viszont itt erősen korlátozott üzemeltetési lehetőségeink vannak.

4.2 Server Manager használata

A Windows Server 2012-be való belépés után automatikusan elindul a Server Manager. Tulajdonképpen ez az eszköz lesz az, amire kiszolgálóink felügyeletében legjobban fogunk támaszkodni. Végre megjelent egy olyan felület, ahol az összes szerverünket tudjuk üzemeltetni, elég egy jobb gombnyomás a kiszolgálón máris elérhetővé válnak a legkülönfélébb üzemeltetési lehetőségek.

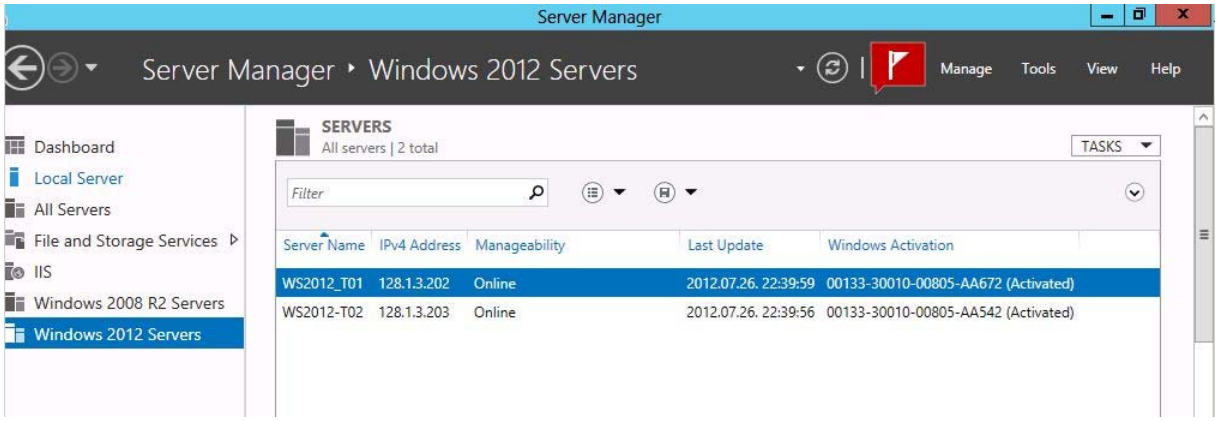
Ezekhez hasonló megoldások már régen elérhetők voltak a nagyvállalatoknak szánt System Center Operations Manager-ben, de most már kisebb cégek is igénybe vehetik ezeket a funkciókat, és ehhez elég egy darab Windows Server 2012.

Legelőször fel kell vennünk a kiszolgálóinkat, majd ezeket csoportosíthatjuk is. Ennek a csoportosításnak csupán annyi jelentősége van, hogy egy adott kiszolgálót vagy kiszolgálókat könnyebben megtaláljuk, ez több ezer szervernél már elég hatásos lehet. De például ha felveszünk egy olyan gépet, amelyen van IIS (Internet Information Services), vagy a kiszolgáló tartományvezérlő, netán DNS vagy DHCP szerepkörökkel rendelkezik, akkor arra automatikusan létrejön egy csoport, benne a kiszolgáló. További lehetőség a „kiszolgáló-érzékeny” menü, egy jobb klikk a gépre, és a szerver szerepkörének megfelelő parancsokat látunk.



Csak annyit kell tennünk, hogy a Location-nél kijelöljük a megfelelő domaint (ha több van), majd a Find Now-ra kattintunk. Itt megtaláljuk az összes szerverünket, azokat pedig, amelyeket szeretnénk felvenni, át kell tennünk a Selected területre.

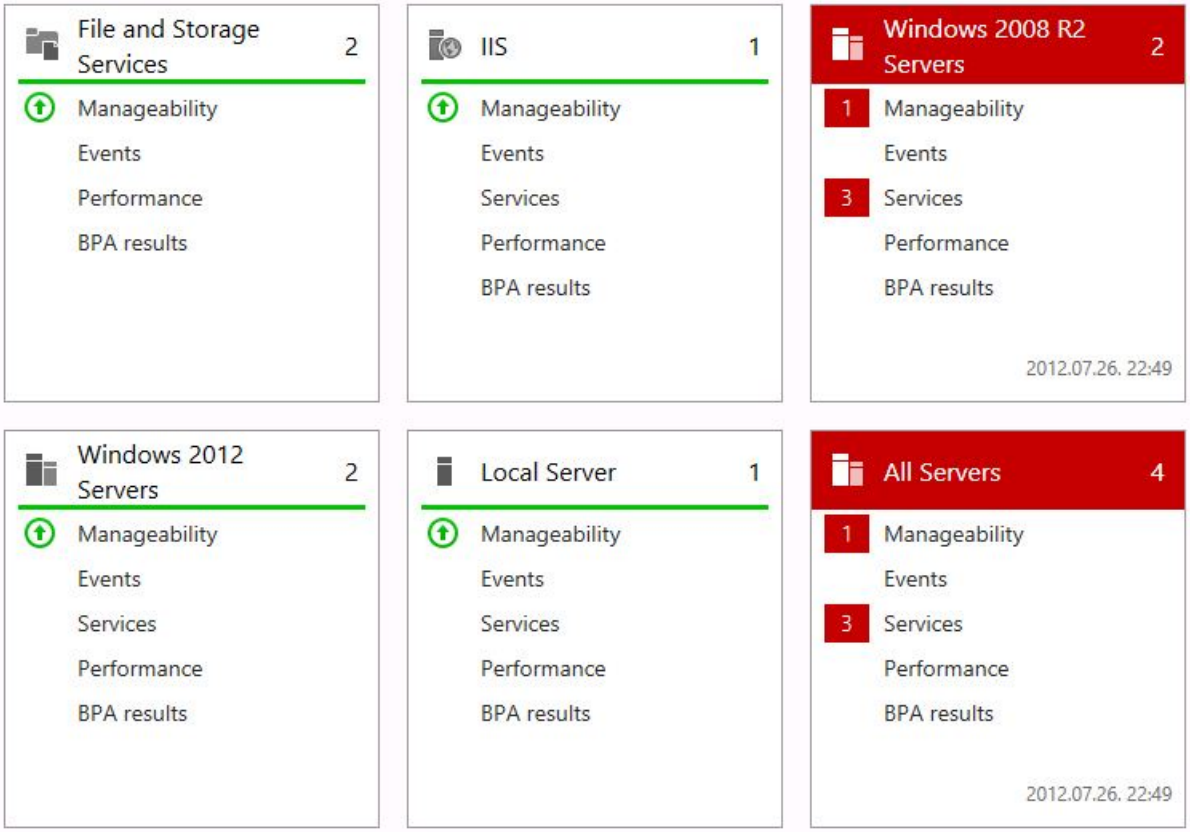
A felvett kiszolgálókat a Manage alatti Create Server Group segítségével csoportokba szervezhetjük, pl. operációs rendszer típusonként, ahogy az a képen is látszik.



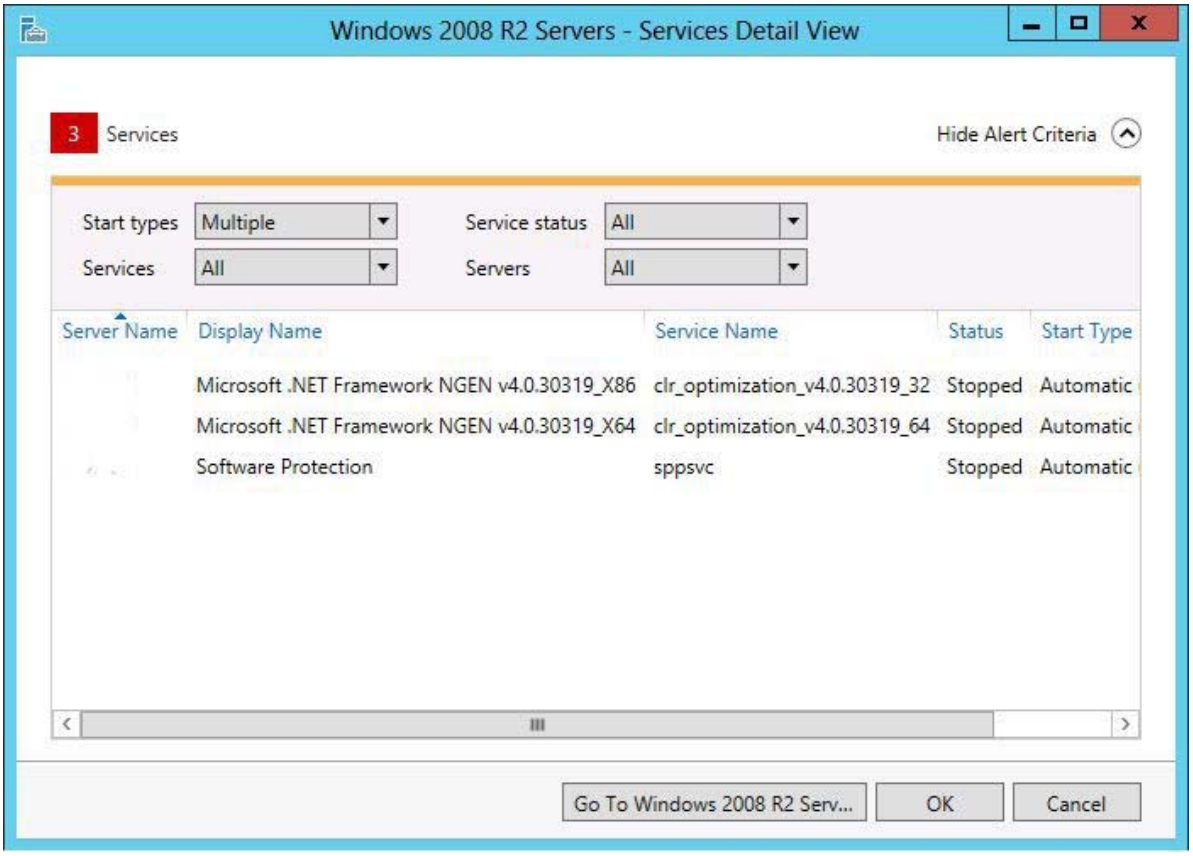
Ha a kijelölünk egy kiszolgálót, akkor számos információt kapunk a Server Managerből. Láthatók az eseménynaplóban lévő üzenetek, a szolgáltatások állapota, a teljesítmény adatok, a kiszolgálón lévő szerepkörök és szolgáltatások.

De ugyanitt felvehetünk illetve el is távolíthatunk szerepköröket és szolgáltatásokat, nem szükséges a bejelentkeznünk a telepítésre szánt kiszolgálóra, hiszen ugyanezt távolról is megtehetjük.

Igen hasznos résznek tekinthető még a Dashboard rész.



Ez egy gyors áttekintés az infrastruktúránk egészségi állapotáról. Itt már indítás után láthatjuk, ha valamelyik kiszolgálónkkal valami probléma van. Ezeket a csoportokat, illetve benne lévő különböző ellenőrzési, mérési pontokat piros színnel jelzi a rendszer. Elég rákattintani a kérdéses részekre máris bővebb információt kapunk.

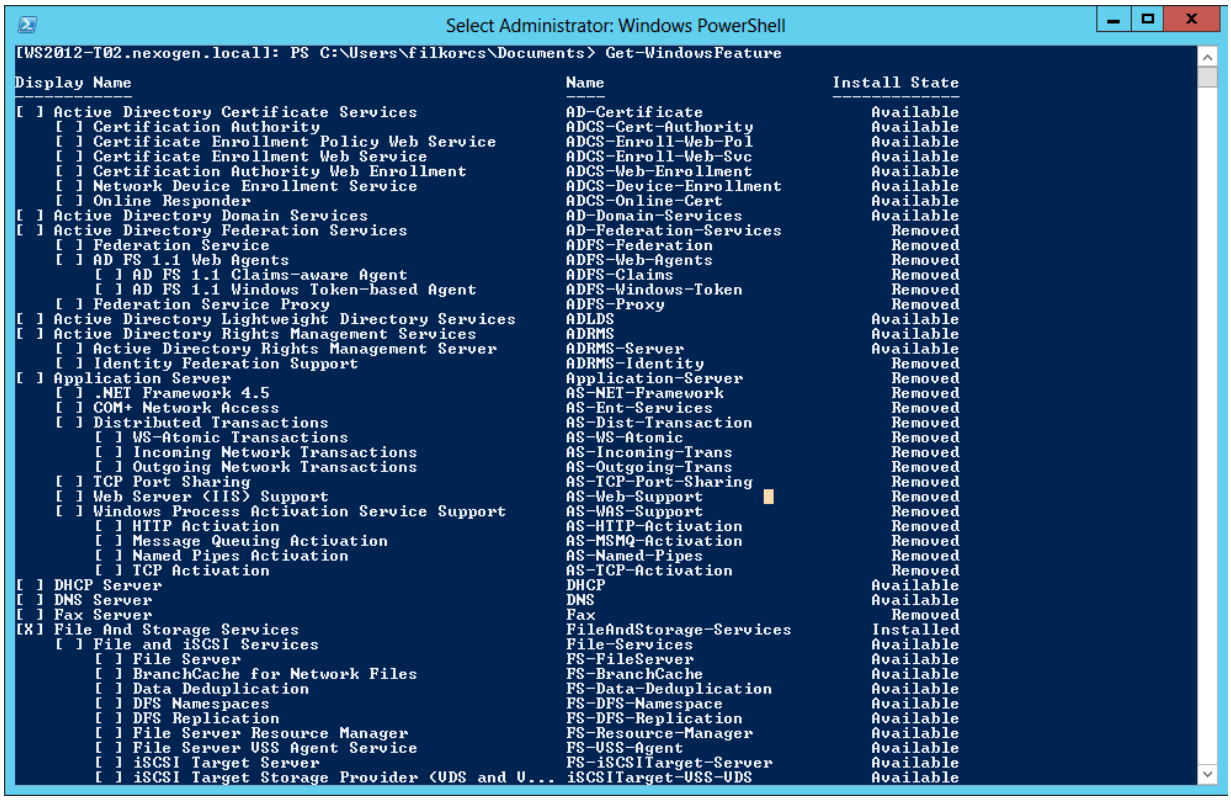


A távoli kiszolgáló adminisztrációja megoldható PowerShell segítségével is. Kattintsunk a kívánt szerverre és az előugró menüből válasszuk a PowerShell parancsot. Telepítsünk egy szerepkört, ehhez nagy segítséget nyújthat a következő parancs:

```
Get-WindowsFeature
```

Nevével ellentétben a parancs felsorolja az összes olyan szerepkört és szolgáltatást, amely telepítve van (Installed) és amely telepíthető (Available, Removed).

Ha szerepkörrel vagy/és szolgáltatással szeretnénk bővíteni kiszolgálónkat, akkor a listában látható „Name” alatti mezőben lévő felsorolás alapján könnyen be tudjuk azonosítani a pontos nevét. Ha több dolgot szeretnénk telepíteni, azokat vesszővel elválasztva soroljuk fel a parancs után.



A telepítés az Install-WindowsFeature paranccsal történhet.

```
Install-WindowsFeature DNS, DHCP
```

A parancs végrehajtását mutatja a képernyő tetején elhelyezkedő folyamatjelző.

További hasznos parancsok a teljesség igénye nélkül:

Process cmdlet-ek:

- Get-Process. – Információk a futó folyamatokról
- Start-Process – Folyamat indítása
- Stop-Process – Folyamat leállítása

Event Log Cmdlet-ek:

- Get-Eventlog – beírva a napló nevét (pl. system, application, setup), kilistázza az eseményeket.
- Clear-Eventlog – beírva a napló nevét (pl. system, application, setup) kitörli belőle az eseményeket.
- Limit-Eventlog – Az eseménynapló méretét szabályozhatjuk ezzel.
- Show-Eventlog – Grafikus felületű eseménynapló, pl. Server Core-nál hasznos lehet.

A Server Managementből elérhető PowerShell alól úgy is tudunk szerepköröket és szolgáltatásokat telepíteni, hogy a telepítendő kiszolgáló egy kikapcsolt virtuális gép. Ennek a következő feltételei vannak:

- A telepítendő gépnek Windows Server 2012-nek kell lennie.

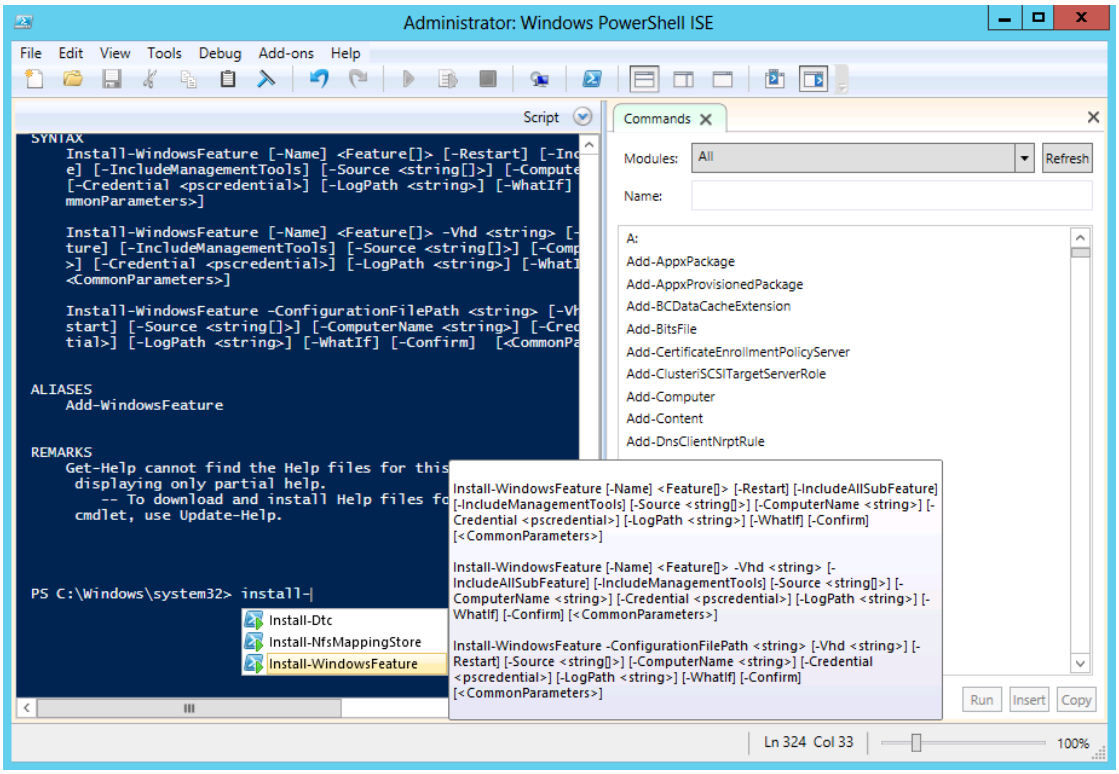
- Nem lehet egynél több partíciója vagy merevlemeze.

A parancs szintaktikája:

```
Install-WindowsFeature -Name <feature_name> –VHD <path> -ComputerName <com-
        puter_name> -Restart
```

Sok segítséget adhat a Windows 2012-ben megjelenő új PowerShell ISE (Integrated Scripting Engine), amely szintén telepíthető a fenti módszerrel, mint szolgáltatás. Található benne:

- Integrated Help – Keresés a PowerShell parancsok között, akár pár karakter beírása után felajánlja a lehetőségeket a parancsok közül.
- IntelliSense – Tanácsot ad a parancs teljes szintaktikájára vonatkozóan.



4.3 Gyakorlati feladatsor

Windows Server 2008 és Windows Server 2008 R2 kiszolgálóinkat tegyük képessé arra, hogy a 2012-es Server Managerből tudjuk őket felügyelni.

1) Válasszunk egy tetszőleges 2008 vagy 2008 R2 operációs rendszerrel ellátott kiszolgálót.
2) Telepeítsük fel a telepítés fejezet által részletezett frissítéseket illetve konfiguráljuk a WinRM-et.
3) Vegyük fel a kiszolgálót a Server Managerbe.
4) Futtassunk rajta Best Practice Analyzert.
5) Hozzunk létre egy csoportot, nevezzük el és adjuk hozzá a kiszolgálót.
6) Ellenőrizzük, hogy elindul-e a távoli PowerShell.
7) Itt adjunk hozzá a Telnet-Client szolgáltatást.

5 Adattárolás

A biztonságos adattárolás minden hálózati operációs rendszer egyik fő feladata. A jelenlegi adattárak nincsenek megfelelően felkészítve a nagyméretű adatok, vagy akár 10-20 terrabájtos partíciók kezelésére. Az új Windows Server ebben a témakörben is rengeteg kisebb-nagyobb változást hoz. Ebben a fejezetben a következő technológiákat nézzük végig:

- Multiterabájtos partíciók
- Data deduplication
- Thin provisioning
- Storage Spaces
- iSCSI kiszolgáló szerepkör
- Offloaded data transfer

5.1 Multiterabájtos partíciók

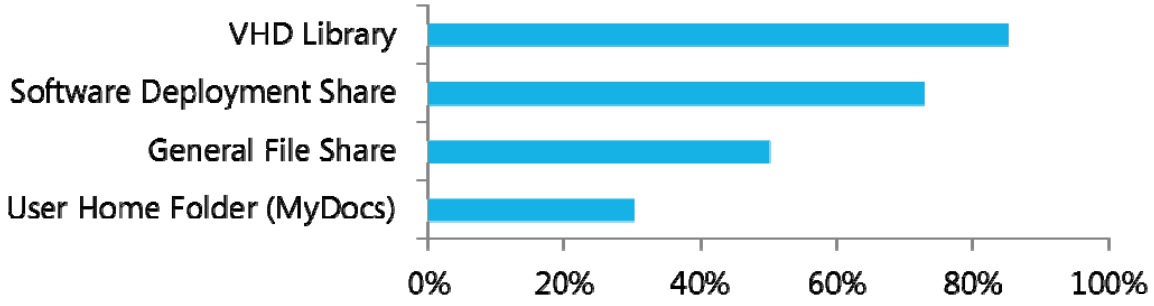
Az előző Windows verziókban a több terrabájtos partíciók kezelése meglehetősen körülményes volt. Ha próbáltunk már chkdsk-et futtatni egy nagyobb partíción, akkor tapasztaltuk, hogy a folyamat akár órákig is tarthat, miközben az adott partíció nem elérhető. A továbbfejlesztett chkdsk viszont képes a nagyobb méretű partíciókat részenként ellenőrizni, miközben a partíció többi része on-line állapotban marad, így elérhető a felhasználók számára.

5.2 Data deduplication

Az Exchange Server régebbi verzióiban létezett egy Single Instance Storage nevű szolgáltatás, ami az adatbázison belül képes volt a duplikált adatokat egyszeri fájltárolással átcsoportosítani, vagyis, ha egy e-mail több példányban szerepelt az adatbázisban, akkor egy levelet megtartott, a többit törölte, helyükre pedig hivatkozásokat helyezett el, amelyek az eredeti levél helyére mutattak.

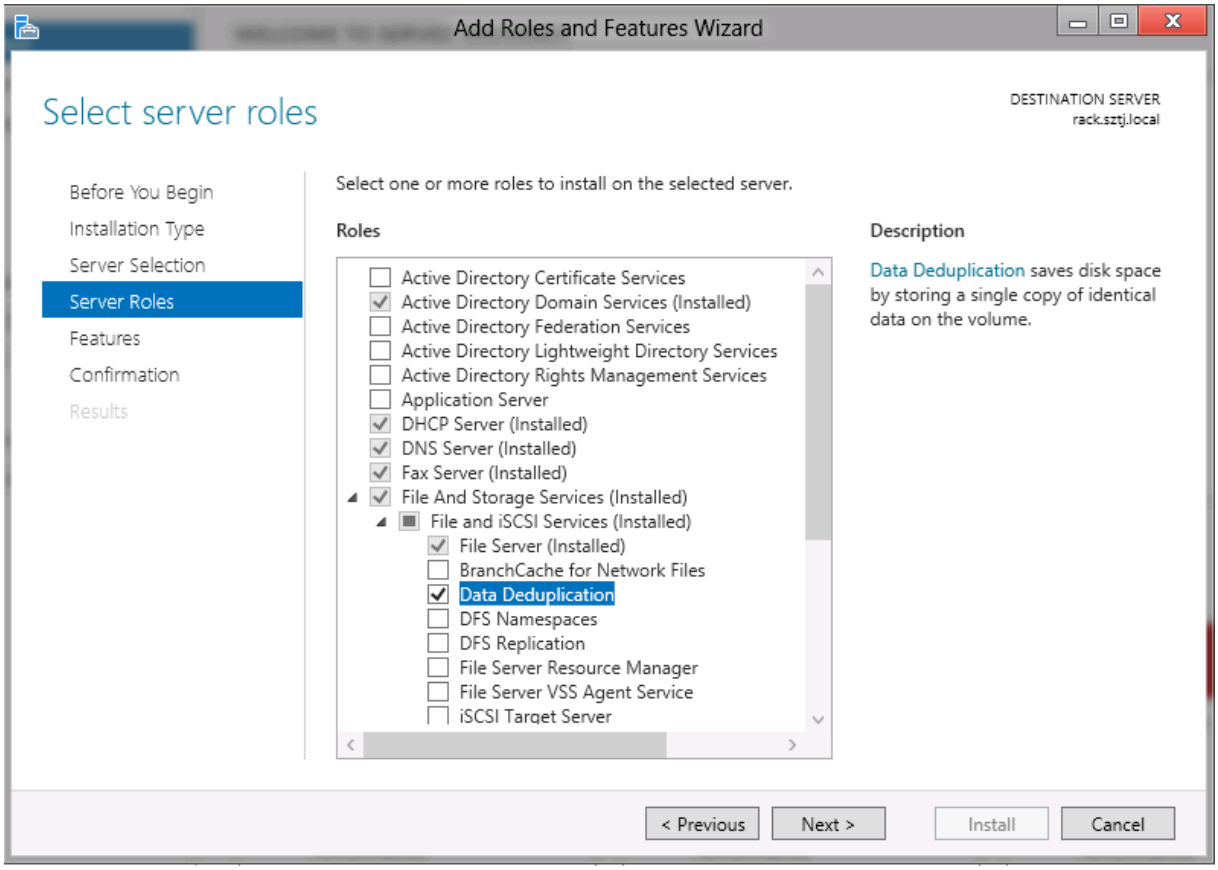
A Windows Server 2012-ben bemutatkozó Data Deduplication szolgáltatás hasonló feladatot lát el a lemezeinken, persze nem csak fájl, hanem blokk szinten, így például különböző VHD fájlokban az azonos tartalmakat felismeri, és konszolidálja.

Ez a funkció nagyon hasznos lehet akár egyszerű fájlmegosztásokon is, de elengedhetetlen kelléke a VHD könyvtáraknak, a szoftvertelepítések disztribúciós könyvtárainak, vagy a Windows központi távtelepítési kiszolgáló adattárának.



Átlagos használati arány, különböző felhasználásnál

A Data Deduplication szolgáltatás rész-szerepköre a File and Storage management szerepkörnek, telepítését tehát a Server Manager/File and Storage management/Add role service-nél tudjuk indítani:



A beállítások partíciónként érvényesülnek, és a File and Storage Manager-ben, a Volume résznél tudjuk őket beállítani. Itt megadható, hogy az 5 napnál régebbi fájlokat kezdje ellenőrizni, illetve, hogy milyen mappákat zárjon ki a folyamatból.

5.3 Thin Provisioning

Ez a funkció a Hyper-V VHD formátumánál használható dinamikus méretű VHD állományokra hasonlít, azzal a különbséggel, hogy a fizikai gép köteteit tudjuk kezelni. A funkció lényege, hogy amikor létrehozunk egy partíciót, az kizárólag a felhasznált tárterületet fogja

használni a lemezen, a többi terület kioszthatóvá további partícióknak. Így akár egy 500GB-os lemezen létrehozhatunk több, 1-1 TB-os partíciót is. Amikor a partíciók elkezdenek betelni, további lemezeket adhatunk a már meglévő partíciók „alá”.

5.4 iSCSI Server szerepkör

Az iSCSI szolgáltatás lehetővé teszi, hogy kiszolgálónk úgy érje el egy másik kiszolgáló lemezét, mintha helyi lemez lenne, tehát nem SMB megosztáson kereszül, hanem közvetlenül SCSI parancsokkal, blokk-szinten. A storage-ban lévő iSCSI meghajtók tehát helyi lemeznek látszódnak az iSCSI kliens gépeken. Ez nagyon hasznos olyan szolgáltatásoknál, amelyek kizárólag helyi meghajtókra képesek dolgozni (pl. Hyper-V, Exchange, SQL Server), de az adatainkat mégis egy központi adattárolón szeretnénk elhelyezni. Az iSCSI tároló használatához szükségünk lesz egy iSCSI kiszolgálóra, ami része a Windows Server 2012-nek, és egy iSCSI kezdeményezőre (initiator), ami már régóta megtalálható a Windows régebbi verzióiban is. A rendszer fontos része a redundancia: lehetőségünk van többirányú IP kapcsolat kiépítésére a kiszolgáló és a kezdeményező között.

Komponensek:

- IP hálózat: legalább gigabites kapcsolat a végpontok között. Használhatjuk a NIC teaming funkciót a nagyobb sebesség és magas rendelkezésre állás eléréséhez.
- iSCSI Target: a tárolón futó szerepkör, hozzáférést biztosít a lemezekhez.
- iSCSI initiator (kezdeményező): szoftver-komponens vagy hardveres eszköz, amely kapcsolatot létesít az iSCSI targettel. Amennyiben hardveres eszköz, akár az operációs rendszer partíciója is lehet iSCSI targeten, így az alap kiszolgálóban egyáltalán nincs merevlemez.
- iSCSI qualified name (IQN) egy egyéni azonosító, amely az iSCSI initiator-t és az iSCSI targeteket azonosítja.

A Windows Server 2012 File and Storage szerepkör része az iSCSI Storage Server. Telepítése után lehetőségünk van iSCSI targetek létrehozására, iSCSI initiator hozzárendelésére, illetve további biztonsági beállításokra, mint a CHAP hitelesítés beállítására, akár mindkét irányba.

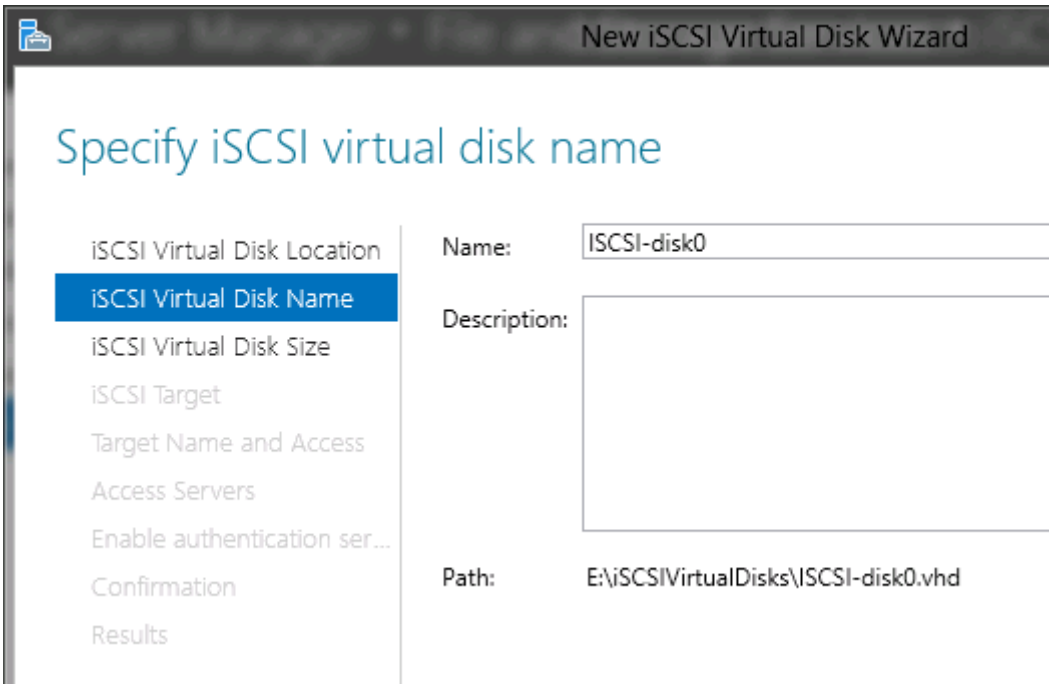
5.4.1 iSCSI magas rendelkezésre állás

A lemezek elérése kritikus az alkalmazásaink és az operációs rendszer számára, így fontos, hogy iSCSI rendszerünk magas rendelkezésre állású legyen. Első lépésben érdemes egy külön, szeparált hálózatot kiépíteni az iSCSI forgalom számára, illetve további funkciókat is használhatunk:

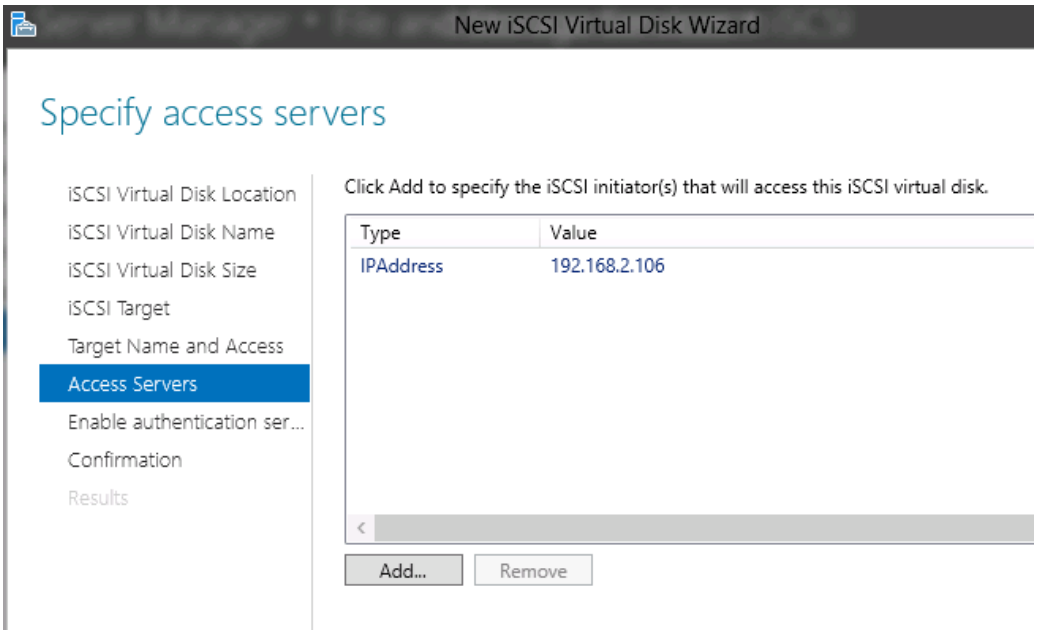
- MCS: lehetőségével több TCP/IP kapcsolatot építhetünk fel a kezdeményező és a target között, és egy kapcsolat megszakadásakor a forgalom automatikusan átterhelődik egy másik TCP/IP session-be.
- MPIO: multipath I/O, szélesebb körben elterjedt eljárás, ilyenkor a targetünket különböző IP címeken érjük el, több hálózati csatolón keresztül. Ha a target célhardver, szükségünk lesz további DSM-re (device specific module), de ha a Windows Server target servert használjuk, semmilyen további funkcióra nincs szükség.

iSCSI rendszer kiépítése

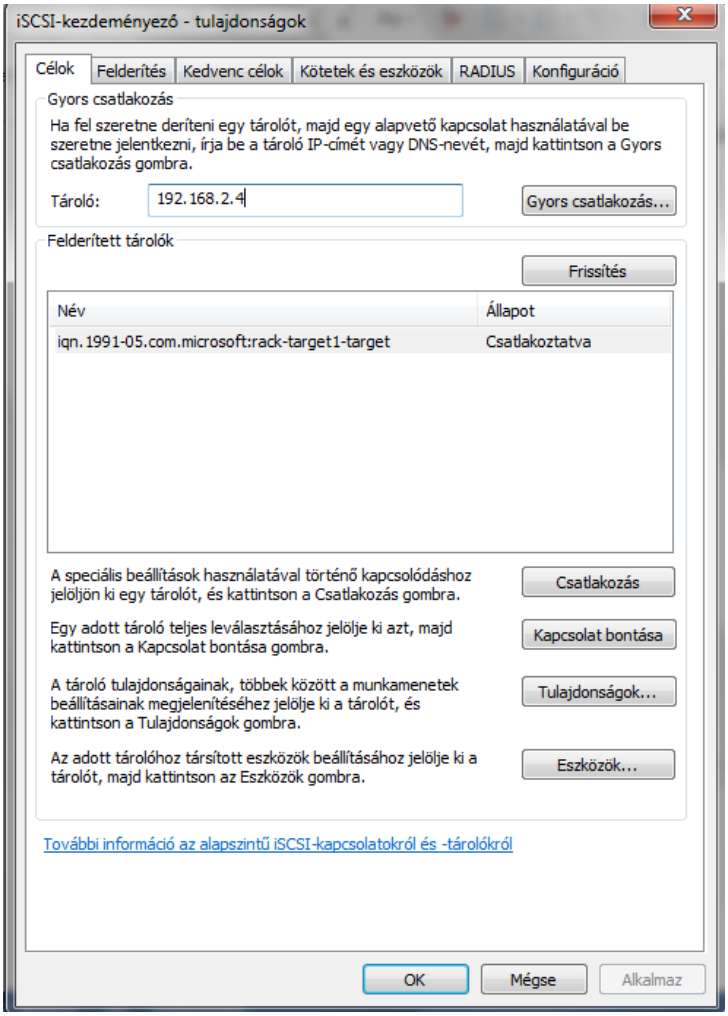
A szerepkör telepítése után létre kell hoznunk iSCSI virtuális lemezeket:



Ezután létre kell hoznunk egy új iSCSI target-et, vagy csatolhatjuk a lemezt egy meglévő iSCSI targethez. Ezt követően meg kell adnunk, hogy melyik initiator férhet hozzá a targethez. Megadhatunk IQN nevet vagy akár IP címet is.



Végül megadhatunk hitelesítési adatokat, mindkét irányba, akár az initiator, akár a target azonosításához (CHAP).



Miután létrehoztuk az iSCSI lemezünket, és a target-et is beállítottuk, a kliens oldalon csatlakozni kell a lemezhez. A csatlakozásnál elég a kiszolgáló IP címét megadni, az IQN nevet automatikusan feloldja:

Ha mindent jól csináltunk, végül az új lemez megjelenik a helyi gép lemezkezelőjében, mint helyi lemez. Ezután az initiatornál lehetőségünk van további IP címeket megadni az MPIO vagy az MCS kiépítéséhez.

5.5 Storage Spaces

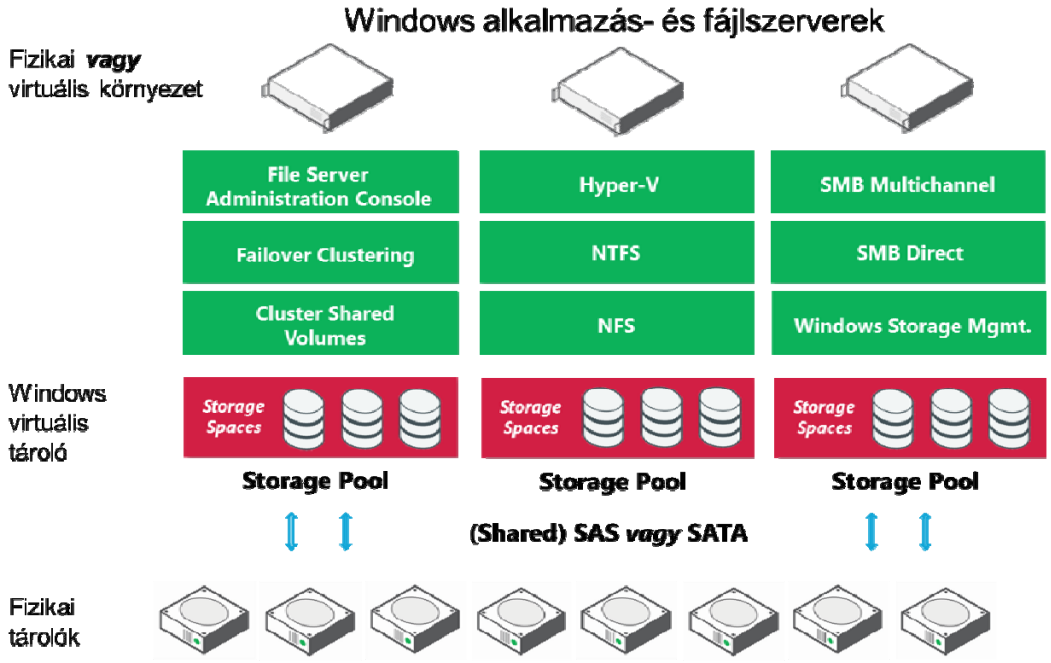
A Windows Server 2012-ben megjelenő új Storage Spaces szolgáltatás lehetővé teszi, hogy kiszolgálónkat SAN eszközként használjuk, legalábbis a különböző lemezeket egy egységként (pool) képes kezelni, és az operációs rendszer felé egy lemezként megjeleníteni.

A szolgáltatás egyfajta lemez-virtualizáció, melynek segítségével egy egységként kezelhetjük különböző lemezeinket.

Felépítése:

- Disk drive: ez a kötet, amit az operációs rendszer elér valamilyen meghajtó betűjellel.

- Virtual Disk: ez az eszköz reprezentálja a lemezt az operációs rendszernek, de szemben a fizikai lemezzel, ez menet közben bővíthető, tükrözhető, illetve egyéb hibatűrő megoldással védhető. Létrehozásakor választhatjuk a thin provisioning eljárást is.
- Storage Pool: fizikai lemezek gyűjteménye, akár helyileg, akár iSCSI-n csatolt lemezekből áll, ebből hozhatunk létre virtual disk-et.
- Physical Disk: SAS, SATA, iSCSI vagy egyéb felületen csatlakoztatott lemez. Legalább egy lemez kell storage pool létrehozásához, kettő a RAID1 virtual disk létrehozásához, illetve legalább 3 RAID5-höz. A SATA, SCSI vagy USB-s lemezeket nem használhatjuk failover cluster kialakításához, csak olyan csatolófelületeket, amelyek lehetővé tesznek több egyidejű kapcsolatot (pl. SAS, iSCSI)



Storage Space létrehozásakor különböző elrendezés közül választhatunk:

- Simple volume: egy vagy több fizikai lemezből álló egyszerű kötet, ami az adatokat egyszerre több lemezen tárolja, így biztosítva gyorsabb elérést. Nem hibatűrő, fontos adatainkat ne tároljuk ilyen lemezen.
- Two-way vagy three-way mirror: az adatokat tükrözve tárolja 2 vagy 3 lemezen, illetve csíkozni is képes több lemez között.
- Parity: RAID5 kötet, legalább 3 lemez használatával.

5.6 Offloaded Data Transfer

Az ODX kifejezetten nagyvállalalati környezetben, storage használatakor érdekes. Használatával úgy tudunk fájlokat, adatbázisokat, virtuális gépeket mozgatni kiszolgálók között, hogy az adat fizikailag nem megy át a hálózaton, hanem a storage-en belül képes mozogni, ezzel sokkal nagyobb sebességet tudunk elérni, és nem terheli a kiszolgáló CPU-t és memóriát.

6 Fájlszolgáltatások

Az adatok és erőforrások megosztása a legalapvetőbb feladat bármely hálózat esetén. A Windows Server 2012 további szolgáltatásokat is nyújt az alapvető megosztási és NTFS jogosultságokon felül, például az árnyékmásolat szolgáltatást, a kapcsolat nélküli fájlok, vagy a jogosultság alapú hozzáférés-vezérlés.

Ebben a fejezetben a következő szolgáltatásokat nézzük végig:

- NTFS jogosultságok
- Megosztási jogok
- Kapcsolat nélküli fájlok
- Árnyékmásolatok
- Kvótázás

6.1 Az NTFS fájlrendszer

Az NTFS fájlrendszer a Windows NT 3.1 óta alapköve a kiszolgáló operációs rendszereknek. Rengeteg beépített szolgáltatást tartalmaz, mint a jogosultság-kezelés, a kvótázás, a titkosítási és tömörítési lehetőségek, amelyek segítségével biztonságban tudhatjuk adatainkat. Ezek a funkciók a következők:

- NTFS jogosultságok fájlokhoz és mappákhoz
- Tömörítés
- Árnyékmásolat
- Titkosítás (EFS)
- Kvótakezelés
- Adat deduplikáció
- 16TB-os fájl- és partíció korlát
- Partíció átméretezhetőség

Az NTFS jogosultságok kezelésével közvetlen engedélyeket definiálhatunk fájlokhoz és mappákhoz. Ezek a jogosultságok mindenképpen érvenyesek, akár helyileg, akár hálózaton keresztül, vagy pl. FTP protokoll segítségével érjük el azokat.

Az NTFS jogosultságok fő tulajdonságai:

- A jogosultságok közvetlenül megadhatók fájlokra, mappákra, vagy fájlcsoportokra.
- A jogok kiadhatók felhasználóknak, csoportoknak, vagy akár számítógépeknek is.
- Engedélyt és megtagadást adhatunk a fájlokra. A megtagadás mindig erősebb lesz, mint az engedély.
- Az NTFS jogosultságok öröklődnek, így amikor egy mappára beállítunk egyéni jogosultságokat, a mappában később létrehozott fájlok és mappák a szülőmappa jogait öröklik.

6.1.1 Kioszthatók jogosultságok

Az NTFS fájlrendszerben a következő, ún. standard hozzáférési jogosultságokat tudjuk kiosztani:

Engedély	**Leírás**
Teljes hozzáférés	A felhasználó minden jogosultságot megkap a fájlokra és mappákra, illetve engedélyeket is állíthat.
Módosítás	A felhasználó írás, olvasás, törlés és létrehozás jogosultságot kap.
Olvasás és futtatás	Fájlok olvasása, program futtatása.
Olvasás	Mappák megnyitása, dokumentumok olvasása.
Írás	Fájl írása
Mappa tartalmának listázása	Csak mappára állítható, a felhasznál látja a mappában lévő fájlokat, de nem tudja megnyitni azokat.

Néhány fontos dolog az NTFS jogok beállításánál:

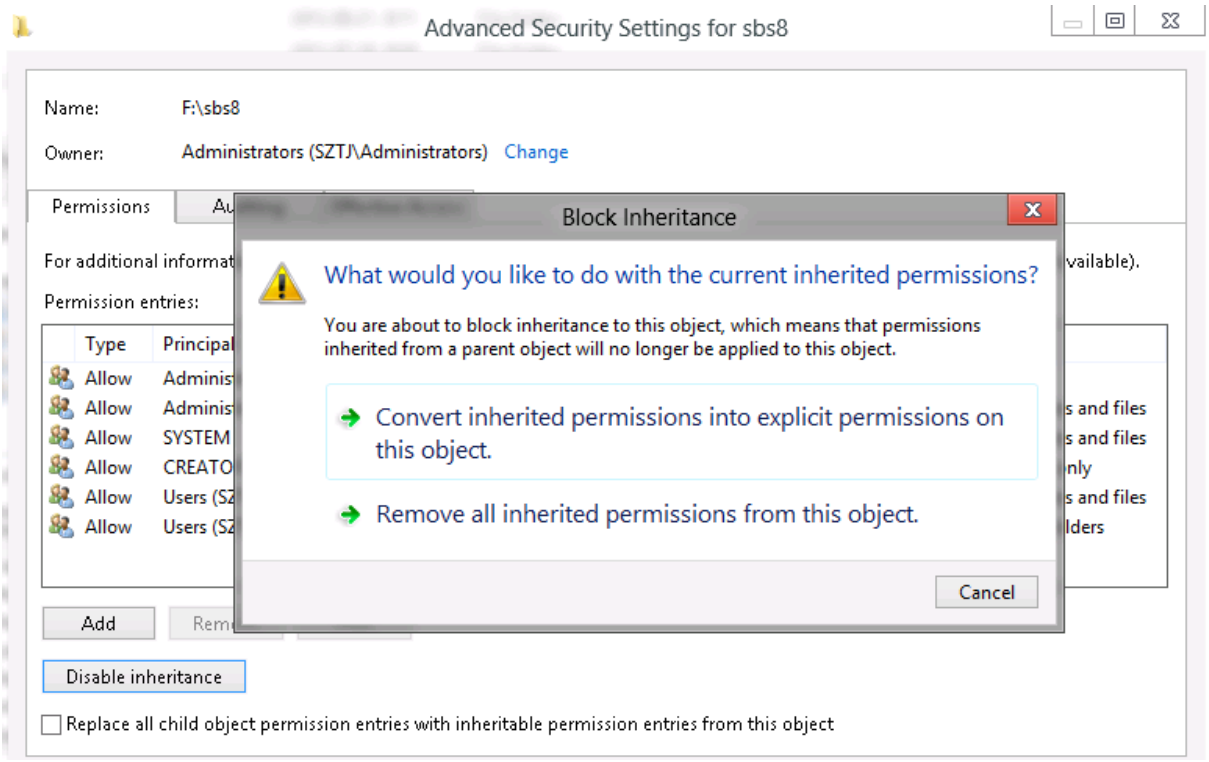
- Ha egy mappára örökölt, és közvetlen (explicit) jogosultság is érvényes, akkor a közvetlen jogok erősebbek lesznek
- Ha egy felhasználó egyszerre kap engedélyt és tiltást az adott objektumra, a tiltás mindig erősebb lesz (azonos szinten)

A kettő összegezve: egy felhasználó kaphat örökölt és közvetlen endegélyeket és megtagadásokat is. Ebben az esetben a sorrend:

- Közvetlen tiltás
- Közvetlen engedély
- Örökölt tiltás
- Örökölt engedély

6.1.2 Öröklődés

Az NTFS jogok alapértelmezésként öröklődnek, tehát amikor létrehozunk egy új fájlt vagy mappát, akkor az a szülőmappa jogait örökli. Ezt az öröklődést blokkolhatjuk, ilyenkor az objektum egyéni (explicit) jogosultságokat kap. Az öröklődés blokkolásakor kiválaszthatjuk, hogy le szeretnénk-e másolni a szülőmappa jogait, vagy törölni szeretnénk azokat, és attól teljesen eltérő jogokat szeretnénk definiálni.



Öröklött jogok blokkolása

Arra is lehetőségünk van, hogy egy szülőmappában visszaállítsuk az összes almappa és fájl jogosultságait örökölt jogokra, így az egyéni jogosultságok elvesznek. Ezt az ábrán látható „Replace all child object permission" opcióval tudjuk elérni.

6.1.3 Megosztási engedélyek

Amikor a fájlkiszolgálón megosztunk egy mappát, az erőforrássá válik. Ezeket az erőforrásokat tudják a felhasználók elérni a hálózaton, és rendszergazdaként az erőforrásoknak külön megosztási engedélyeket tudunk állítani. Ez egy plusz lépcső az NTFS jogosultságok mellett, egyfajta főkapcsolóként érdemes tekinteni: a globális jogosultságokat állítjuk megosztási szinten, a speciális, egyéni jogosultságokat pedig az NTFS-ben.

A megosztott erőforrásokat ún. UNC névvel tudjuk elérni:

\\kiszolgáló\erőforrás\mappanév\fájlnév

Pl: \\server\közös\képek\logo.jpg

Megosztásokat létrehozni a Windows Server 2012-ben többféleképpen is tudunk:

- A File and Storage Services programban
- Az intéző megosztás gyorsmenüjével (mappa/jobb klikk/megosztás)
- parancssorból a netsh vagy a net share parancsok segítségével
- A mappa tulajdonságain a megosztás fülön a speciális megosztásra klikkelve

6.1.4 Felügyeleti megosztások

A Windows Server 2012 automatikusan megosztja az összes merevlemezes partíciót rejtett megosztásként, amihez kizárólag a rendszergazdák férhetnek hozzá. Például a SERVER nevű számítógép C: meghajtójához a \\server\c$ UNC elérési úton férhetünk hozzá.

Rejtett megosztásokat mi is létrehozhatunk, ha a mappa megosztási nevének végére egy $ jelet teszünk, így a megosztás nem tallózható megosztássá válik.

6.1.5 Megosztási jogosultságok

A legfontosabb tudnivaló, hogy a megosztási jogok kizárólag akkor érvényesek, ha az adott mappát hálózaton keresztül érjük el. Amennyiben a mappát a felhasználók helyileg is elérik, akkor NTFS engedélyeket kell használnunk.

Megosztási jogosultságot adhatunk felhasználókra, csoportokra és számítógépekre, de megosztani csak mappát tudunk, egyéni fájlokat nem, így megosztási jog is csak mappánként állítható. A következő jogokat használhatjuk:

Megosztási jog	**Leírás**
Olvasás	A felhasználók megnézhetik a mappákat és a fájlokat, programokat tudnak futtatni, le tudják másolni a tartalmát, és a fájlok tulajdonságait is megnézhetik.
Módosítás	A felhasználók létrehozhatnak, módosíthatnak és törölhetnek mappákat és fájlokat.
Teljes hozzáférés	A fenti engedélyeken kívül jogosultságot is módosíthatnak fájlokon és mappákon. Ezt a jogosultságot általában csak rendszergazdáknak javasolt kiadni.

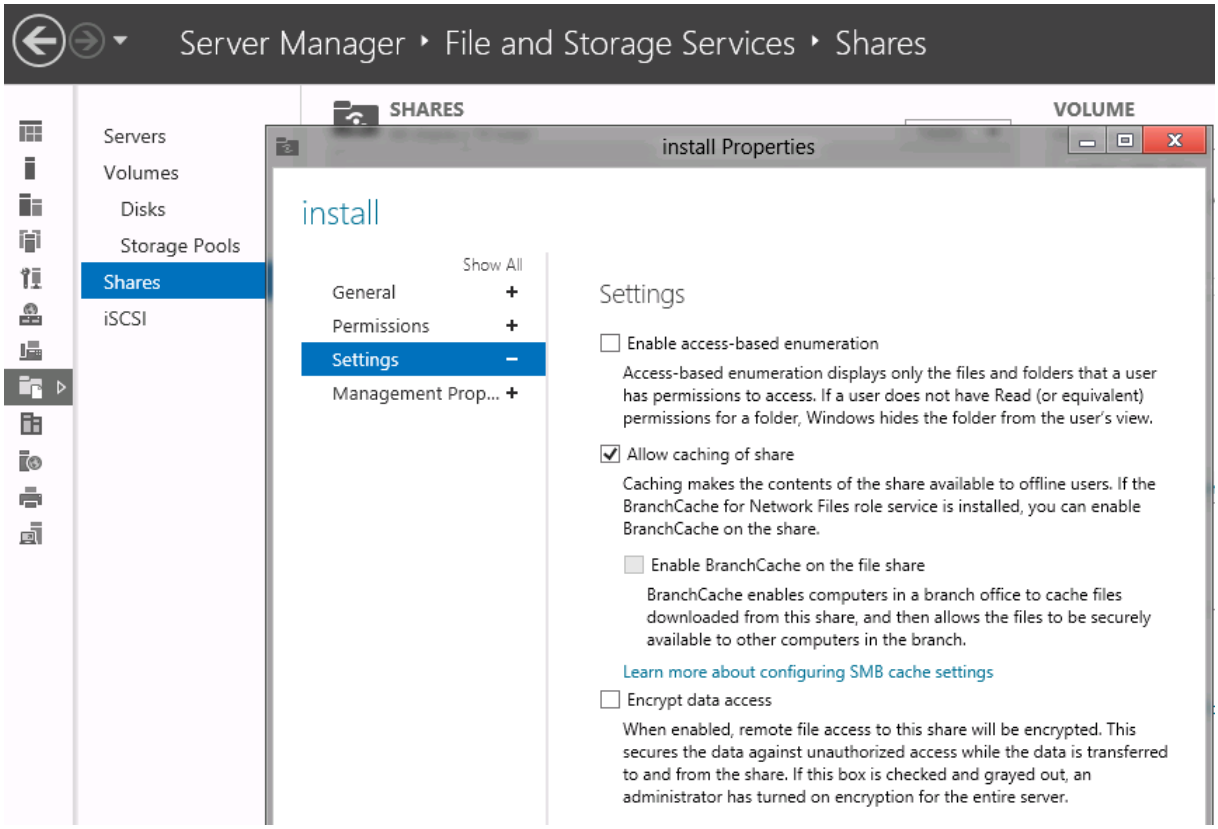
6.1.6 Effektív jogosultságok

Engedélyeket tehát megosztási és NTFS szinten is állíthatunk, illetve mindkét szinten egy felhasználó több jogosultsággal is rendelkezhet, attól függően, milyen csoportoknak a tagja.

Ha azonos szinten (pl. csak megosztásnál) több jogot is definiálunk, akkor mindig a nagyobb jog érvényesül. Tehát ha Gipsz Jakab, aki az alkalmazottak csoport tagja, egyénileg olvasás jogot kap, az alkalmazottak csoport pedig módosítás jogot, akkor a nagyobb jog, a módosítás érvényesül. Ugyanez igaz az NTFS jogosultságoknál is. Azonban, ha megosztási és NTFS szinten is definiálunk jogot, akkor az effektív jog a két jogosultság metszete lesz, vagyis mindig a kisebb jog érvényesül. Ezért a javasolt beállítás, hogy megosztási szinten adjuk ki a mappaszerkezetben bárhol használandó legnagyobb jogosultságot, és NTFS szinten szűkítsük a felhasználók hozzáférését az egyéni mappákhoz vagy fájlokhoz.

Access-based Enumeration (Hozzáférés-alapú vezérlés)

Az ABE lehetőséget ad arra, hogy a felhasználók elől elrejtsük azokat a mappákat, amikhez nincs hozzáférésük, ezzel egyszerűsíthetjük a munkát, biztonságosabbá tesszük rendszerünket, és megspórolunk néhány helpdesk hívást. Az ABE megosztásonként külön definiálható, a Server Manager File and Storage Services menüjében:



6.1.7 Kapcsolat nélküli fájlok

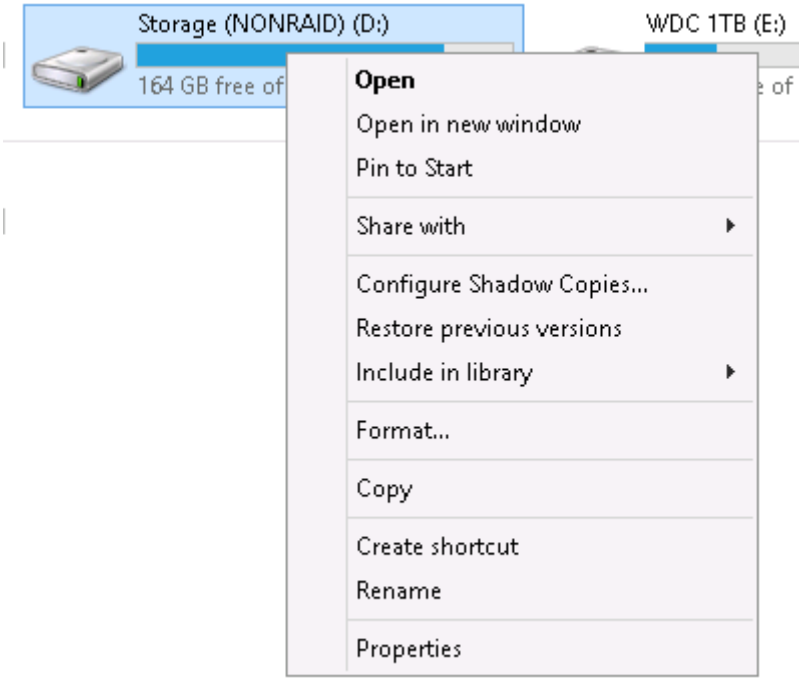
A megosztásokra állíthatunk kapcsolat nélküli elérést is, így a felhasználók akkor is elérhetik a megosztott mappák tartalmait, ha nincsenek kapcsolatban a kiszolgálóval, és a következő kapcsolódáskor a kliens gép szinkronizálja a változásokat a kiszolgálóval. Ehhez a megosztásnál engedélyezni kell a cache használatát, illetve a kliens gépeken (Windows XP-től felfelé) engedélyezni kell a kapcsolat nélküli fájlok használatát.

A Windows 2012-ben lehetőségünk van arra is, hogy a felhasználók folyamatosan off-line módban dolgozzanak, még akkor is, ha éppen hozzáférnek a kiszolgálóhoz, és csak a szinkronizálási ütemezés szerint fogják a módosításaikat felmenteni a serverre. Ezt a beállítást csoportházirendből tudjuk kikényszeríteni, a felhasználó beállításai/felügyeleti sablonok/hálózat résznél.

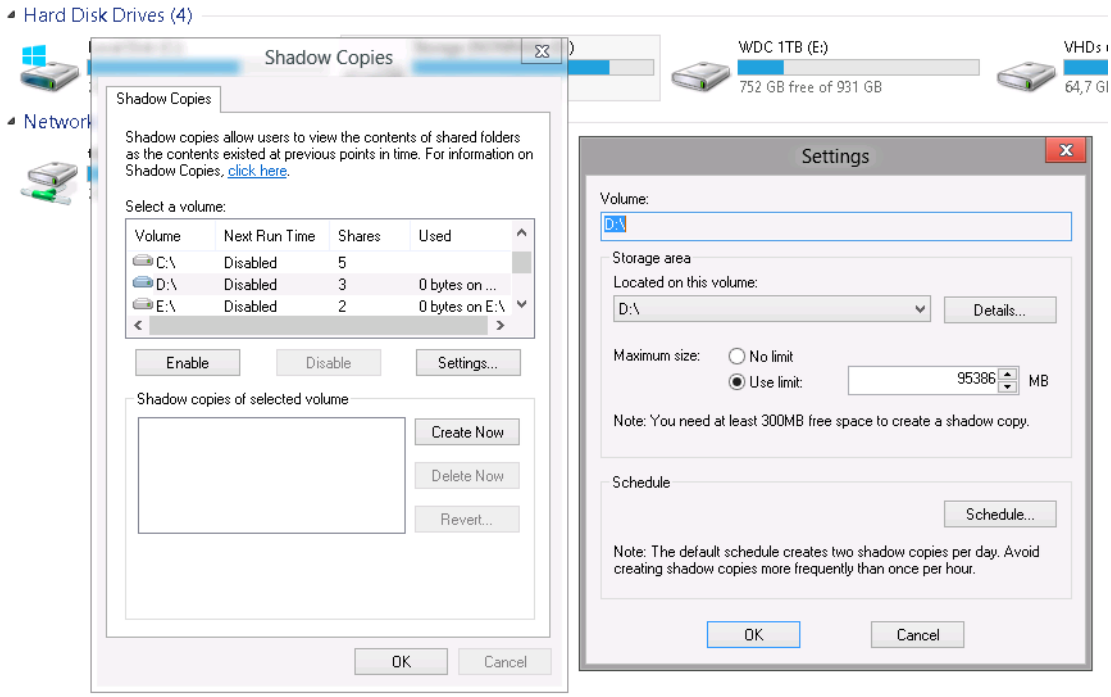
6.1.8 Árnyékmásolatok

Az árnyékmásolat szolgáltatás beépített része az NTFS fájlrendszernek, használatával a fájljaink és mappáink előző verzióit tudjuk visszaállítani, nem csak rendszergazdaként, hanem akár egyszerű felhasználói jogosultsággal is. Használatával csökkenthetjük a mentésből történő visszaállítások gyakoriságát.

Az árnyékmásolatokat partíciónként tudjuk beállítani, Windows intézőből, a Configure Shadow Copies menüpontban:



Konfigurálásakor megadhatjuk, hogy melyik lemezen tároljuk a fájlok előző verzióit, az árnyékmásolatok készítésének időpontját, illetve a maximálisan felhasználható lemezterületet. Alapértelmezésként a rendszer minden nap reggel 7-kor és délben készít mentést a módosult fájljainkról, illetve a kötet 10%-át használja fel árnyékmásolatok tárolására:

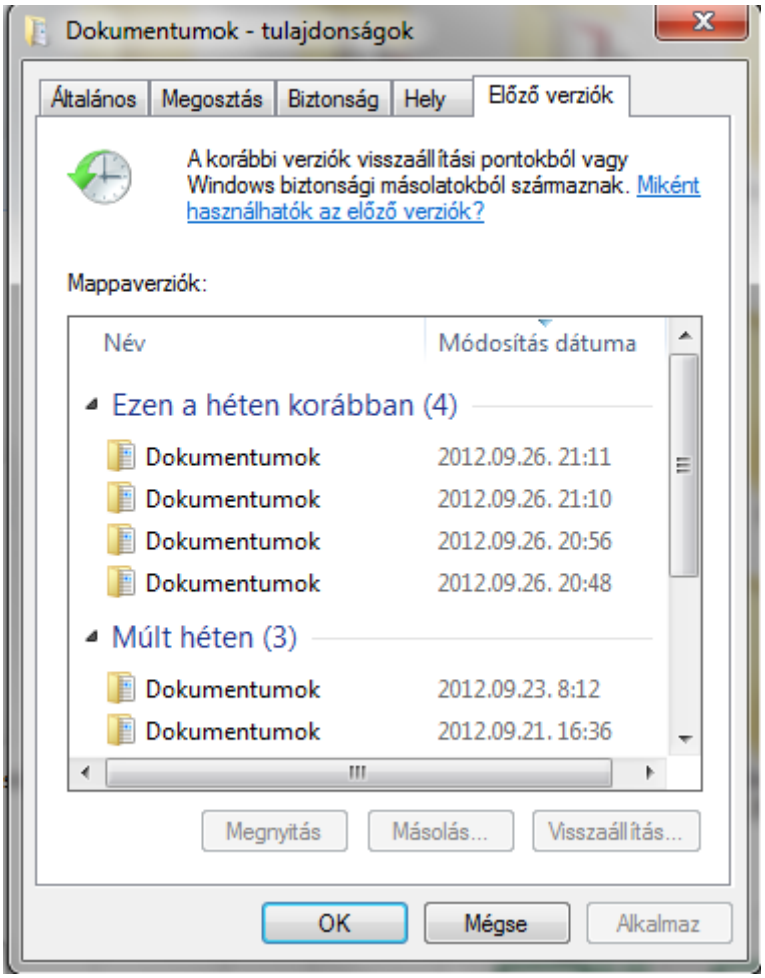


6.1.9 Az árnyékmásolatok működése

Az árnyékmásolat szolgáltatás tehát naponta kétszer készít mentés a fájljainkról, és annyi előző verziót tárol, amennyi elfér a fenntartott 10%-os lemezterületen. Ha a fenntartott terület megtelik, a legrégebbi árnyékmásolatokat automatikusan törli. Mivel az éles adatok és az árnyékmásolat ugyanazon a lemezen helyezkedik el, ez a megoldás nem váltja ki a rendszeres biztonsági mentés használatát.

6.1.10 Dokumentumok visszaállítása

Az árnyékmásolattal mentett dokumentumokat a felhasználók is vissza tudják állítani, ha a Windows intézőben a mappa tulajdonságainál az előző verziók fület választják:



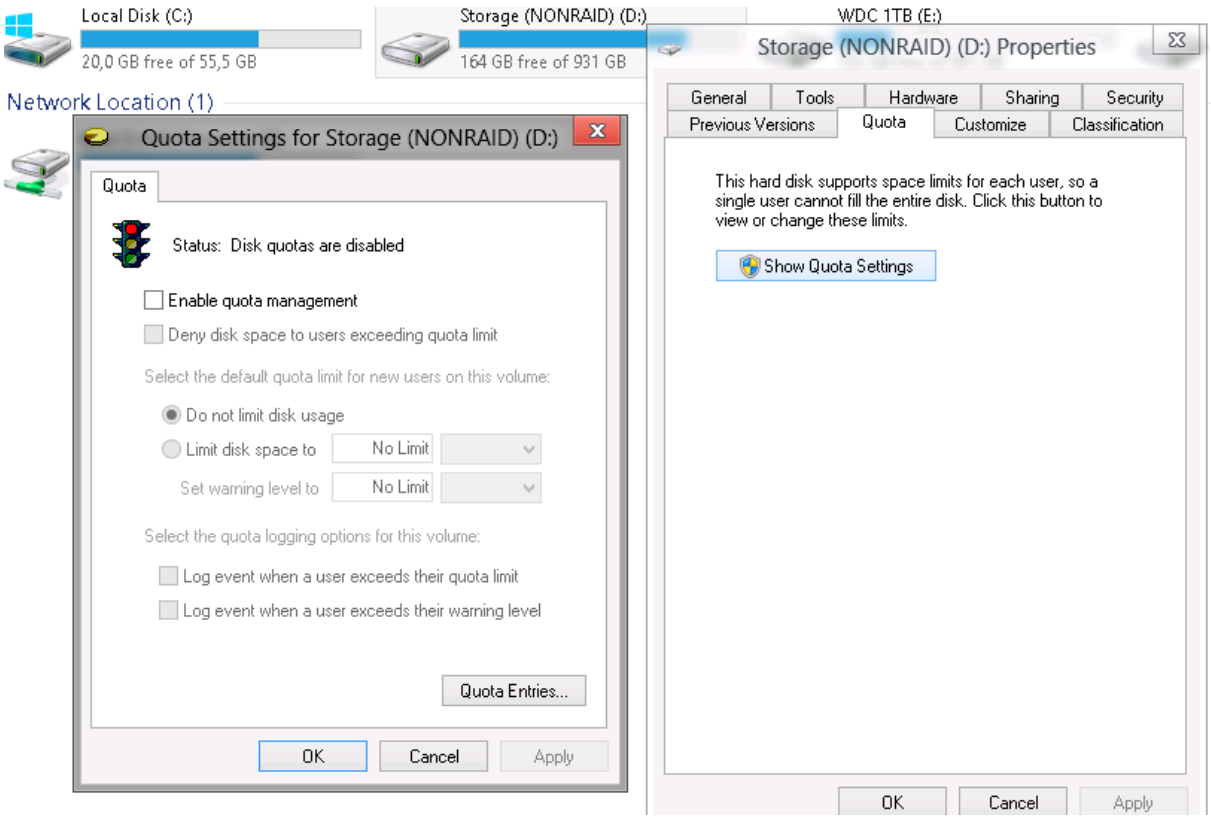
Itt láthatjuk a fájlok korábbi mentéseit, lehetőségünk van egy adott mappát megnyitni, egy régebbi időpontbéli tartalommal, a mappa régebbi állapotát lementeni egy másik helyre (másolás), illetve felülírni az aktuális verziót a régebbi állapottal (visszaállítás). Ha egy törölt fájlt vagy mappát szeretnénk visszaállítani, akkor a szülőmappa tulajdonságait kell megnyitnunk, illetve ennek a mappának a korábbi állapotát kell visszaállítanunk. A visszaállításkor figyelnünk kell arra, hogy az árnyékmásolat készítése óta létrejött vagy módosult fájlok törlésre kerülnek.

6.1.11 Kvótázás

Az NTFS fájlrendszerben lehetőségünk van korlátozni a felhasználók által használható lemezterületet.

A korlátozásra két lehetőségünk van: partíciónként kvótázhatunk a lemezkvóták használatával, vagy mappánként a fájlkiszolgálói erőforrás-kezelő segítségével.

Az egyszerű kvótázás tehát csak teljes partíciókra érvényes, és a partíción lévő összes mappára érvényes, függetlenül attól, hogy a fájlok hol helyezkednek el. A felhasználók által létrehozott és felmásolt, vagyis az ő tulajdonukban lévő fájlok számítanak bele a kvótájukba.



Bekapcsolni tehát partíciónként, a Windows Intézőből tudjuk. Megadhatunk ún. soft quota-t, ilyenkor a rendszer csak figyelmezteti a rendszergazdát, hogy bizonyos felhasználók túl sok tárterületet használnak, illetve megadhatunk hard quota-t is, ilyenkor a rendszer ténylegesen korlátozza a felhasználók lemezterületét. Engedélyezéskor meg kell még adnunk egy alapértelmezett kvótát, ami a már meglévő felhasználókra, és a meghajtót később használó felhasználókra is érvényes lesz, illetve a quota entries résznél egyéni kvótaértékeket definiálhatunk. Ez az egyéni érték pozitív és negatív irányban is eltérhet az alapértelmezett kvótától.

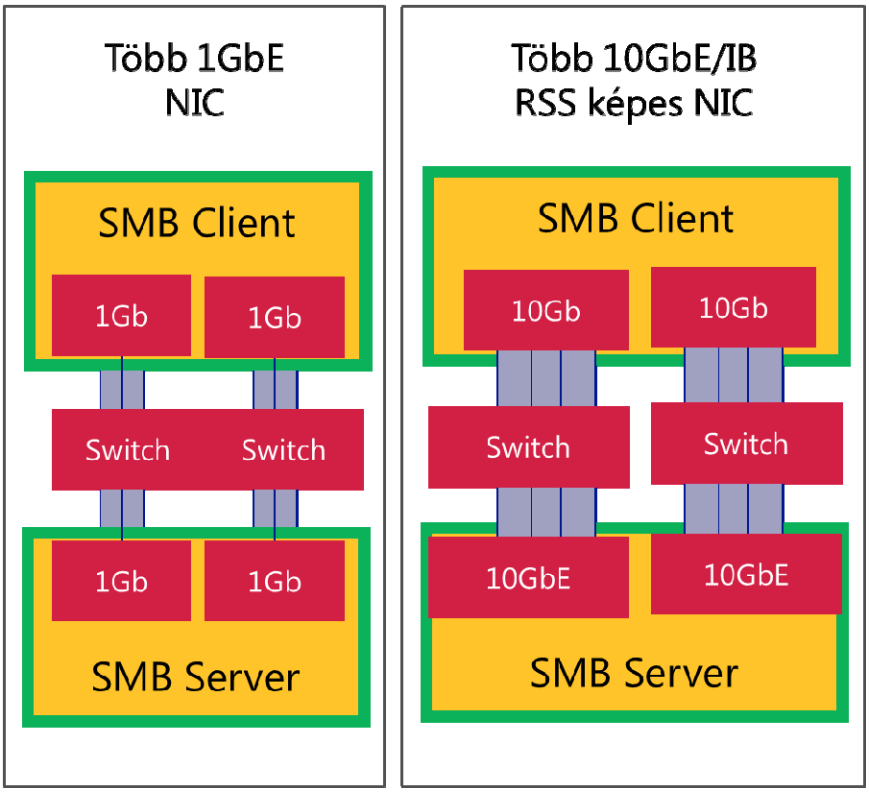
6.1.12 Újdonságok a Windows Server 2012-ben

A Windows Server 2012 SMB 3.0 protokollja hozott néhány újdonságot a fájlkiszolgáló szerepkörben is, ezek a következők:

- SMB titkosítás
- Multichannel
- Skálázhatóság
- Hibatűrés

SMB titkosítás használatával titkosított csatornát hozhatunk létre a fájlkiszolgáló és a kliens között, így nem kell IPSec titkosítást használunk. Megosztásonként engedélyezhető, vagy akár az egész fájlkiszolgálóra.

Az SMB multichannel összekapcsol több SMB csatornát, akár több hálózati kártyán keresztül, így nagyobb sávszélességet tudunk elérni, és nincs szükségünk MPIO vagy MCS konfigurálására:



Az SMB multichannel alapértelmezésként engedélyezve van a Windows Server 2012 kiszolgálón, PowerShellből tudjuk kikapcsolni:

```
Set-SmbServerConfiguration -EnableMultiChannel $false
```

Az SMB multichannel előnyei:

- nagyobb sávszélesség több hálózati csatoló összefűzésével
- hibatűrés: egy kapcsolat megszakadásakor a forgalmat automatikusan átterheli a maradék kapcsolatra
- Automatikus konfiguráció: a szerver az új hálózati kapcsolatokat automatikusan elkezdi használni.
- Több TCP csatornát használva a terhelést több CPU-ra szétoszthatjuk.

Az SMB skálázhatóság segítségével létrehozhatunk fürtözött fájlmegosztást több kiszolgálón, ahol a terhelést aktív-aktív módon szétosztjuk a szerverek között, így nagyobb teljesítményt, és hibatűrést érünk el. A több kiszolgálós megosztással a szerverek karbantartása alatt is elérhetőek a megosztásaink.

7 Active Directory

7.1 Active Directory újdonságok

Az alábbiakban összefoglaljuk a Windows Server 2012 Active Directory főbb újdonságait.

Funkció	**Fejlesztés**
Telepítés	A Server Managerből immár elérhető az AD DS szerepköri telepítés nem csak a helyi, hanem távoli gépre is. A telepítést megtehetjük PowerShell alól is. A Windows Server 2012 az AD DS telepítésekor egy Prerequisite check-et végez, amelyben feltérképezi a jelenlegi Active Directory infrastruktúrát.
Egyszerű adminisztráció	Konfigurálás és adminisztráció a Server Manager konzolban: Grafikus felületű Active Directory Lomtár Grafikus felületű Password management Group policy egészségi állapotfelmérés AD DS specifikus teljesítménymonitorozás és Best Practice analyzer Server Managerből elérhető AD adminisztrációs eszközök
Virtualizált tartományvezérlők támogatása	Tartományvezérlő klónozás az Automated Deployment and Rollback Protection segítségével. Tartományvezérlő visszaállítás snapshotból problémamentesen
Active Directory Module for Windows PowerShell	Új PowerShell parancsok a replikációs topológiához, Dynamic Access Controlhoz és egyéb tevékenységekhez. Nincs szükség DCPromo-ra az Active Directory kialakításához, mindezt PowerShell alól az új cmdlet-ek segítségével kényelmesen és egyszerűen megtehetjük.
Windows PowerShell History Viewer	Ha kezdők vagyunk PowerShellben, rövid idő alatt el tudjuk sajátítani az Active Directory Administrative Centerben, ahol láthatók, milyen PowerShell parancsok hajtódnak végre.
Active Directory Federated Services (AD FS)	Az AD FS Service szerepkört tartalmazza a Windows Server 2012, amely elengedhetetlenül szükséges felhő alapú hibrid telepítésekhez.

7.2 Active Directory telepítés

Az Active Directory telepítést négyféle módszer alapján tudunk elvégezni:

- Server Managerből, grafikus felületű varázslókkal
- Server Managerből, Powershell alapon
- Unattend telepítéssel (DCPromo)
- Virtuális tartományvezérlő klónozásával

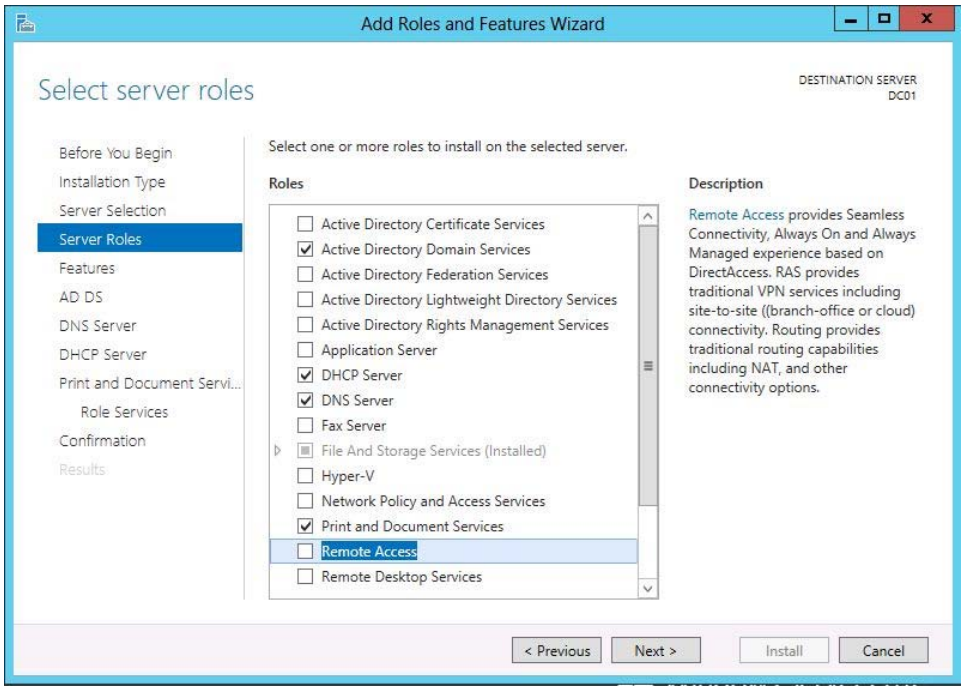
7.3 Ellenőrző lépések

A telepítés előtt ellenőrizendő lépések:

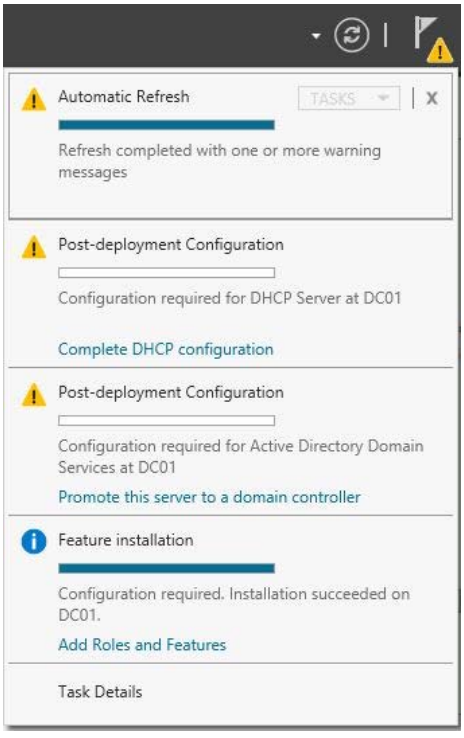
- a kiszolgálón Windows Server 2012 alaptelepítését elvégeztük
- a kiszolgáló rendszerpartíciója NTFS partíció
- a TCP/IP protokollt telepítettük és megfelelően beállítottuk; a hálózati kapcsolat kifogástalanul működik
- már van egy tartományvezérlőnk, az elérhető, a szükséges DNS-szolgáltatások hozzáférhetők és a DNS névfeloldás kifogástalanul működik
- megfelelő jogosultságokkal rendelkezünk a telepítés végrehajtásához.

7.4 Telepítés Server Managerből

A Server Managerből kiválasztjuk azt a kiszolgálót amelyre Active Directory Domain Services (ADDS) szerepkört szeretnénk telepíteni, lehet a helyi gép vagy bármelyik távoli kiszolgáló. Majd navigáljunk az adott kiszolgáló Roles and Features részére, és a Task-ban válasszuk az Add Roles and Features lehetőséget, aztán a megjelenő varázslóban válasszuk ki a következő szerepköröket.



A beállításokat követően újra kell indítanunk a kiszolgálónkat. Majd a bejelentkezés után a Server Manager „zászlós” Notifications részénél a következőt láthatjuk:



Nyomjunk a Post-deployment Configuration-re, állítsuk be az AD DS-t a kiszolgálón.

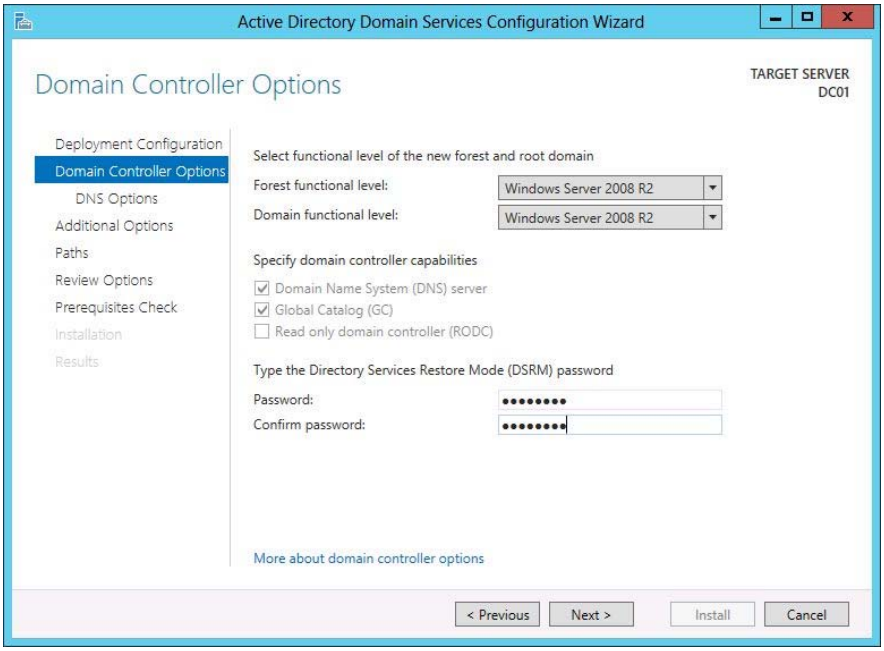
Az első képernyőn el kell döntenünk az Active Directory telepítés módját:

- hozzáadjuk a kiszolgálót egy meglévő tartományhoz
- hozzáadunk egy új tartományt egy már meglévő erdőhöz
- egy új erdőt telepítünk.

(Jelen példában a második lehetőséget választjuk.)

Majd meg kell adnunk a tartomány nevét.

Ezután meg kell adnunk az AD erdő és tartományi szintű funkcionalitást, illetve az Active Directory visszaállításának jelszavát.



A következő képernyőnél írjuk be a tartományunk NETBIOS nevét. Állítsuk be az adatbázis, a napló fájlok és a SYSVOL állományok helyét.

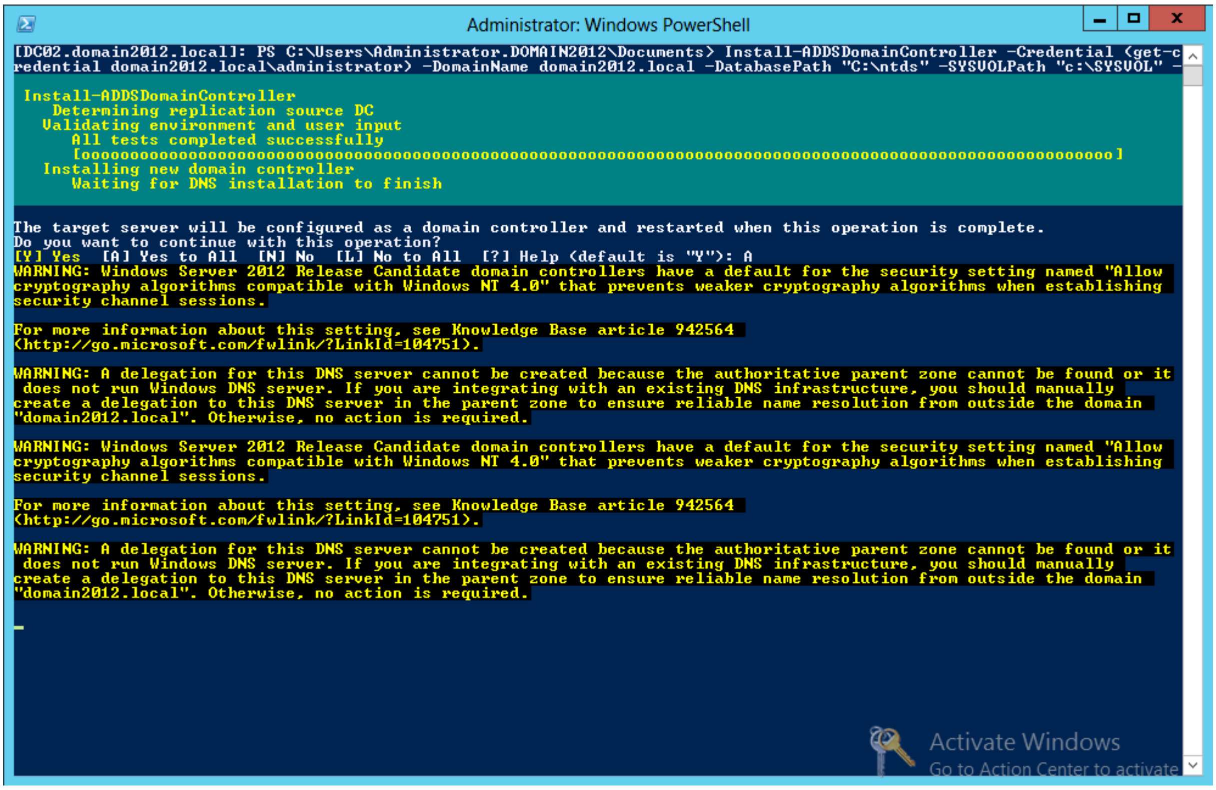
A Prequisites Check újdonság a Windows Server 2012-ben, itt még telepítés előtt felsorolja az összes problémát, ajánlást, amelyet az átvizsgálás során talált. Ha minden rendben, indíthatjuk a telepítést.

7.5 Telepítés Powershell segítségével

Indítsuk el az egyik kiszolgálónkon a Server Managert és válasszuk ki a tartományvezérlő szerepkörrel felruházandó kiszolgálót és indítsuk el a PowerShellt.

A kiszolgálónk felvétele egy már meglévő tartományba:

```
Install-ADDSDomainController –Credential (get-credential
        domain2012.local\Administrator) -CreateDNSDelegation –DomainName
        domain2012.local –DatabasePath "c:\NTDS" –SYSVOLPath "c:\SYSVOL"
        –LogPath "c:\Logs"
```



Új Forest létrehozása:

```
Install-ADDSForest [-SkipPreChecks] -DomainName <string> -
         SafeModeAdministratorPassword <SecureString> [-
         CreateDNSDelegation] [-DatabasePath <string>] [-
         DNSDelegationCredential <PS Credential>] [-NoDNSOnNetwork] [-
         DomainMode <DomainMode> {Win2003 | Win2008 | Win2008R2 |
         Win2012}] [-DomainNetBIOSName <string>] [-ForestMode <ForestMode>
         {Win2003 | Win2008 | Win2008R2 | Win2012}] [-InstallDNS] [-
         LogPath <string>] [-NoRebootOnCompletion] [-SkipAutoConfigureDNS]
         [-SYSVOLPath] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]

Install-ADDSForest -DomainName domain2012.local -CreateDNSDelegation -
         DomainMode Win2008R2 -ForestMode Win2008R2 -DatabasePath
         "c:\NTDS" -SYSVOLPath "c:\SYSVOL" -LogPath "c:\Logs"
```

Új gyerektartomány létrehozása:

```
Install-ADDSDomain [-SkipPreChecks] -NewDomainName <string> -
         ParentDomainName <string> -SafeModeAdministratorPassword
         <SecureString> [-ADPrepCredential <PS Credential>] [-
         AllowDomainReinstall] [-CreateDNSDelegation] [-Credential <PS
         Credential>] [-DatabasePath <string>] [-DNSDelegationCredential
         <PS Credential>] [-NoDNSOnNetwork] [-DomainMode <DomainMode>
         {Win2003 | Win2008 | Win2008R2 | Win2012}] [DomainType
         <DomainType> {Child Domain | TreeDomain} [-InstallDNS] [-LogPath
         <string>] [-NoGlobalCatalog] [-NewDomainNetBIOSName <string>] [-
         NoRebootOnCompletion] [-ReplicationSourceDC <string>] [-SiteName
         <string>] [-SkipAutoConfigureDNS] [-Systemkey <SecureString>] [-
         SYSVOLPath] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]
```

```
Install-ADDSDomain -SafeModeAdministratorPassword -credential (get-
         credential domain2012.local\Administrator) -NewDomainName child -
         ParentDomainName domain2012.local -InstallDNS -
         CreateDNSDelegation -DomainMode Win2003 -ReplicationSourceDC
         DC1.domain2012.local -SiteName Office -DatabasePath "d:\NTDS" -
         SYSVOLPath "d:\SYSVOL" -LogPath "e:\Logs" -Confirm:$False
```

7.6 Telepítés Server Core-on

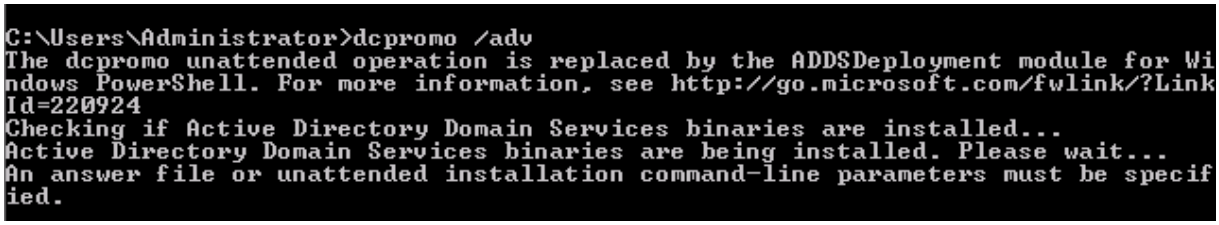
A Server Core ideális eszköz az Active Directory telepítésére, egyrészt kevesebb szervizt futtat, ezáltal kevesebb erőforrást és biztonsági frissítést igényel. Bár az adminisztratív eszközöket közvetlenül nem érjük el a kiszolgálón, viszont egy vele egy tartományban lévő gép Server Manageréből igen.

Lépjünk be Local Administratorként a már létrehozott Server Core-ra, amelyen *sconfig*-al már beállítottuk a nevét, domain tagságát, hálózati beállításait.

Adjuk ki a következő parancsot:

```
dcpromo.exe /adv
```

Ennek hatására elkezdődik az Active Directory bináris fájlaink telepítése.



A telepítés befejeztével létre kell hoznunk egy unattend.txt nevű fájlt, amely tartalmazza a telepítésre vonatkozó információkat. A telepítési beállításokat a következő paranccsal tudjuk kilistázni.

```
dcpromo.exe /?Promotion >  promotion.txt
```

Mivel elég sok telepítési kapcsoló létezik, ezért fenti parancs egy txt fájlba exportálja a kapcsolókat a könnyebb áttekinthetőség kedvéért.

Nyissunk meg egy üres unattend.txt fájlt a notepad.exe-vel, és a fenti kapcsolók segítségével írjuk bele a telepítési válaszainkat, például a következőt:

```
[DCInstall]
SafeModeAdminPassword=Passw0rd
ReplicaOrNewDomain=Replica
ReplicaDomainDNSName=domain2012.local
InstallDNS=Yes
ConfirmGC=Yes
DomainLevel=4
UserName=Administrator
UserDomain=Domain2012.local
Password=Passw0rd
```

Mindezek után már csak ki kell adnunk a parancsot:

```
dcpromo /unattend:unattend.txt
```

A telepítés után a fenti kapcsolók értelmében újraindul a kiszolgáló.

7.7 Operációs rendszer frissítése

Lépjünk be a Windows Server 2008 R2 operációs rendszerű tartományvezérlőnkre, miután eldöntöttük, hogy frissítjük Windows Server 2012-re. Menjünk a telepítő média Support\Adprep könyvtárába és futtassuk a következő parancsokat:

```
adprep /forestprep
adprep /domainprep
```

Az in-place upgrade a schema és tartományelőkészítést nem teszi meg. Ezután indíthatjuk az operációs rendszer frissítését.

Tegyük be a telepítő médiát és indítsuk el a telepítőt, majd nyomjunk egy Install Now-t.

- A Get important updates for Windows Setup résznél engedélyezzük, hogy a legfrissebb frissítéseket telepítse.
- Válasszuk ki, hogy a Windows Server 2012 melyik verzióját szeretnénk telepíteni.
- Az Installáció típusánál válasszuk az Upgrade lehetőséget.
- Compatibility Report résznél a telepítő átvizsgálja a kiszolgálót. Ellenőrzi a rendelkezésre álló tárhelyet és a hardvereszközöket.
- Next-re kattintva elindul a telepítés.

Bár maga az inplace upgrade egy egyszerű folyamat, a Microsoft ennek ellenére a friss telepítést ajánlja.

7.8 Tartományvezérlő klónozás

Könnyen létrehozható új tartományvezérlő a Windows 2012-ben beépített klónozásos technikával. Mindennek alapvető feltétele, hogy a klónozandó tartományvezérlő virtuális gép legyen.

További feltételek:

- A PDC Emulátor szerepkör Windows Server 2012 alatt fusson.
- A klónozandó tartományvezérlő tagja legyen a Cloneable Domain Controller csoportnak.
- Nem klónozható, nem kompatibilis alkalmazások ne legyenek rajta.

Legelőször adjuk hozzá a klónozandó tartományvezérlőnket a Cloneable Domain Controller csoporthoz az Active Directory Administrative Center-ben. Jobb gomb a pl. DC03-ra, Add to group.

Mindez PowerShell alól:

```
Add-ADGroupMember –Identity "CN=Cloneable Domain Controllers,CN=Users,
         DC=domain2012,DC=local" –Member "CN=DC03,OU=Domain
         Controllers,DC=domain2012,DC=local"
```

Azonosítsuk azokat az alkalmazásokat és szerepköröket, amelyeknek a klónozása nem támogatott.

Nem klónozható szerepkörök:

- Dynamic Host Configuration Protocol (DHCP)
- Active Directory Certificate Services (AD CS)
- Active Directory Lightweight Directory Services (AD LDS)

PowerShell alól adjuk ki a következő parancsot:

```
Get-ADDCCloningExcludedApplicationList
```

A parancs felsorolja azokat az alkalmazásokat és szerepköröket, amelyek klónozása nem támogatott. Amennyiben a parancs hatására a No excluded applications were detected jelenik meg, akkor a klónozás támogatott a tartományvezérlőn, ellenkező esetben a felsorolt alkalmazásokat, illetve szerepköröket távolítsuk el, vagy az adott tartományvezérlőt ne klónozzuk.

Konfiguráljuk a jövőbeni tartományvezérlőnket:

```
PS C:\Users\Administrator.DOMAIN2012> New-ADDCCloneConfigFile -Static -IPv4Address "172.16.1.10" -IPv4DNSResolver "172.1
6.1.1" -IPv4SubnetMask "255.255.255.0" -CloneComputerName "DC04" -IPv4DefaultGateway "172.16.1.1"
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or late
r...
Passed: The domain controller hosting the PDC FSMO role (DC01.domain2012.local) was located and running Windows Server 2
012 or later.

Verifying authorization: Checking if this domain controller is a member of the 'Cloneable Domain Controllers' group...
Located the local domain controller: (DC03.domain2012.local).
Querying the 'Cloneable Domain Controllers' group...
Pass: The local domain controller is a member of the 'Cloneable Domain Controllers' group.

Starting test: Validating the cloning allow list.
No excluded applications were detected.
Pass: No excluded applications were detected.

No valid clone configuration files were found at any of the supported locations.

All preliminary validation checks passed.

Starting creation of the clone configuration file...
Finding the path to the Directory Service database...
The clone configuration file was generated at:
C:\Windows\NTDS\DCCloneConfig.xml
Generating the clone configuration file content...
The clone configuration file has been created.

PS C:\Users\Administrator.DOMAIN2012>
```

Az egész klónozás kulcsa a SCCloneConfig.xml, elkészült.

Mindezek után állítsuk le a tartományvezérlőt.

```
Stop-VM –Name DC03 –ComputerName HyperV1
```

Leállítás után töröljük az összes Snapshotot, amennyiben létezik ilyen.

```
Get-VMSnapshot DC03 | Remove-VMSnapshot –IncludeAllChildSnapshots
```

Majd exportáljuk grafikus felületről vagy PowerShell alól:

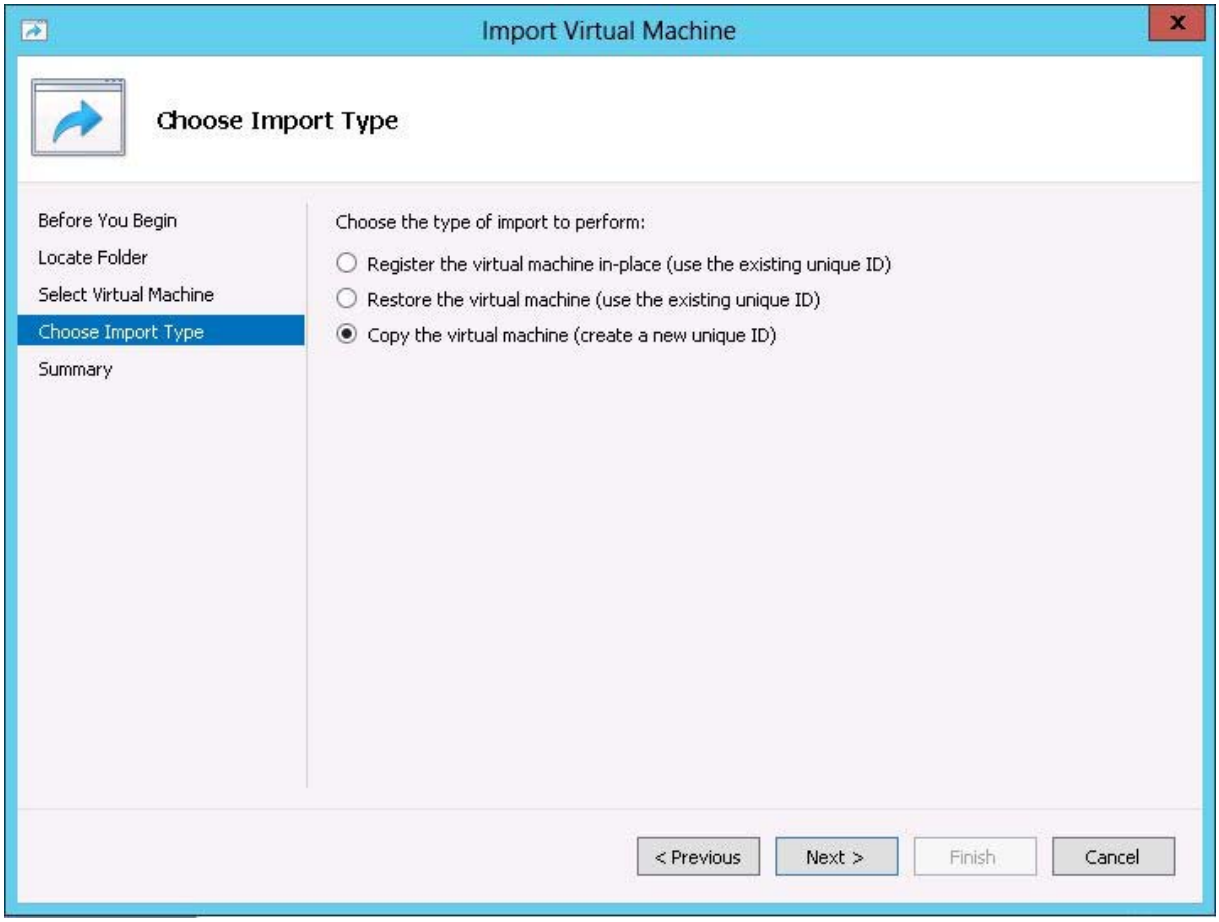
```
Export-VM –Name DC03 –ComputerName HyperV1 –Path c:\CloneDCs\DC03
```

Majd importáljuk az adott Hyper-V kiszolgálóra vagy akár egy másikra:

PowerShellből:

```
$path = Get-ChildItem "C:\CloneDCs\DC03\DC03\Virtual Machines"
$vm = Import-VM –Path $path.fullname –Copy -GenerateNewId
Rename-VM $vm DC04
```

Vagy grafikus felületről:

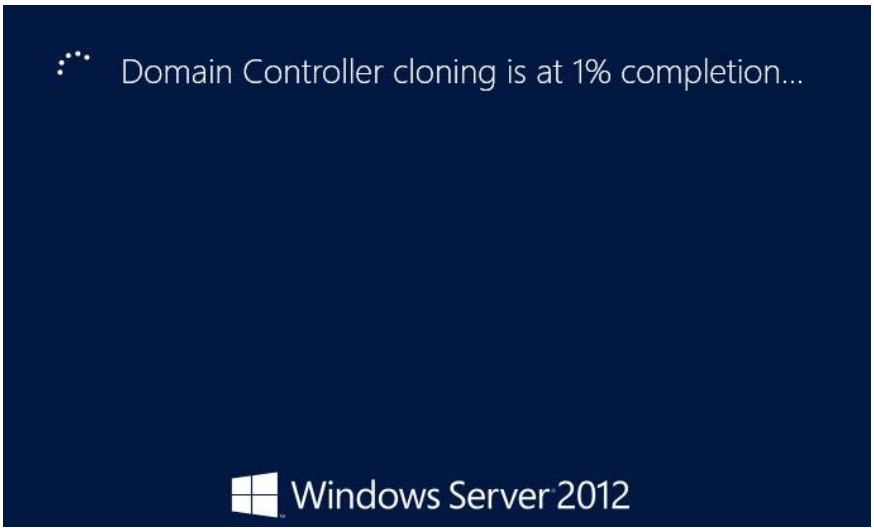


Fontos, hogy az importnál a DC-nek új egyedi azonosítója legyen.

Amennyiben az import sikeresen befejeződött, indítsuk el mindkét tartományvezérlőt (DC03 és az új DC04).

```
Start-VM –Name DC03 –ComputerName HyperV1
Start-VM –Name DC04 –ComputerName HyperV1
```

A DC04 indulása után megkezdődik az XML beolvasása és az annak megfelelő konfigurálás. 100 % elérése után a virtuális gépünk újraindul.



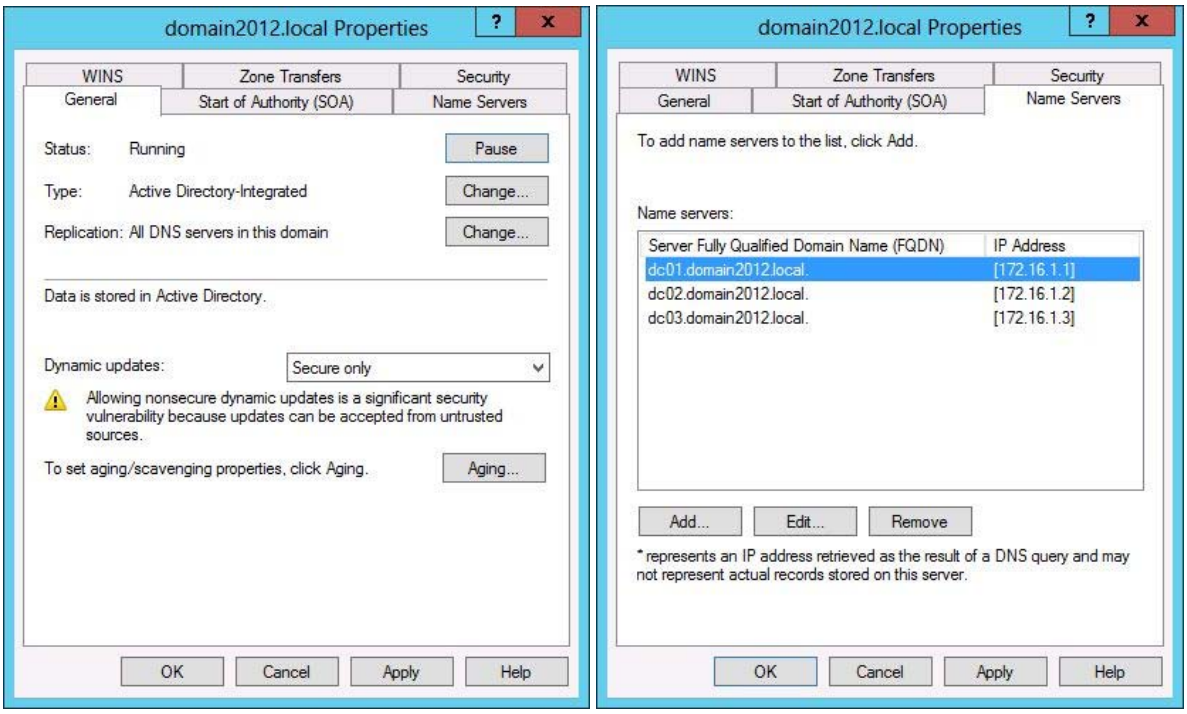
7.9 DNS beállítása

A DNS névfeloldás helyes működése alapvetően befolyásolja az Active Directory működését. A kliensek a DNS-től kapják meg, hogy mely számítógépek a tartományvezérlők, és a tartományvezérlők a DNS-ben tárolt információk alapján találnak replikációs partnereket.

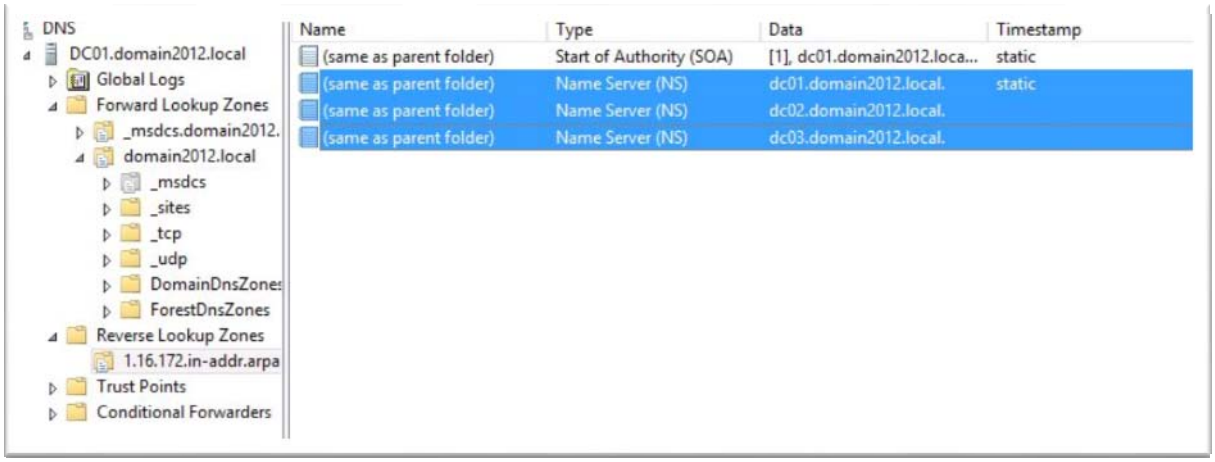
Az Active Directory által beállított DNS már használatra kész, minimális konfiguráció még szükséges lehet (mint pl. reverse lookup zone felvétele, esetleges conditional forwarders beállítása).

A tartományvezérlők DNS beállítása Active Directory integrált, ami azt jelenti, hogy a DNS adatok az AD-ban tárolódnak. A DNS adatok konzisztenciájának biztosítása a Dynamic Updates feladata.

A domain2012.local zóna tulajdonságaiban ezeket láthatjuk:



Vegyünk fel a domain2012.local Forward Lookup Zone-hoz egy Reverse Lookup Zone-t, majd adjuk hozzá az összes DNS szerepkörrel rendelkező tartományvezérlőnket.



Ajánlott beállítások a DNS-re vonatkozóan:

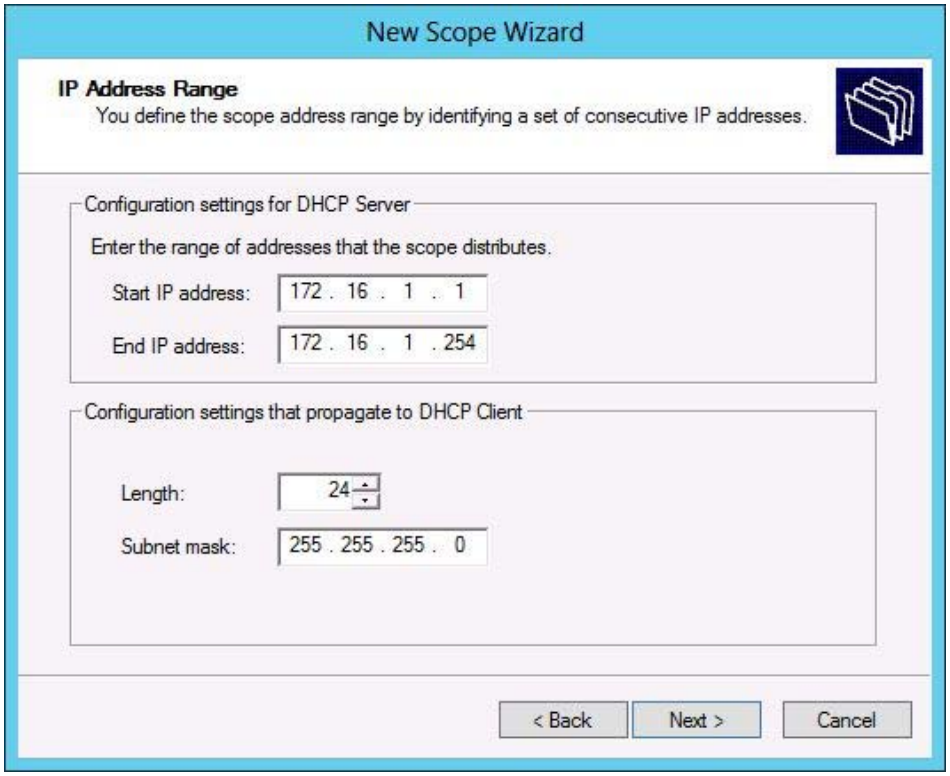
- Legalább két tartományvezérlőnk legyen.
- Minden tartományvezérlő legyen DNS kiszolgáló is egyben.
- A tartományvezérlők saját maguk DNS kliensei, másodlagos DNS-ként pedig egy másik tartományvezérlő kerüljön megadásra.
- A DNS rendszer Active Directoryba integrált zónák formájában valósuljon meg. Az Active Directory-ba integrált zónáknak köszönhetően nem kell külön zóna-transzfer beállításokkal foglalkozni.
- Minden DNS szerveren tartsuk meg a root hints beállításokat.

7.10 DHCP beállítása

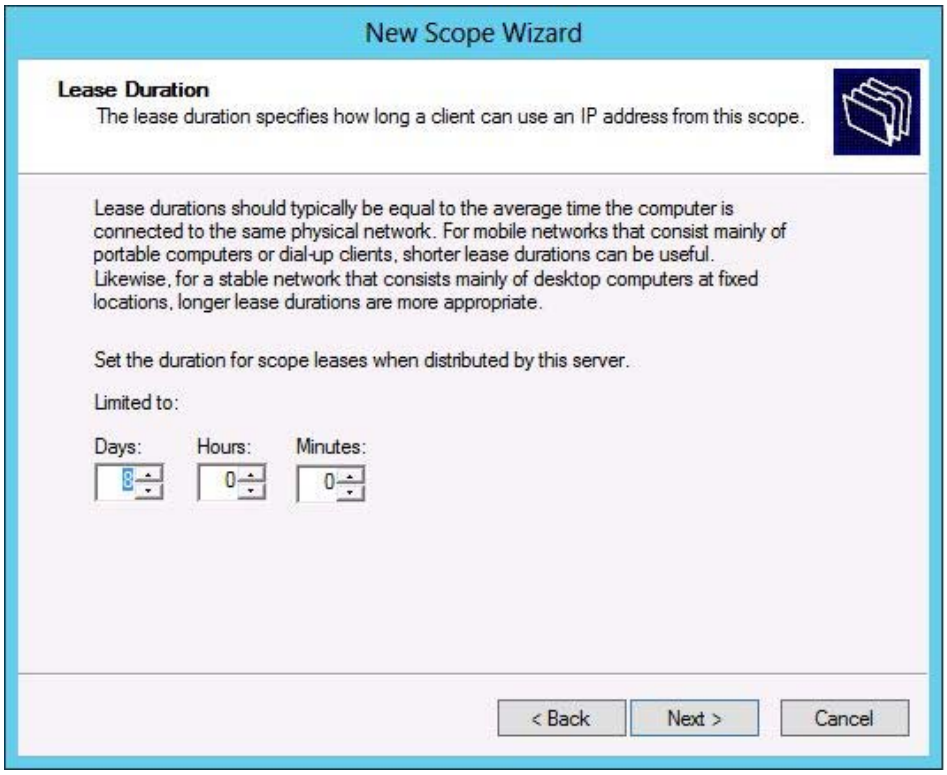
A DHCP szolgáltatás segítségével lehetővé válik a TCP/IP címek és beállítások dinamikus kiosztása. A munkaállomások számára kioszthető IP címeket határozunk meg, amelyeknek a bérleti ideje alapbeállításban 8 nap. A bérleti idő után a DHCP szerver új IP címet oszt a munkaállomásnak.

Szerverek esetén vagy statikus IP címet adunk meg, és nem használjuk a DHCP szolgáltatást, vagy pedig a DHCP szerver Reservations opcióját alkalmazzuk, amely azt jelenti, hogy az IP címet hozzákötjük a kiszolgáló MAC címéhez, ezáltal ez a cím már nem kerül kiosztásra, és a kiszolgálóhoz rendelődik.

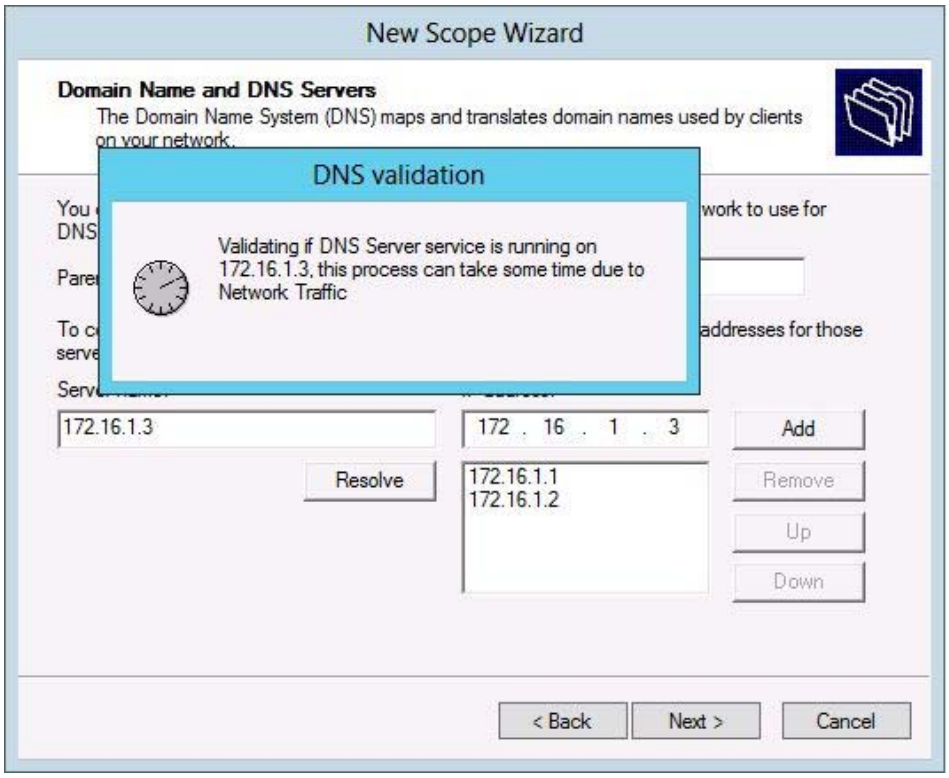
A DHCP konfigurációjához először egy DHCP Scope-ot kell felvennünk:



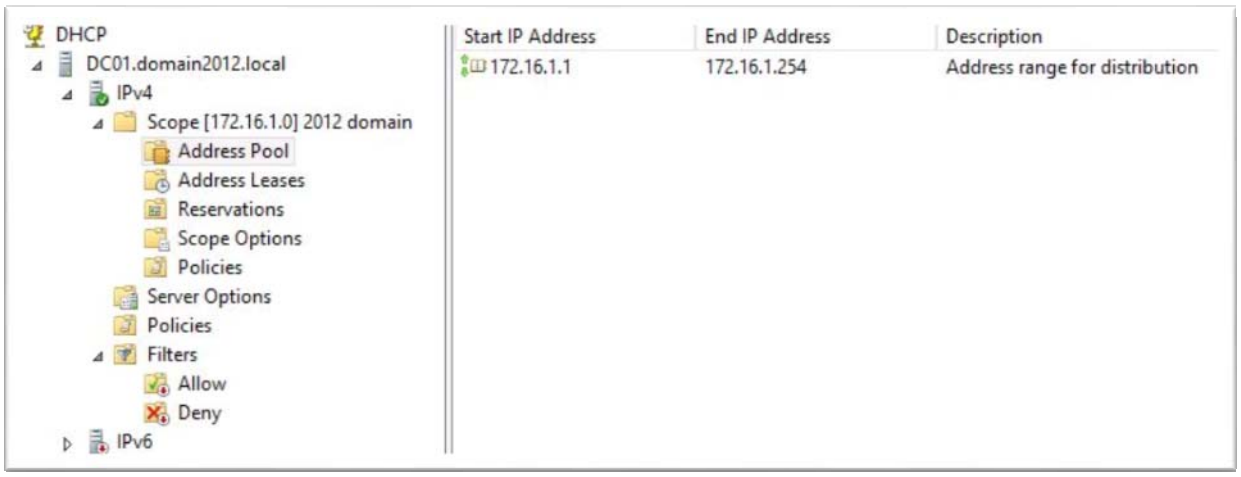
Majd beállítjuk a DHCP bérleti időt:



Mindezek után meg kell adnunk az alapértelmezett átjárót, majd a DNS kiszolgálókat:



Ha mindent megadtunk, akkor a Finish-re kattintva, ehhez hasonló képet kapunk:

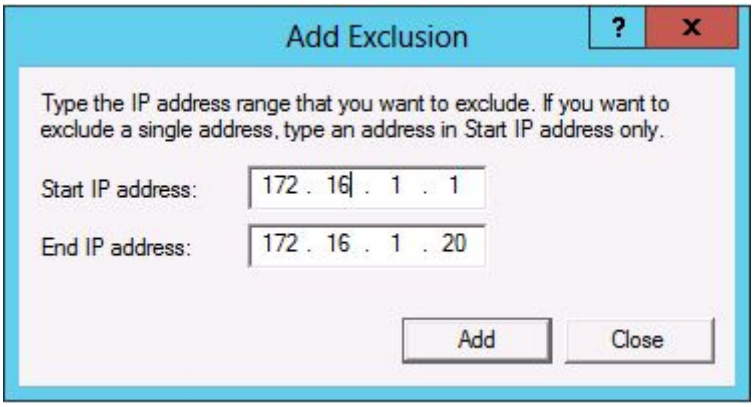


A Server Options-nél be kell állítanunk azokat az információkat, amelyeket ki szeretnénk küldeni a klienseknek, itt ajánlott megadni a következőket:

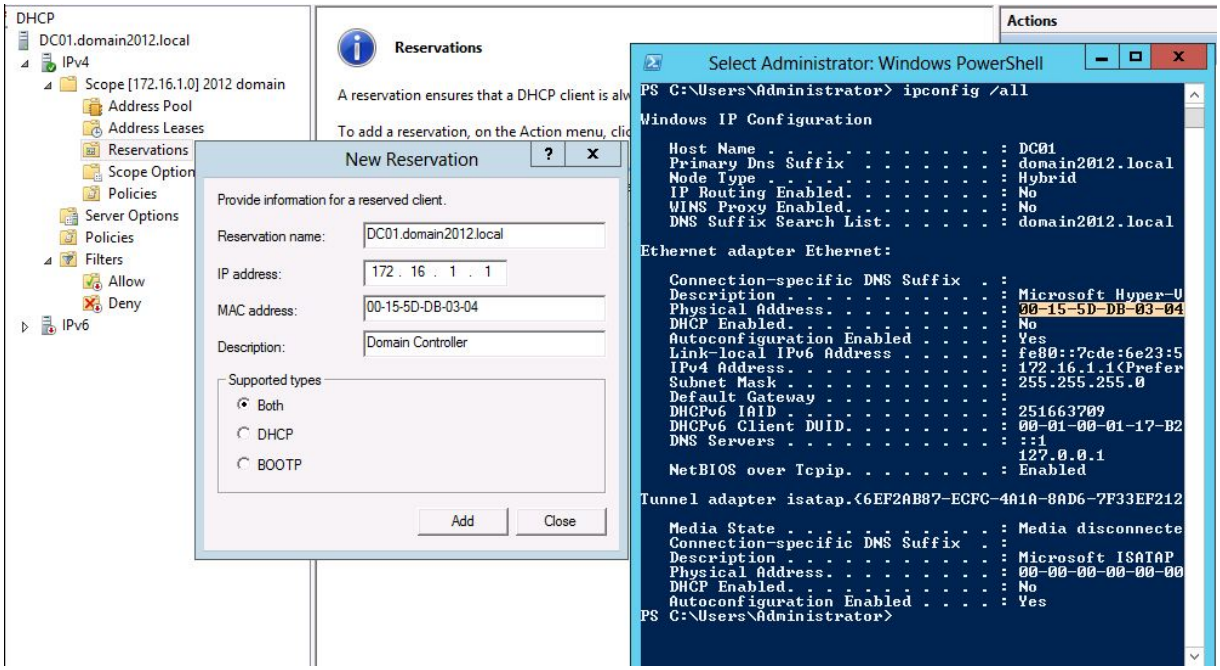
Option Name	Vendor	Value	Policy Name
006 DNS Servers	Standard	172.16.1.1, 172.16.1.2, 172.16.1.3	None
015 DNS Domain Name	Standard	domain2012.local	None

Ezeket a beállításokat a kliens ipconfig /all parancsával megtaláljuk.

Ha szeretnénk, hogy a DHCP osztaná a kiszolgálóknak is az IP címet, akkor lefoglalhatunk nekik egy intervallumot.



Mindezek után foglaljuk le az IP-jét a DC01-nek. A MAC címet könnyen megállapíthatjuk az ipconfig /all paranccsal.



A regisztráció után a kiszolgáló hálózati konfigurációjánál be kell állítanunk, hogy immár DHCP-vel kérdezze le az IP címét.

7.11 DHCP Failover

Az előző verziókban a DHCP rendelkezésre állásának javítását legtöbbször cluster technológiával vagy DHCP Split Scope-al oldottuk meg. A Windows Server új verziójában bemutatkozik a DHCP Failover.

A kliensek bizonyos időközönként a DHCP szerverhez fordulnak, hogy megújítsák IP címüket. A DHCP szolgáltatás kiesése esetén a kliensek nem kapnak új IP címet, ezáltal nem tudnak csatlakozni a hálózathoz. Ennek a problémának az áthidalására készült a DHCP Failover, amely két DHCP kiszolgálóból állhat. A DHCP kiszolgáló kiesése esetén a másik (partner) DHCP kiszolgáló veszi át az IP cím osztását. Az adatok frissességét a lease replikáció garantálja. A replikációs technológia időérzékeny, ezért a két DHCP szerver idejét a beállítás előtt egyeztessük, a technológia 1 percnél nagyobb eltérést már nem tud tolerálni. A DHCP Failover működhet tartományi tagság vagy munkacsoport tagság esetén is. Az IPv6-os címek magas rendelkezésre állását a DHCP Failover nem teszi lehetővé.

A DHCP Management felületén a DHCP IPv4 ágán érhetjük el a DHCP Failovert. Két lehetőségünk van a konfigurációra:

- Load Balancing
- Hot Standby

Load Balacing esetén mind a két szerver részt vesz az IP címek osztásában, még azt is be tudjuk állítani, hogy milyen arányban történjen ez meg. Alapbeállításban ez 50-50 % (active-active). Javasolt egy telephelyes kiépítettségben.

Hot Standby esetén az aktív DHCP szerver egyedül osztja az IP címeket, a passszív DHCP csak akkor lép működésbe, amikor az aktív kiszolgáló kiesik (active-passive). Javasolt több telephelyes kiépítettségben.

A létrehozott Failover konfiguráció után a Replicate Failover Scopes paranccsal máris tesztelhetjük a replikációt.

7.12 Print and Document Services

A nyomtatók kezelésére a Windows Server 2012-ben elérhető Print Management MMC konzol használható.

A konzol legfontosabb tulajdonságai:

- Több nyomtató szerver (spooler) kezelése
- Nyomtatók szűrt listázása egyedi szűrő feltételek segítségével
- Nyomtató driver kezelés
- Nyomtató port kezelés
- Jogosultság kezelés
- Mentés/visszaállítás

A nyomtatók telepítését, terítését a munkaállomásokra Group Policy-n keresztül is megoldhatjuk. A Deployed Printers menüpontban válasszuk ki a telepítendő nyomtatókat, majd nyomjunk a Deploy with Group Policy menüpontra. Itt már csak ki kell választanunk azt a GPO-t, amelybe a beállításokat be szeretnénk illeszteni.

A nyomtatók rendelkezésre állását a következőképpen oldhatjuk meg:

- A Printer Management-ben a Printer Servers alatt válasszuk az Export printers to a file… pontot, a konfigurációs fájlt másoljuk át egy másik tartományvezérlőre, ahol szintén telepítve van a nyomtatók támogatása.
- A tartományvezérlő kiesése esetén a másik tartományvezérlőn lévő Printer Management Console-ban Import Printers from a file menüpontot választva a nyomtatók települnek.
- A Group Policy beállítások módosítása szintén szükséges. A GPO *Computer Configuration/Policies/Windows Settings/Printer Connections/* alatt lévő printer elérési utakat módosítjuk:
  \\BackupDC\Nyomtató1
  \\BackupDC\Nyomtató2

Új nyomtató esetén fontos, hogy megfelelő minőségű és megbízhatóságú drivert használjunk, ehhez a következő sorrend a javasolt:

- Jóváhagyott és már telepített gyártó specifikus universal driver
- Windows operációs rendszerrel együtt érkező nyomtató specifikus driver
- WHQL aláírással rendelkező nyomtató specifikus driver a gyártó weboldaláról

Fontos, hogy a nyomtató 32 és 64 bites driverrel egyaránt rendelkezzen, és a két driver neve (Driver Name mező) pontosan megegyezzen.

Használjuk a Windows 2008 R2-ben már bevezetett driver isolation-t. Az új lehetőség a különböző drivereket egymástól elkülöníti, így egy hibás komponens nem befolyásolja a szerver működését.

A Drivers ágnál kapcsoljuk be az ún. *Isolated módot* az összes felvett printer esetében.

A Windows Server 2012 számos újítást hozott a nyomtatás területén, ennek egyik megtestesítője a Branch Office Direct Printing. Ezt a lehetőséget olyan esetben érdemes használni, amikor egy távoli telephelyen keresztül nyomtatunk az ugyanezen a telephelyen lévő nyomtatóra, de a nyomtatószerver a cég központjában van. A Branch Office Direct Printing előtt az adatok végigutaztak a drága és egyébként is erősen leterhelt WAN hálózatunkon majd onnan vissza a telephelyen lévő nyomtatóra. Ez a technológia ezt az adatutazást zárja ki a folyamatból, úgy, hogy a munkaállomások közvetlenül a nyomtatóra kapcsolódnak. Könnyen belátható, hogy esetleges hálózati kiesés a két telephely között, nem befolyásolja a nyomtatóhoz történő csatlakozásunkat. A Branch Office Direct Printing lehetőség csak a print serverként működő Windows Server 2012 és Windows 8 kliens esetén érhető el.

A Print and Document Services már konfigurálható PowerShell alól is, megkönnyítve ezzel az adminisztrációt. Ez tulajdonképpen 20 db parancsot jelent, a parancsok listáját megkapjuk a következő paranccsal:

```
Get-Command –Module PrintManagement
```

A Branch Office Direct Printer konfigurációját a Print and Document Services-ben is beállíthatjuk, de legegyszerűbb mindez PowerShell alól:

```
Set-Printer -name <String> -ComputerName <String> -RenderingMode
         BranchOffice
```

A Windows Server 2012-ben jelent meg a Print Class Driver framework. A keretrendszer tartalmazza az alapvető nyomtatási képességeket, ezért a gyártóknak csak a nyomtatók speciális képességeit kell az eszközvezérlőbe integrálniuk. Ennek folyománya, hogy a driverek mérete jelentősen csökken és az eszközvezérlőkből származó lehetséges hibák száma is redukálódik. A Windows Vista 768 MB-ja mellett eltörpül a Windows 8 mintegy 180 MB-nyi drivere.

7.13 Read-Only Domain Controller

A Read Only Domain Controller – mint neve is mutatja – csak olvasható tartományvezérlő; egy teljes értékű tartományvezérlő, viszont a rajta lévő adatok nem módosíthatók. Ezt a megoldást olyan helyre érdemes telepíteni, ahol az adataink biztonsága nem garantálható. Ilyen lehetőség például cégünk egyik kisebb telephelye, ahol szerverszoba sincs. Feltörés vagy eltulajdonítás esetén garantált, hogy a rajta lévő tartományi adatokhoz nem tudnak hozzáférni, hiszen tulajdonképpen nem tárol semmit. Ehhez használjunk fel egy Server Core-al telepített kiszolgálót, és erre telepítsünk az RODC-t.

Mielőtt hozzákezdenénk, ellenőrizzük, hogy az erdőnk funkcionalitási szintje legalább Windows 2003-mas.

A telepítést indítsuk el a következő paranccsal a Server Core-os gépen bejelentkezve:

```
dcpromo /unattend /InstallDns:yes /confirmGC:yes /replicaOrNewDomain:ReadOnlyReplica
          /replicaDomainDNSName:domain2012.local /databasePath:"c:\ntds"
          /logPath:"c:\ntdslogs" /sysvolpath:"c:\sysvol" /rebootOnCompletion:yes
```

Server Managerből egy távoli gépen indítva a telepítést PowerShellen keresztül:

Létre kell hozni egy RODC fiókot a következőképpen:

```
Add-ADDSReadOnlyDomainControllerAccount –DomainControllerAccountName RODC1
          –DomainName domain2012.local DelegatedAdministratoraccountName
          RO_Admin
```

Telepítsük az Active Directory Domain Services-t:

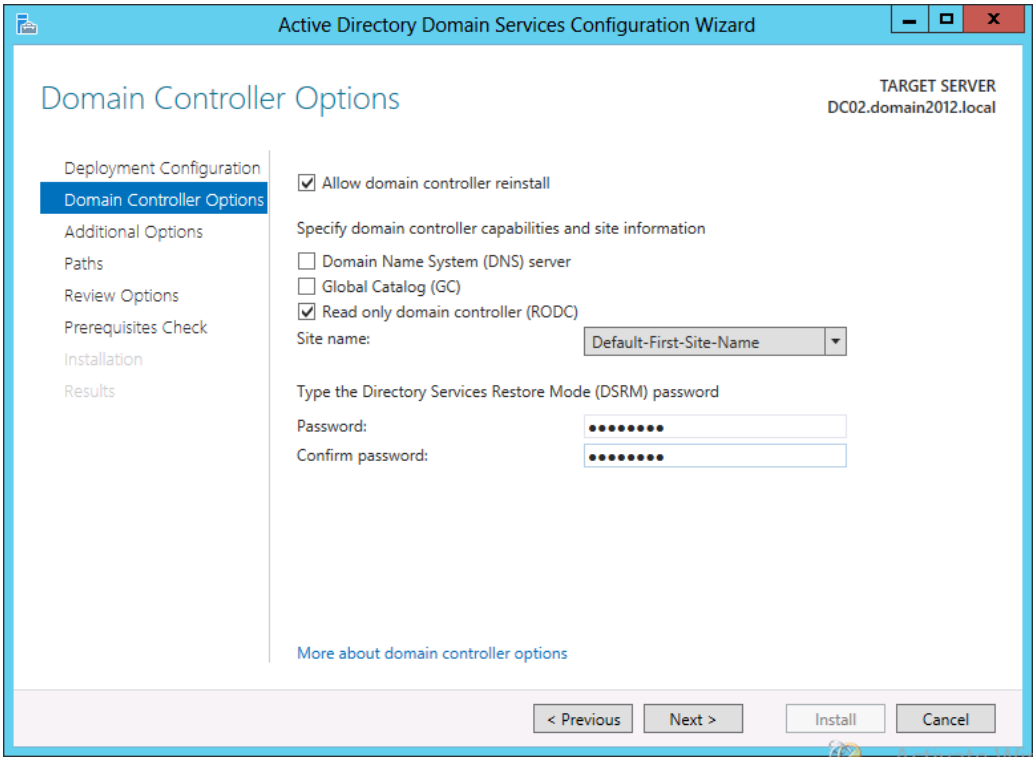
```
install-windowsfeature –name AD-Domain-Services -includemanagementtools
```

Majd a következő paranccsal hozzuk létre a RODC-t:

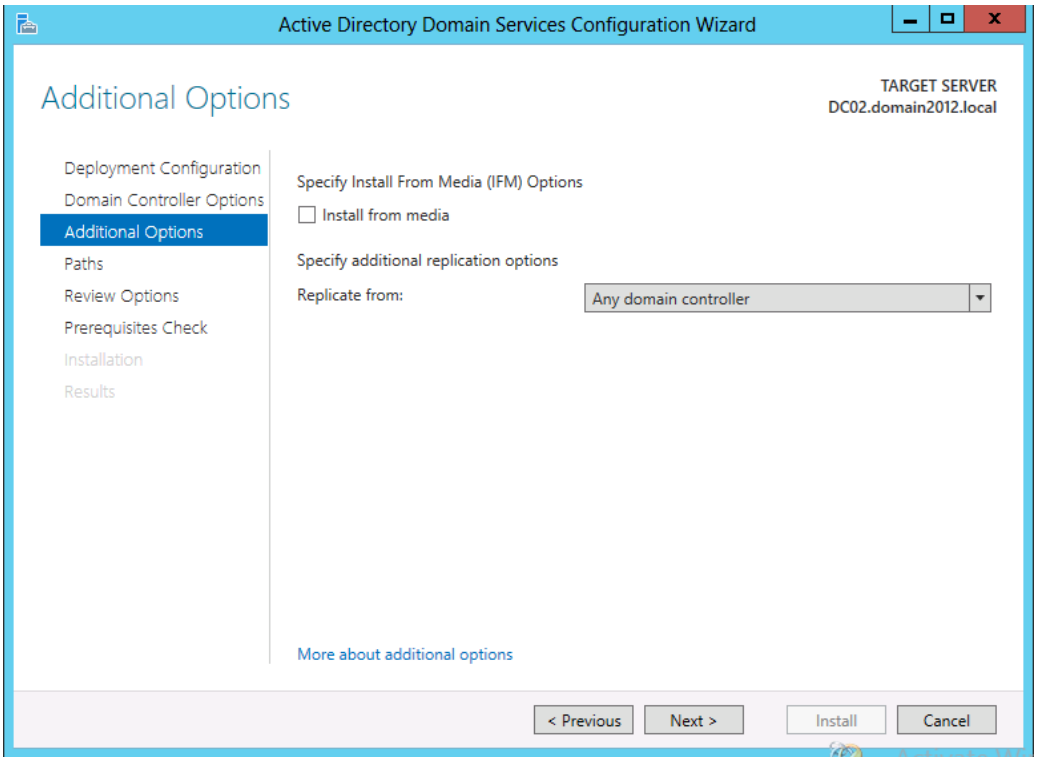
```
Install-ADDSDomainController –DomainName domain2012.local –
          SafeModeAdministratorPassword (read-host –prompt "DSRM Password:"
          –assecurestring) –credential (get-credential domain2012\RO_Admin)
          -useexistingaccount
```

A Server Managerből indítva a telepítést:

A Server Managerből alapvetően ugyanaz az út az RODC-hez, mintha írható tartományvezérlőt telepítenénk. Először fel kell telepítenünk az Active Directory binárisokat, majd a post installation során a következőket kell konfigurálni:



Ezt követően meg kell határoznunk, hogy melyik írható tartományvezérlővel replikálhat. Majd a topológia vizsgálata után telepíthetjük az új RODC-t.



7.14 Utómunkálatok

7.14.1 Időszinkron

A rendszeridő pontossága a teljes Active Directory-ra nézve kritikus fontosságú.

A tartományvezérlő a PDC Emulátor szerepköre felel az időszinkronizációért. A tartományba belépett gépek szintén a PDC emulátor FSMO szerepkörrel rendelkező géphez szinkronizálják a saját rendszeridejüket. A Kerberos hitelesítés megfelelő működéséhez elengedhetetlen a rendszeridő pontossága. Alapbeállítás szerint 5 percnél nagyobb rendszeridő eltérés már problémákat okozhat a rendszer működése szempontjából.

A PDC emulátor szerepkörrel rendelkező tartományvezérlőnek külső forrásból kell megoldanunk az időszinkronizációt, amelyhez a tűzfalunkon engedélyezni kell az udp 123-as porton a kommunikációt. Alapbeállítás szerint a tartományvezérlő a time.windows.com-hoz igazítja az idejét.

A PDC szerepkör – hacsak át nem helyeztük máshova – az első telepített tartományvezérlőn található. De megállapíthatjuk így is:

```
w32tm /monitor /domain:domain2012.local
```

Állítsunk be két megbízható forrást:

```
w32tm /config /computer:dc01.domain2012.local /update /manualpeerlist:
        ”time.kfki.hu 0.hu.pool.ntp.org” /reliable:yes
```

Indítsunk el egy azonnali szinkronizációt:

```
w32tm /resync
```

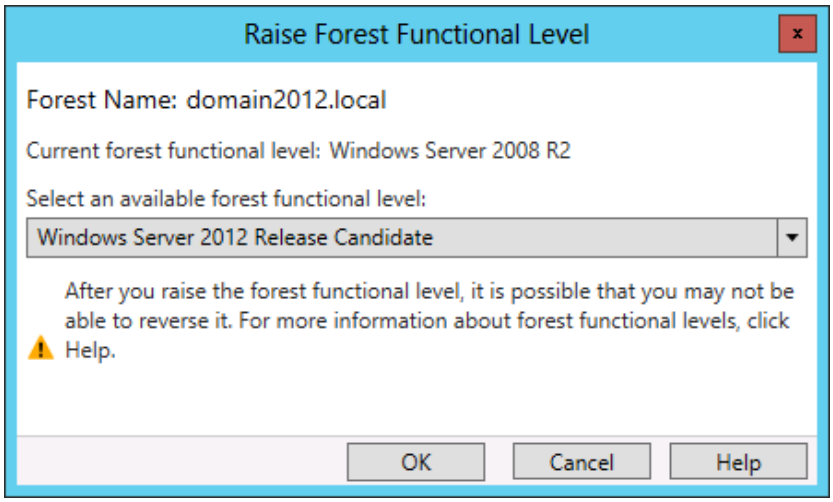
Majd kérdezzük le a státuszt:

```
w32tm /query /status
```

7.15 Funkcionalitási szintek

A Windows Server 2012-ben a funkcionalitási szintek növeléséhez lépjünk be az Active Directory Administrative Centerbe Enterprise Admins jogosultsággal rendelkező felhasználóval, majd kiválasztva bal oldalt a domain nevet, jobb oldali sávban megjelenik az erdő, illetve a tartomány funkcionalitásának növelése menüpont.

A funkcionalitási szint növelése csak abban az esetben lehetséges Windows Server 2012-re, ha az összes tartományvezérlőnk ezen az operációs rendszeren fut. Visszalépés a Windows 2008 R2 szintre csak abban az esetben lehetséges, ha nem kapcsoltuk be az AD Recycle Bin-t.



A növelés nem hoz semmiféle további lehetőségeket az Active Directory-ban az előző verziókkal ellentétben.

7.16 FSMO szerepkörök

Az első tartományvezérlő telepítésekor az összes FSMO szerepkör telepítésre kerül. Javasolt a szerepkörök több gépre történő szétosztása, főleg elérhetőségi és terhelés-megosztási szempontból.

Két lehetőségünk van a szerepkörök áthelyezésére:

- Egyszerű áthelyezés
- Erőszakos (seize) áthelyezés

Az egyszerű áthelyezésnél könnyű dolgunk van, mivel a szerepkört tartalmazó tartományvezérlő működik, azaz az áthelyezés minden probléma nélkül megtörténik.

Az erőszakos áthelyezést akkor használjuk, amikor a szerepkört vagy szerepköröket tartalmazó tartományvezérlő kiesik, és visszaállítását nem tervezzük. Ilyenkor csak ezzel a módszerrel tudjuk a szerepkört áttenni a még működő tartományvezérlőnkre.

Az öt egyedi főkiszolgáló-művelet (Flexibile Single Master Operations, FSMO) a következő:

- RID-főkiszolgáló (RID Master): Tartományszintű műveleti főkiszolgáló szerepkör, vagyis minden tartományban legfeljebb egy lehet belőle. A szerepkörrel ellátott tartományvezérlő saját, vagy valamelyik másik tartományvezérlő kérésére egy létrehozandó új objektum (felhasználói fiók, csoport stb.) számára kiad egy relatív azonosító (Relative Identifier, RID) részt a leendő objektum biztonsági azonosítójához. A biztonsági azonosító neve SID (= Security Identifier). A RID Mastertől a tartományvezérlők 200-as csomagokban (RID Pool) kapják a relatív azonosítókat, amivel azután önállóan gazdálkodnak. Az ütközések elkerülése érdekében a sorszámokat egy központ bocsátja ki. A relatív azonosító rész egyértelműen azonosítja az objektumot a tartományon belül. Ha nem érhető el a RID-főkiszolgáló, csak addig lehet a tartományban új objektumokat létrehozni, amíg a korábban kiosztott RID Poolok el nem fogynak (max. 200).
- PDC-emulátor (PDC Emulator): Tartományszintű műveleti főkiszolgáló szerepkör, minden tartományban csak egy lehet belőle. A Windows 2000 előtti ügyfelek számára elsődleges Windows NT tartományvezérlőként (Primary Domain Controller, PDC) működik, vagyis feldolgozza az ügyfelek bejelentkezéseit, jelszóváltozásait, és replikálja a változásokat a többi tartományvezérlő felé. Feladatai közé tartozik még a tartomány összes tartományvezérlője által mutatott idő automatikus szinkronizálása a Windows Time szolgáltatás segítségével.
- Infrastruktúra-főkiszolgáló (Infrastructure Master)**:** Szintén tartományszintű műveleti főkiszolgáló szerepkör, amelyből szintén egy lehet a tartományon belül, de csak akkor van rá szükség, ha a hálózat több tartományból áll. Feladata a saját tartományának objektumai és a többi tartományban található objektumok közötti hivatkozások frissítése. Ha nem érhető el, a tartományon belül nem veszünk észre változást, azonban a többi tartománnyal való kapcsolattartás során frissítési problémák keletkeznek.
- Tartománynév-nyilvántartási főkiszolgáló (Domain Naming Master)**:** Erdőszintű műveleti-főkiszolgáló szerepkör, amelyből az erdőben kizárólag egy lehet. A speciális szereppel bíró tartományvezérlő szabályozza az erdőben a tartományok hozzáadását és törlését. A tartományfákkal kapcsolatos változtatások nem hajtódnak végre, ha a szerepet megvalósító tartományvezérlő nem érhető el.
- Séma-főkiszolgáló (Schema Master)**:** Erdőszintű műveleti-főkiszolgáló szerepkör, központosítva végzi el a séma összes frissítését és módosítását. Amennyiben az erdő sémáját frissíteni kívánjuk, hozzáférési joggal kell rendelkeznünk a séma-főkiszolgálóhoz. Az előző szerephez hasonlóan séma-főkiszolgálóból is csak egy lehet az erdőben, és szintén nem vesszük észre a hiányát, egészen addig, amíg nem kerül sor a séma frissítésére vagy bővítésére.

FSMO szerepkörök átvitele:

- Kattintsunk a Start menü Futtatás parancsára, írjuk be az ntdsutil parancsot a Megnyitás mezőbe.
- Írjuk be a roles parancsot.
- Írjuk be a connections parancsot.
- Majd a connect to server *kiszolgálónév* parancsot, a *kiszolgálónév* helyére annak a tartományvezérlőnek a nevét írjuk, amelyhez az FSMO-szerepkört rendelni szeretnénk.
- Írjuk be a server connections parancssorba a q parancsot.
- Írjuk be a transfer *szerepkör* parancsot. A *szerepkör* helyére az átadni kívánt szerepkör neve kerül. Az átadni kívánt szerepkörök listájának megjelenítéséhez írjuk be a ? pa-

rancsot az fsmo maintenance parancssorba. A szerepkörök kezelésekor azok angol elnevezését használhatjuk: a RID-főkiszolgálói szerepkör átadásához például írjuk be a transfer rid master parancsot. Az egyetlen kivételt a PDC-emulátor szerepkör jelenti, melynek szintaxisa transfer pdc, nem pedig transfer pdc emulator.
- Az fsmo maintenance parancssorban írjuk be a q parancsot, az ntdsutil parancssor eléréséhez. Írjuk be a q parancsot az Ntdsutil segédprogram bezárásához.

Erőszakos áthelyezés:

- Kattintunk a Start menü Futtatás parancsára, írjuk be az ntdsutil parancsot a Megnyitás mezőbe.
- Írjuk be a roles parancsot.
- Írjuk be a connections parancsot.
- Írjuk be a connect to server *kiszolgálónév* parancsot, a *kiszolgálónév* helyére annak a tartományvezérlőnek a nevét írja, melyhez az FSMO-szerepkört rendelni szeretnénk.
- Írjuk be a server connections parancssorba a q parancsot, Írja be a seize *szerepkör* parancsot. A *szerepkör* helyére a zárolni kívánt szerepkör neve kerül. A zárolni kívánt szerepkörök listájának megjelenítéséhez írjuk be a ? parancsot az fsmo maintenance parancssorba. A szerepkörök kezelésekor azok angol elnevezését használhatjuk: a RID-főkiszolgálói szerepkör zárolásához például írjukbe a seize rid master parancsot. Az egyetlen kivételt a PDC-emulátor szerepkör jelenti, melynek szintaxisa seize pdc, nem pedig seize pdc emulator.
- Az fsmo maintenance parancssorban írjuk be a q parancsot az ntdsutil parancssor eléréséhez. Írjuk be a q parancsot, az Ntdsutil segédprogram bezárásához.

7.17 Active Directory struktúra és építőelemei

Az Active Directory-ban történő nyilvántartás objektumokban tárolódik. Objektumok a felhasználók, csoportok, számítógépek, szervezeti egységek és a megosztott erőforrások (pl. nyomtatók). Ezeknek az objektumoknak vannak attribútumai, ami természetesen az objektum típusától függ. Egy felhasználói fiók attribútumainak felel meg a bejelentkezési neve, jelszava, e-mail címe, csoporttagsága. Mindezt könnyen megfigyelhetjük az ADSIedit segítségével. A címtár objektumait és hozzájuk kapcsolódó attribútumokat a séma írja le. Az Active Directory Users and Computers-t megnyitva láthatjuk az AD struktúráját, amelyben vannak már meglévő tárolók (container) és benne objektumok. A rendszergazda felvehet további tárolókat is, ezeket Organizational Unitnak, nevezünk. Egy OU-ban számtalan egymásba ágyazott OU-t létrehozhatunk, de könnyebb áttekinthetőség kedvéért törekedjünk a minél laposabb struktúra kialakítására. Az OU-kban felhasználókat, számítógépeket és egyéb objektumokat tárolhatunk és ezeket az objektumokat szabadon mozgathatjuk, költöztethetjük.

A beépített tárolók a Domain Controllers, amelybe kerül minden létező illetve később létrejövő tartományvezérlő számítógép objektuma. A Builtin tartalmazza a már létrejött csoportokat, Computers az Active Directory-ba beléptetett (tartománytag) számítógépeket tárolja, a Users, a tartományi felhasználókat tartalmazza. Az említett tárolókra nem alkalmazhatunk csoportházirendet (Group Policy), az Organizational Unitokra ellenben igen. A csoportházirendekkel központilag szabályozhatjuk a felhasználók számítógépes környezetét, beállításait. Számos beállítást eszközölhetünk, kezdve a felhasználók asztalának megjelenésével, a biztonsági beállításokon keresztül az automatikus alkalmazástelepítésig. A csoportházirend ennek a könyvnek egy külön fejezetét képezi.

Az címtárban kétféle csoportot állíthatunk be: biztonsági csoport (security group) és terjesztési csoport (distribution group). A biztonsági csoportok tagjai kapnak hozzáférési engedélyeket (pl. egy fájlmegosztáshoz) a terjesztési csoportokat elsősorban levelezési csoportoknak használjuk. A két csoporttípust kölcsönösen konvertálhatjuk, azaz a már meglévő terjesztési csoportból létrehozhatunk biztonsági csoportot és fordítva.

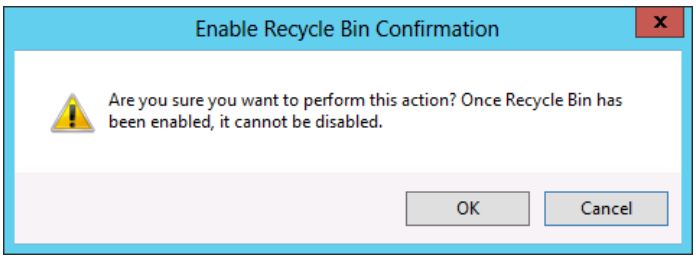
A csoportok hatóköre (scope) határozza meg a csoport tartományi tagságát, mely tartományokban lehet eleme más csoportoknak, mely tartományban kaphat hozzáférési engedélyeket.

- Tartományon belüli csoportok (Domain local groups): Mint neve is mutatja, az ilyen csoportok csak saját tartományuk számítógépein kaphatnak hozzáférési engedélyeket. A tartományi csoportokba viszont szabadon vehetünk fel globális és univerzális csoportokat más tartományokból illetve további tartományi csoportot is felvehetünk, azaz ezek a csoportok szabadon egymásba ágyazhatók. Mindez csak a tartomány natív üzemmódjában használható.
- Globális csoportok (Global groups): Az erdőn belül bármelyik tartományban felhasználhatók. A globális csoportok viszont csak saját tartományukból tartalmazhatnak tagokat. Globális csoportba csak egy másik globális csoportot vehetünk fel. Mindez csak akkor, ha natív üzemmódban működik a tartományunk.
- Univerzális csoportok (Universal groups): A csoport tagjai bármelyik tartományunkból származhatnak. Globális és további univerzális csoportok lehetnek a tagjai, szintén bármelyik tartományunkból. Tetszőleges tartományban kaphatnak hozzáférési engedélyeket. Az univerzális csoportok összes adata a globális katalógusban tárolódik.

7.18 Active Directory Lomtár

Az Active Directory Recycle Bin már Windows Server 2008 R2-nél is jelen volt, viszont grafikus megvalósítása a Windows Server új verziójában történt meg.

A bekapcsolásához navigáljunk a Server Manageren keresztül az Active Directory Administrative Centerbe, ott kattintsunk a tartományunk nevére, és a jobb oldali tasknál megtaláljuk a Enable Recycle Bin lehetőséget. Ennek bekapcsolásához legalább Windows Server 2008 R2 erdő és tartomány funkcionalitási szinten kell lennünk.

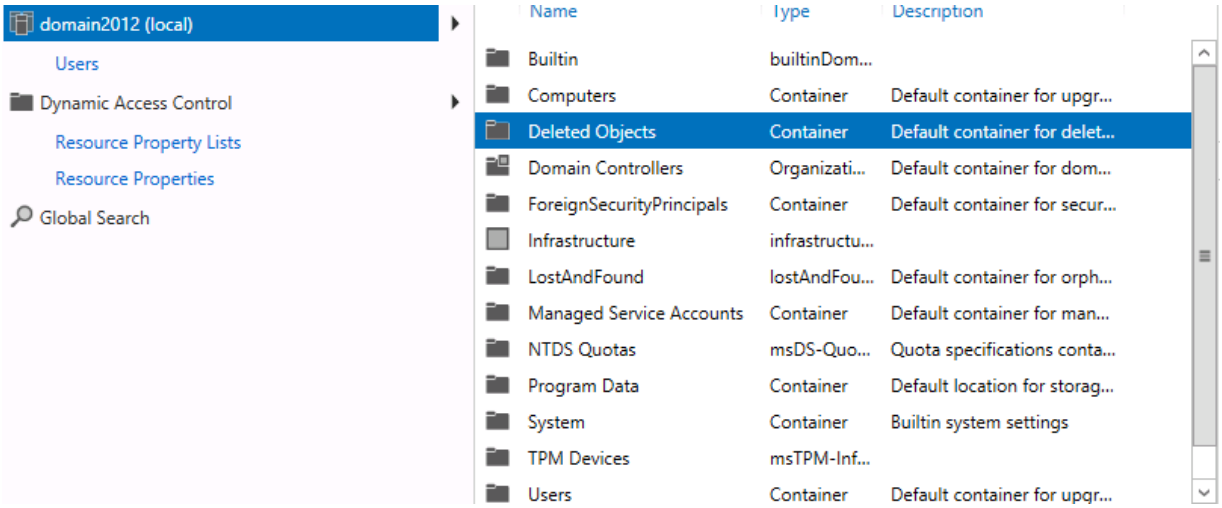


A bekapcsolást elvégezhetjük PowerShell alól is:

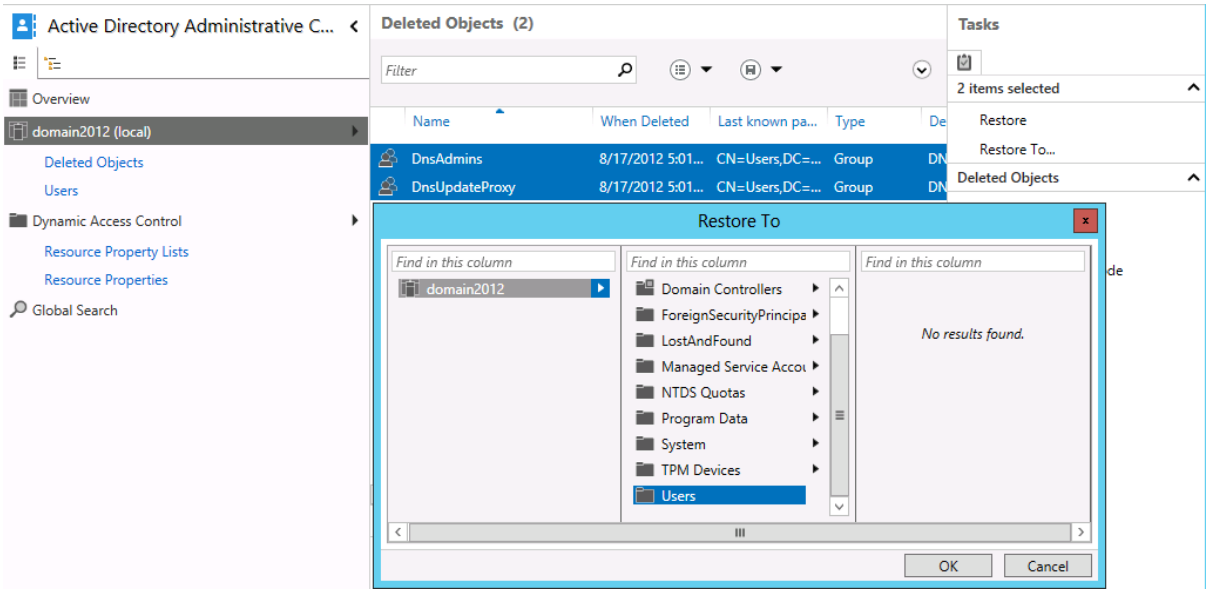
```
Enable-ADOptionalFeature –Identity ‘CN=Recycle Bin Feature,CN=Optional
        Features,CN=Directory Service,CN=Windows
        NT,CN=Services,CN=Configuration,DC=domain2012,DC=local’ –Scope
        ForestOrConfigurationSet –Target ‘domain2012.local’
```

Használata:

Amint bekapcsoltuk megjelenik a tartományunkban egy Deleted Object konténer.



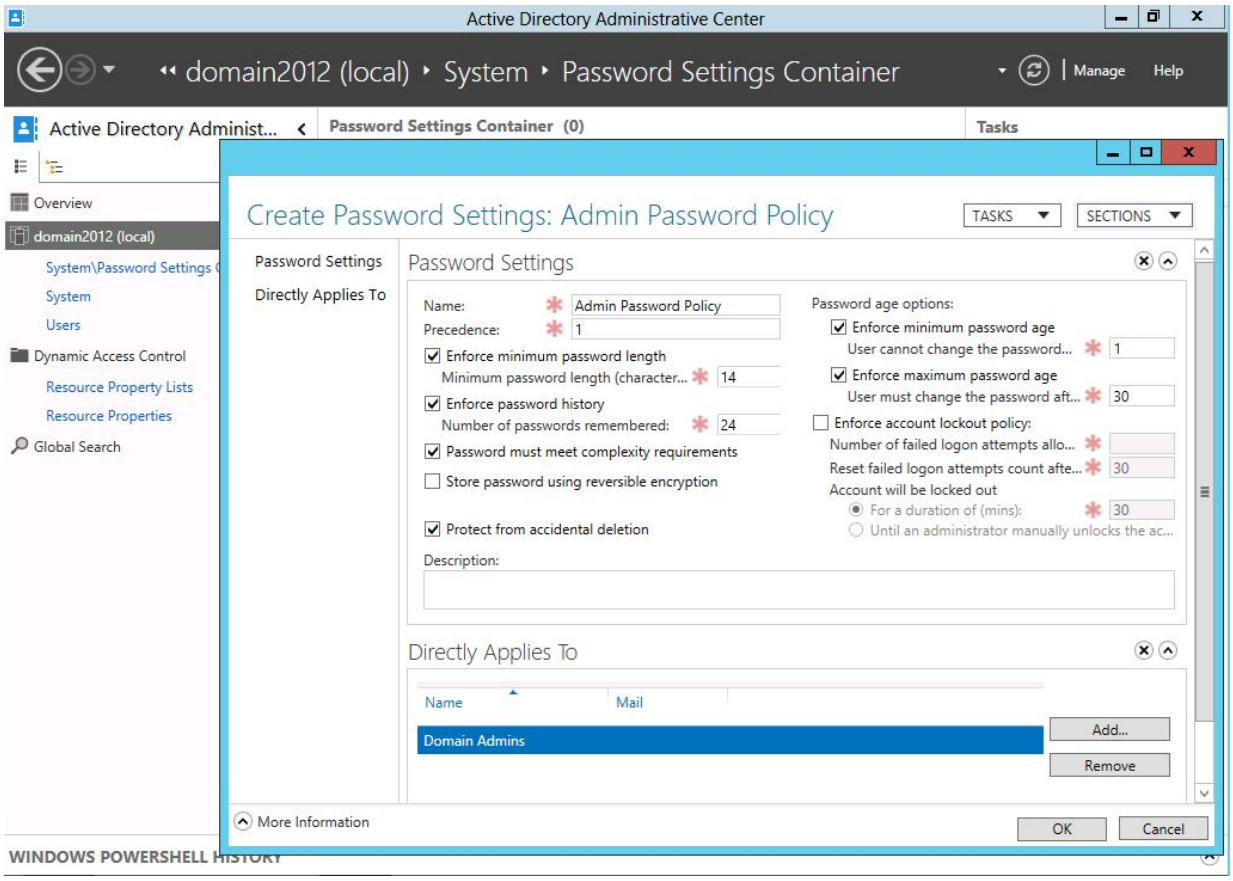
A kitörölt felhasználók automatikusan ebbe a konténerbe kerülnek és innen vissza is állíthatóak:



7.19 Jelszó menedzsment

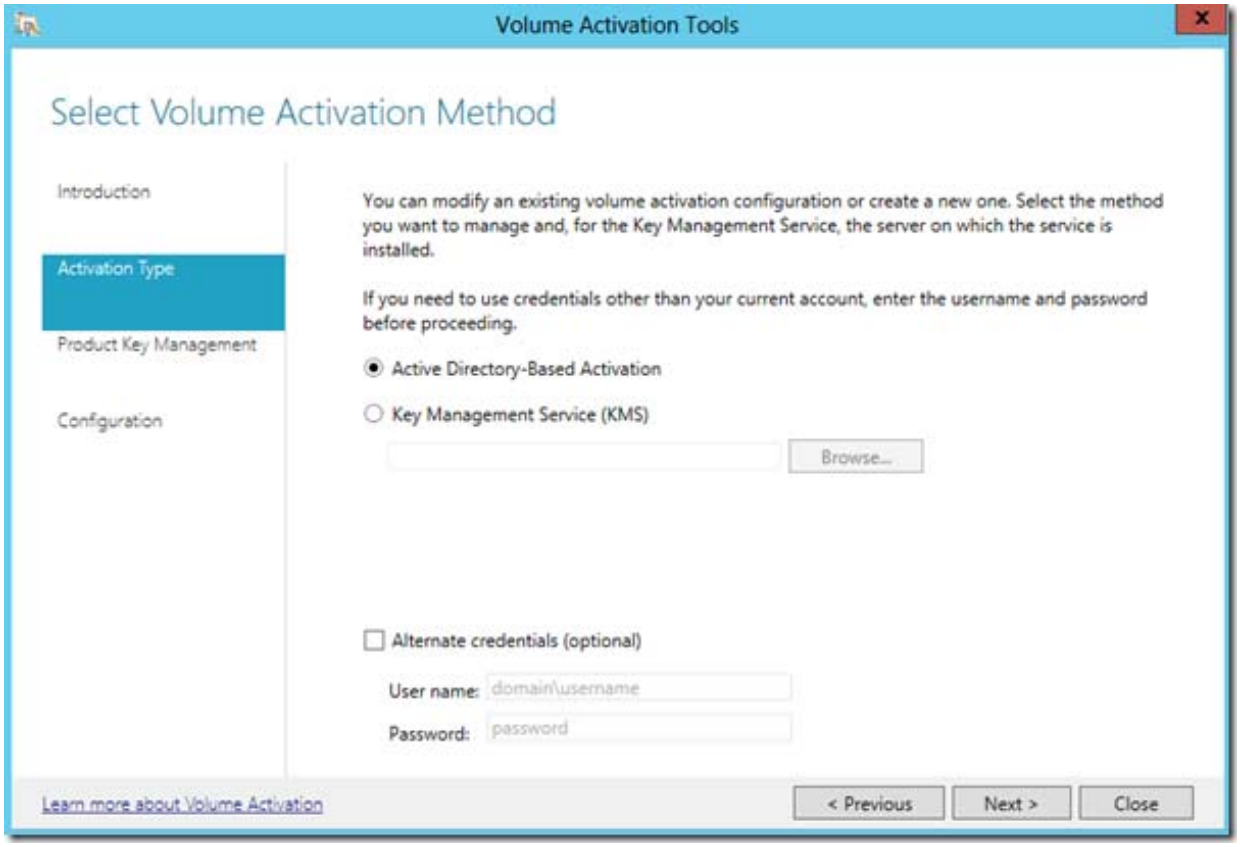
Már a Windows Server 2008-ban is meglévő jelszókezelés (Fine-Grained Passwords) jelentős mértékben egyszerűsödött. Adsiedit helyett immár megtalálható az Active Directory Administrative Center-ben. Itt különböző jelszó házirendeket hozunk létre, és azokat megfelelő csoportokhoz csatolhatjuk. Ennek jelentősége az, hogy például az adminisztrátoroktól sokkal „erősebb” jelszóhasználatot követelünk meg (több karakteres komplex jelszó, gyakori csere), mint pl. a felhasználóktól.

Elérhetősége az ADAC → Tartománynév → System → Password Settings Container. Itt kattintsunk a New Password Settings lehetőségre.



7.20 AD Based Activation

Az Active Directory központú aktiváció szintén egy új képesség a Windows Server 2012-ben. Gyakorlatilag a kissé korosodó KMS architektúrát válthatjuk le vele. Viszont a két eszközt párhuzamosan is használhatjuk, főleg abban az esetben, ha Windows Server 2012 és Windows 8-on kívül korábbi Windows operációs rendszerekkel is rendelkezünk. Mennyiségi licenc esetén AD alapú aktiválást nyújt. Az aktiválás akkor történik meg, amikor a számítógép a tartomány tagjává válik. A használatához a tartományi sémánkat módosítanunk kell a Windows Server 2012-re, de nem szükséges Windows Server 2012 DC-t telepítenünk, sőt Read-only Domain Controllereknél is használhatjuk. Az új eszközt, mint új szerepkört kell telepítenünk.


Volume Activation Tools
Select Volume Activation Method
Introduction
Activation Type
Product Key Management
Configuration
You can modify an existing volume activation configuration or create a new one. Select the method you want to manage and, for the Key Management Service, the server on which the service is installed.
If you need to use credentials other than your current account, enter the username and password before proceeding.
Active Directory-Based Activation
Key Management Service (KMS)
Browse...
Alternate credentials (optional)
User name:
domain\username
Password:
password
Learn more about Volume Activation
< Previous
Next >
Close

8 Virtualizáció

A Windows Server 2012-őt sokan úgy emlegetik, mint a felhő operációs rendszer, és nem véletlenül. A virtualizáció területén is rengeteg fontos fejlesztés történt az előző verzióhoz képest. Ebben a fejezetben az alapoktól mutatjuk be a Microsoft virtualizációs technológiáját, megismerkedünk a virtuális hálózat-kezeléssel, az új VHDX formátummal, és a rengeteg biztonsági újítással.

8.1 Alapok

Amikor virtualizációról beszélünk, nem csak a Hyper-V alapú számítógép virtualizációra kell gondolni. A Microsoft palettáján van néhány egyéb, más területeken működő virtualizációs témakör, ezek a következők:

- Számítógép virtualizáció
- Microsoft Azure
- Desktop virtualizáció
- Megjelenés-virtualizáció

Nézzük végig, melyik témakörben milyen szolgáltatásokat használunk:

8.2 Számítógép virtualizáció

A Hyper-V környezetben komplett számítógépeket virtualizálunk, akár kiszolgáló, akár kliens gépeknél is használhatjuk. Számos előnye közül a legelső, hogy egy fizikai gépen több virtuális gépet futtathatunk. Ezek a virtuális gépek teljes értékű számítógépek, bármilyen operációs rendszert telepíthetünk rájuk. A virtuális gépeket hívjuk vendég operációs rendszernek, a Hyper-V-t futtató fizikai gépet pedig hosztnak.

A számítógép virtualizációval optimálisabb hardver-kihasználást érhetünk el, mivel a mai hardverek általában nagyobb teljesítményre képesek, mint amit a rajtuk futó operációs rendszer és kiszolgáló alkalmazások igényelnek. A Hyper-V használatával tehát konszolidálni tudjuk a szerverparkunkat, és maximalizálhatjuk a gépeink kihasználtságát. A konszolidáció viszont komoly tervezést igényel: nem mindegy, milyen szolgáltatásokat, terheléseket rakunk ugyanarra a fizikai gépre.

A rendszer másik nagy előnye, hogy különböző kiszolgálói szerepköröket, amiket egyébként nem rakhatunk ugyanarra az operációs rendszerre, képesek vagyunk mégis egy fizikai gépen futtatni, például tartományvezérlő mellé nem javasolt Exchange vagy SQL kiszolgálót telepíteni, virtuális környezetben viszont ezek a terhelések mehetnek különböző virtuális gépekre.

Virtuális környezetben sokkal könnyebb új kiszolgálót üzembe helyezni: a System Center 2012 Virtual Machine Managerrel létrehozhatunk előre felkonfigurált kiszolgáló sablonokat, amiket percek alatt életre tudunk hívni.

8.3 Windows Azure

A Microsoft felhő-szolgáltatása, ami a teljes IaaS, PaaS, SaaS termékpalettát lefedi. Vásárolhatunk virtuális gépeket, SQL tárterületet, webtárhelyet, tárterületet, vagy akár médiaszolgáltatásokat is. A szolgáltatás havidíjas előfizetésben működik, így rugalmasan, menet közben változtathatjuk gépparkunkat, az igényeknek megfelelően bármikor növelhetjük vagy csökkenthetjük a virtuális gépeink számát. A Windows Azure elérhető a http://www.windowsazure.com/en-us/ címen, ahol lehetőségünk van 90 napig ingyenesen kipróbálni a különböző szolgáltatásait.

8.4 Desktop virtualizáció

Bizonyos esetekben szükség van arra, hogy a kliens gépünk is tudjon virtualizálni: ha a gépen szeretnénk futtatni egy régebbi operációs rendszert kompatibilitási problémák miatt, vagy tesztelni szeretnénk különböző kliens vagy akár szerver funkciókat. A Windows 8 Pro és Enterprise verziójában megtalálható a Hyper-V szerepkör, szinte azonos funkcionalitással, mint a Windows Server 2012-ben: a kliens verzió nem támogatja a magas rendelkezésre állást, illetve a migrációs szolgáltatásokat.

A Windows 7-ben bevezetett Windows XP mód már nem található meg a Windows 8-ban, így nincs lehetőségünk arra, hogy a virtuális gép programjait publikáljuk a host gép start menüjébe. Erre a feladatra nagyvállalati környezetben a MED-V (Microsoft Enterpise Deskotop Virtualization) rendszert ajánlja a Microsoft, ahol lehetőségünk van a szervereken futó kliens virtuális gépek (XP-től felfelé) telepített programjait publikálni az éles kliensgépekre.

8.4.1 VDI

A Virtual Desktop Infratructure környezetben a komplett kliensgép állományunkat futtatjuk Hyper-V alatt, a felhasználók pedig távoli asztallal csatlakoznak a gépeikhez, gyakorlatilag bárhonnan. A VDI egy összetett infrastruktúra, kihasználja a virtualizáció és a távoli asztal szolgáltatások különböző képességeit, a bevezetése viszont nagyon leegyszerűsödött a Windows Server 2012-ben: a Server Manager szerepkörök hozzáadásakor, mint egy szcenáriót tudjuk kiválasztani, megadhatjuk, mennyi virtuális gépre van szükségünk, és a telepítő felkonfigurálja az összes szükséges szerepkört.

A VDI előnye, hogy a kliens gépek mentése csak a Hyper-V hosztok mentését jelenti, a magas rendelkezésre állás könnyen megoldható, és egy kliens gép meghibásodásakor nincs adatvesztés, illetve szolgáltatás-kiesés sem. A VDI további előnye, hogy a cégnél bevezethetjük a „Bring your Own Device” elvet, vagyis a dolgozók akár a saját notebookjukról, táblagépükről is dolgozhatnak, hiszen bizalmas információ nem kerül a kliens gépekre. A VDI-jal részletesebben egy külön fejezetben foglalkozunk.

8.5 Megjelenítés virtualizáció

A megjelenítés virtualizáció főleg a távoli asztal szolgáltatásokat rejti magában, ahol egy központi RDP kiszolgálóra jelentkeznek be a felhasználók, a programok ezen a központi gépen futnak, és csak a megjelenítés történik a kliens gépeken. Ez annyiban különbözik a VDI-tól, hogy nem mindenki a saját virtuális gépét használja, hanem egy központi gépre egyszerre többen jelentkeznek be, és ugyanazokat az alkalmazásokat futtatják külön munkafolyamatban.

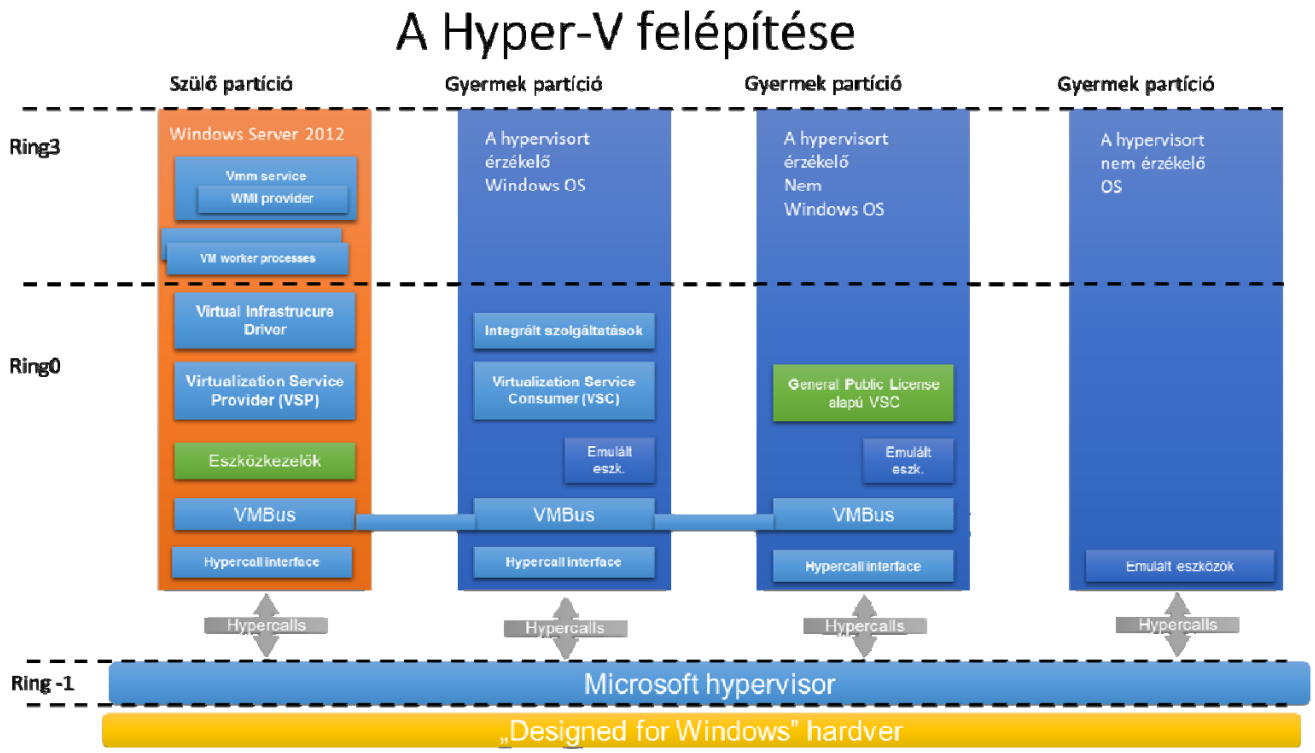
Ebben a környezetben általában nem beszélünk virtualizációról. A rendszer több kiegészítő szolgáltatással, és néhány korlátozással is rendelkezik:

- Távoli asztal környezetben használhatunk RemoteApp programokat, így a felhasználók a saját start menüből érhetik el a távoli asztal alkalmazásokat
- A RemoteApp alkalmazásokat akár weboldalra is publikálhatjuk RDWeb-en keresztül
- A távoli asztal kiszolgálókat Internetről is biztonságosan érhetjük el a Remote Desktop Gateway alagúton keresztül
- A rendszer korlátozása, hogy az RDP kiszolgálókon a felhasználók nem kaphatnak rendszergazdai jogosultságot, és néhány alkalmazás nincs felkészítve arra, hogy ugyanazon a gépen, egyszerre több példányban fusson.

9 Hyper-V

A Hyper-V hardveres virtualizációt tesz lehetővé a megfelelő hardver használatával. A szerepkör megtalálható a Windows Server 2012 grafikus és Core verziójában, és az ingyenes Hyper-V Server 2012-ben.

A hardveres virtualizáció a hypervisor segítségével hozzáférést ad a virtuális gépeknek a fizikai erőforrásokhoz, mint a processzor, a memória, stb., így sokkal gyorsabb működést tudunk elérni pl. a Virtual PC és Virtual Server termékekhez képest, ahol szoftveres virtualizációt használtunk, vagyis a virtuális gépek a hoszt gépen keresztül, nem pedig vele azonos szinten érték el a hardvert.



A Hyper-V szerepkört felügyelhetjük a Hyper-V Manager konzolból, PowerShellből, illetve távoli gépen futó Hyper-V Manager-ből is. Ez utóbbi főleg Hyper-V server és Server Core használatakor lehet előnyös.

9.1.1 Hardver feltételek

Virtualizációs hardver kiválasztásánál a következő feltételekre érdemes figyelni:

- A Hyper-V használatához 64 bites processzorra van szükségünk, ami támogatja a Data Execution Prevention-t és a SLAT-ot. A processzorok lehetnek Intel VT vagy AMD-V technológiát támogató CPU-k, de arra érdemes odafigyelni, hogy a két CPU gyártó processzorai nem működnek együtt Hyper-V clusterben, sem Hyper-V replikációnál, tehát ha lehetőségünk van, azonos gyártó processzorait használjuk.

- A fizikai gép tervezésekor vegyük figyelembe, milyen terhelésű virtuális gépeket szeretnénk elhelyezni rajta. A virtuális gépek maximum 1 TB memóriát használhatnak, és max. 32 virtuális CPU-t tudunk kiosztani számukra.
- A fizikai gép minimális memória-igénye 4GB.
- A lemezek elérése általában a sarkalatos pontja a virtualizációnak. A különböző virtuális gépeket érdemes külön fizikai diszkekre elhelyezni, vagy ha storage-ot használunk, akkor külön LUN-okra. A virtuális lemezeket mindenképpen érdemes magas rendelkezésre állású (RAID1 vagy RAID5) lemezeken tárolni, illetve használhatunk SSD-tömböt is.
- A hálózatnál több lehetőségünk van: akár dedikálhatunk külön fizikai NIC-et mindegyik virtuális géphez, akár használhatunk egy fizikai NIC-et megosztva több virtuális gép között, ha nincs szükségünk nagy hálózati sebességre, vagy konfigurálhatunk NIC Teaminget a hoszt vagy akár a virtuális gépen belül is, így összefűzhetünk több fizikai hálózati kártyát.

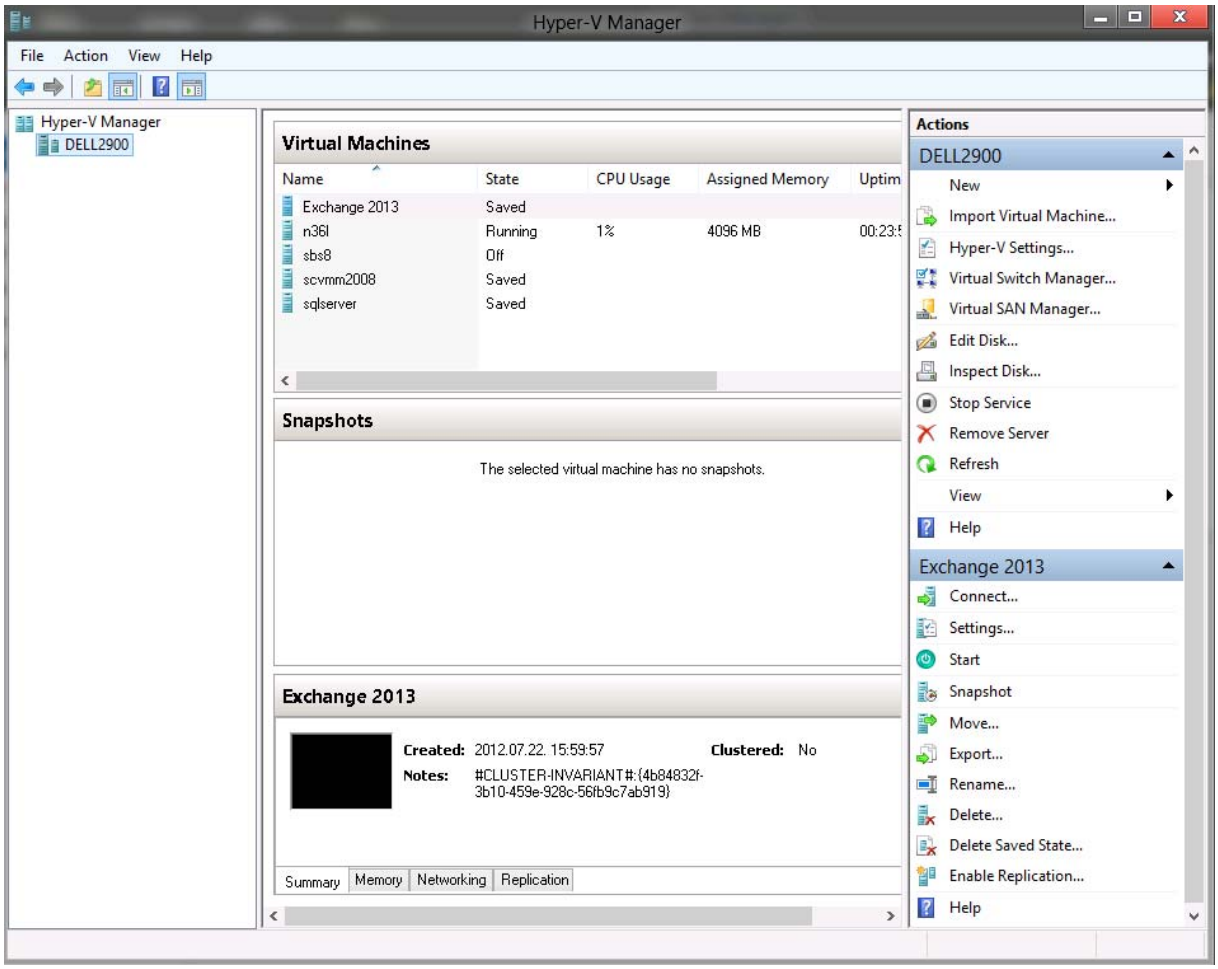
A virtuális gép létrehozásakor ugyanolyan hardver-feltételeket érdemes biztosítanunk, mintha a szervert fizikai gépre telepítenénk. A virtuális gépnek a következő erőforrásokat adhatjuk:

- CPU: 1-32 virtuális processzort tudunk egy virtuális géphez rendelni, ezen kívül megadhatunk minimális fenntartást, amit ez a gép mindenképpen megkap, és maximális terhelést is, nehogy egy virtuális gép elvegye az erőforrást a többi gép elől.
- Memória: virtuális memóriát 1TB-ig allokálhatunk a gépünknek, illetve használhatunk dinamikus memóriakezelést, pl. egy virtuális Exchange kiszolgáló kaphat 8-32GB RAM-ot, aktuális terheléstől függően.
- Lemezvezérlő: konfigurálhatunk IDE és SCSI vezérlőket is. IDE eszközről tud bootolni a virtuális gép, viszont maximum 4 lemezt tudunk csatlakoztatni, SCSI vezérlő esetén maximum 128 VHD csatolható, és maximum 4 SCSI vezérlőt adhatunk egy gépnek, így összesen 512 VHD lemezt tudunk csatlakoztatni. Az IDE és SCSI vezérlők között már nincs teljesítmény-különbség.
- NIC: szintén kétféle hálózati csatoló közül választhatunk: szintetikus vagy örökölt. Az örökölt hálózati csatoló egy létező kártya emulációja, így megvannak a maga korlátozásai, sávszélességben, és funkcionalitásban, de kompatibilis a legtöbb – nem csak Microsoft - operációs rendszerrel, és rendelkezik PXE támogatással, tehát hálózati bootolásra alkalmas. A Szintetikus hálózati csatoló semmiféle korlátozással nem rendelkezik, akár 10GB/sec-os sebességre is képes, de natívan csak Windows Server 2008-tól támogatott, a régebbi gépekre fel kell telepítenünk az integrációs szolgáltatást, hogy használni tudjuk. Szintetikus NIC-ből maximum 8-at, örököltből maximum 4-et használhatunk virtuális gépenként.
- Fibre Channel kártya: újdonság a 2012-ben, a fizikai gépben lévő FC kártyát tudjuk felcsatolni a virtuális gépbe, amennyiben a drivere ezt támogatja
- RemoteFX video vezérlő: 3D-s video vezérlő, használatával a virtuális gép kihasználhatja a fizikai gép GPU-ját és DirectX képességét.

9.1.2 Hyper-V telepítése

A szerepkör telepítése előtt meg kell győződnünk, hogy a BIOS-ban be van kapcsolva a DEP és a Virtualizáció (Intel-VT vagy AMD-V). Ha nincs, bekapcsolás után áramtalanítanunk kell a gépet.

Telepítés után már használhatjuk is a Virtual Machine Managerünket:



A Hyper-V Manager egy MMC 3.0-ra épülő konzol: a bal oldali részben további Hyper-V hosztokat tudunk felvenni, középen felül a virtuális gépeinket látjuk, alatta a kiválasztott gép pillanatfelvételét, illetve kis ablakban a gép képernyőjét. Jobb oldalt, az ún. Akció panelen, felül a hosztnál, alatta pedig az adott virtuális gépeknél elérhető műveleteket láthatjuk.

9.2 Virtuális gépek létrehozása

Mielőtt létrehoznánk egy virtuális gépet, érdemes először létrehozni egy hálózati kapcsolatot, illetve egy VHD lemezt.

9.2.1 Virtuális hálózatok

Ahhoz, hogy a virtuális gépeink hozzáférjenek a hálózathoz, először virtuális switcheket kell létrehoznunk. Ezek a virtuális switchek a fizikai hálózaton használt hálózati switchek virtualizált megoldásai, segítségükkel a virtuális gépek különböző hálózatokhoz férhetnek hozzá. Létrehozni a Hyper-V Manager Virtual Switch Manager részénél tudjuk. a következő típusú switcheket hozhatjuk létre:

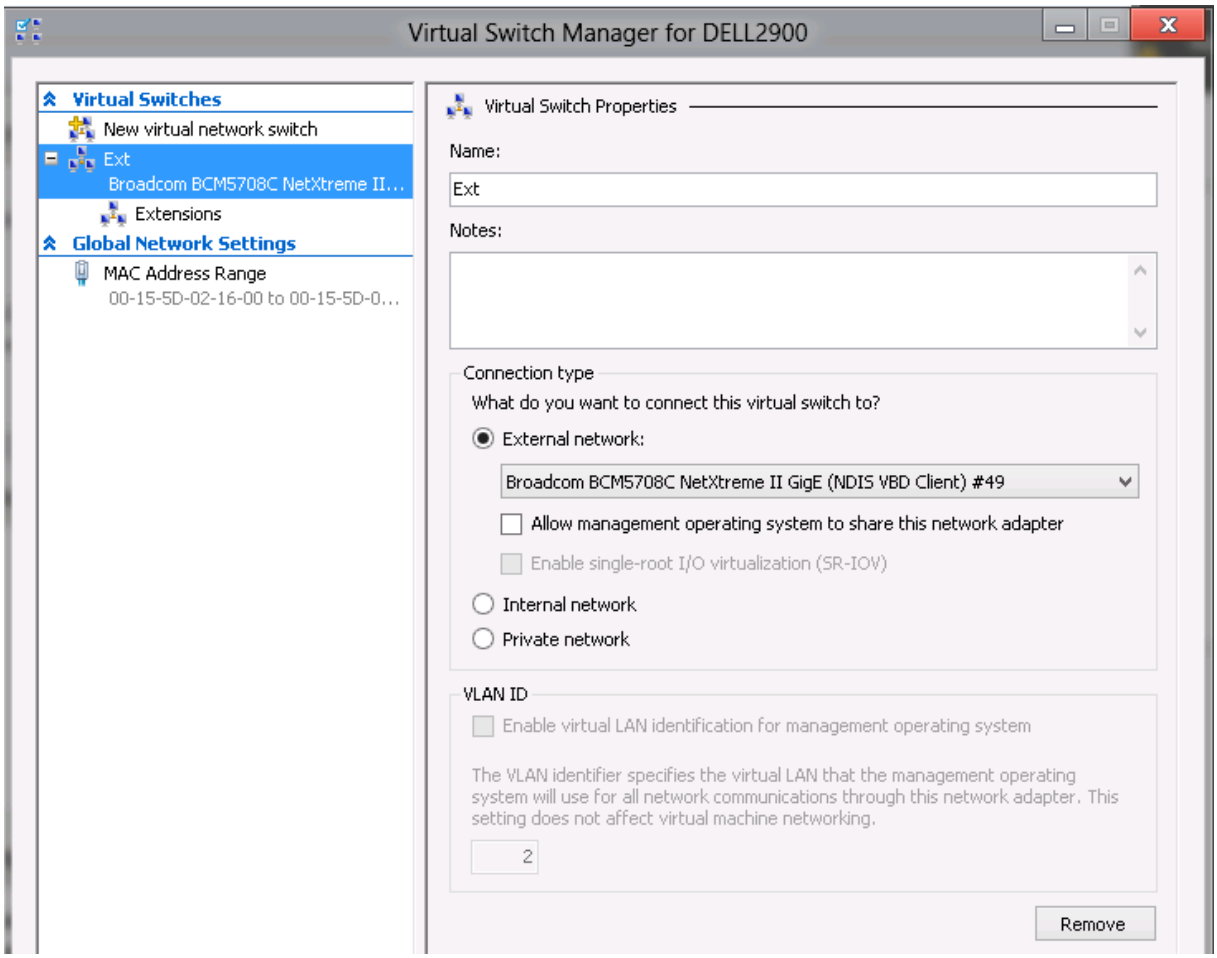
- External: külső hálózatokhoz csatlakozhatunk. Létrehozásakor meg kell adnunk egy fizikai hálózati kártyát, NIC Teaminget, vagy egy vezeték nélküli LAN adaptert. Ha csak egy fizikai kártyán van a hoszt gépben, akkor megoszthatjuk a virtuális és a hoszt gép között, de javasolt egy külön fizikai kártyát fenntartani a hoszt gép üzemeltetéséhez, amihez nem csatolunk external switch-et

- Internal: a belső switch a fizikai géppel, és a többi virtuális géppel tud kommunikálni, a külső hálózattal nem.
- Private: kizárólag a virtuális gépek kommunikálhatnak egymással, akik ugyanazon a privát switchen vannak.

A külső hálózatnál konfigurálhatunk VLAN azonosítót is, ha a fizikai hálózatunkon is használunk VLAN-t, így szegmentálhatjuk a forgalmat.

Hálózat létrehozásakor két további bővítményt adhatunk meg:

- Microsoft NDIS capture: ha valamilyen hálózat-elemző programmal elemezni akarjuk a virtuális hálózat forgalmát
- Microsoft Windows Filtering Platform: ha a hálózati forgalmat szűrni szeretnénk.



9.2.2 Virtuális lemezek kezelése

A virtuális lemez egy speciális fájlformátum, amely magában foglal egy teljes merevlemezt: partícionálni tudjuk, különböző fájlrendszereket tudunk létrehozni, adatokat tudunk másolni rá. Először a Microsoft Virtual PC-ben jelent meg, és fő felhasználási területe a virtuális gépek tárolása, de a Windows Server 2008-ban már a mentés is VHD formátumban tárolódik, illetve az iSCSI lemezek is VHD állományok. Egy VHD fájlról a virtuális gépeink képesek bootolni is, illetve a Windows Server, a Windows 7 és Windows 8 néhány verziója fizikai gépeken is képes VHD bootolásra. A virtuális lemezeinket kezelhetjük a Hyper-V Managerből, illetve a fent felsorolt operációs rendszerek lemezkezelőjéből is létrehozhatunk, módosít-

hatunk és felcsatolhatunk VHD állományokat. Ezen kívül PowerShellből a New-VHD cmdlet-tel vagy akár diskpart segítségével is hozhatunk létre ilyen fájlokat.

A Windows Server 2012-ben megjelent VHDX formátum nagyobb lemezek kezelését teszi lehetővé, és nagyobb üzembiztonságot biztosít ezeknek a nagyméretű állományoknak. A VHD fájlformátum maximum 2TB-os lemezeket támogat, míg a VHDX maximális mérete 64TB lehet.

9.2.3 Virtuális lemez típusok

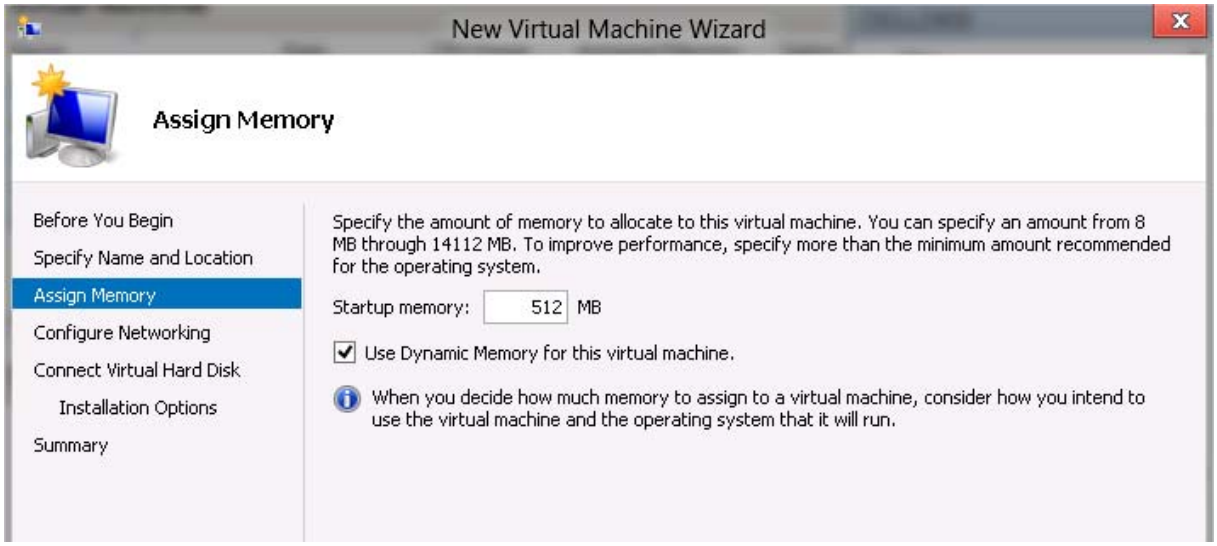
Lemez létrehozásakor, felhasználástól függően a következő típusok közül választhatunk:

- Fixed disk (Fix méretű lemez) a VHDX létrehozásakor a rendszer lefoglalja a teljes lemezterületet a fájl számára. Erre ritkán van szükség.
- Dynamic disk: (Dinamikusan növekvő) A virtuális lemez létrehozásakor csak minimális területet foglal, és ahogy elkezdjük feltölteni adattal, a fájl mérete dinamikusan növekszik. Teljesítmény-különbség nincs a dinamikus és a fix méretű lemezek között, és mivel általában nem tudjuk, hogy az adott kiszolgálón mennyi adatot fogunk tárolni a jövőben, érdemes ezt a lemeztípust választani. Ha adatokat törlünk egy dinamikus lemezről, a mérete nem fog automatikusan csökkeni, ilyenkor zsugorítani kell a VHD fájlunkat.
- Pass-through Disk (közvetlen hozzáférésű lemez) ebben az esetben a virtuális gép közvetlenül hozzáfér egy fizikai lemezhez. Általában iSCSI rendszereknél használjuk, hiszen az iSCSI a targeten egyébként is VHD formátum, és pass-through disk használatával elkerüljük az egymásba ágyazott VHD-k használatát. Ahhoz, hogy egy fizikai lemezt be tudjunk csatolni egy virtuális gépbe, a fizikai gépen offline állapotban kell helyeznünk azt a lemezkezelőben.
- Differencing Disk (különbözeti lemez) egy már meglévő VHD-t, mint szülőpartíciót tudunk használni, emellett létrehozunk egy különbözeti lemezt, ahol a módosításokat tároljuk. A szülő VHD-t csak olvasásra érjük el, így egy szülőhöz bármennyi különbözeti VHD-t csatolhatunk. Pl. létrehozunk egy Windows 8 VHD-t, ide feltelepítjük a Windows 8 szükséges verzióját, majd további virtuális gépeket hozunk létre, egyiken Office 2010, a másikon Office 2013, és így tovább. Így a Windows 8 telepítésünket csak egy példányban tároljuk, ezzel jelentős tárterületet spórolhatunk meg.

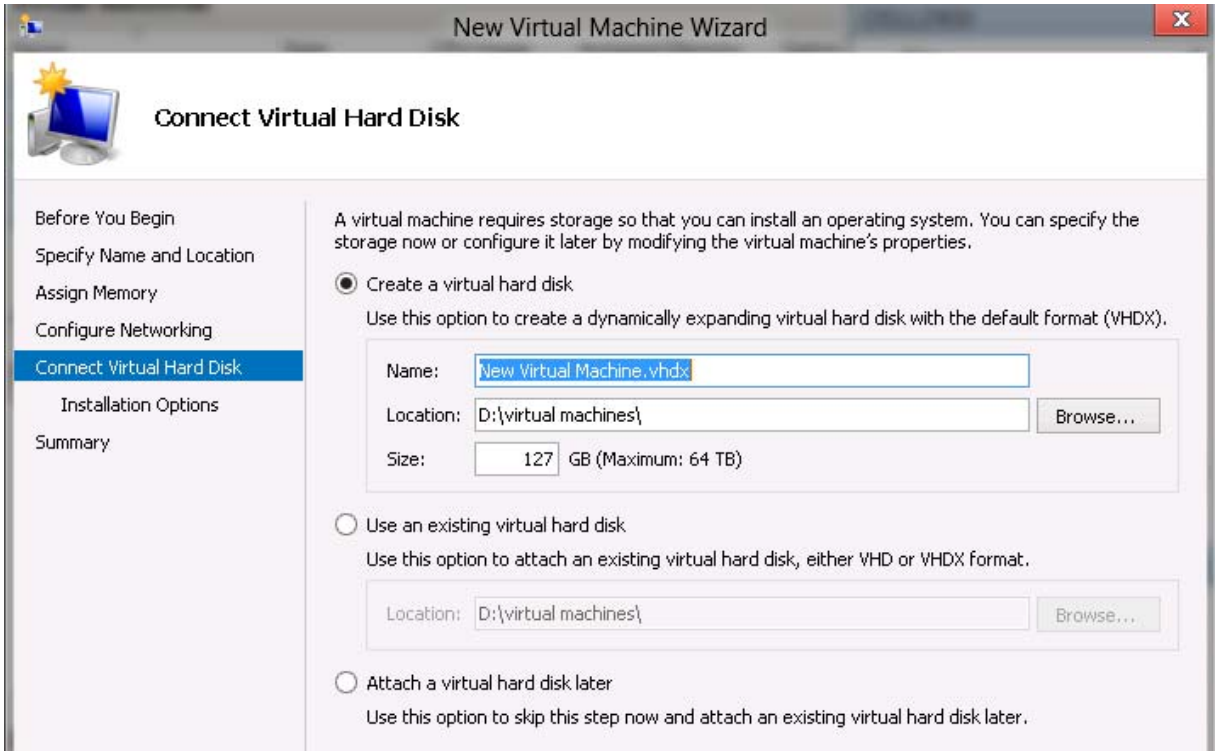
9.2.4 Virtuális gép létrehozása

Ha létrehoztunk virtuális hálózatokat, és esetleg virtuális lemezeket is, akkor nekifoghatunk a virtuális gép létrehozásának: Hyper-V Manager/New virtual machine.

Létrehozáskor meg kell adnunk egy nevet, illetve egy könyvtárat, ahol a virtuális gépünk beállításai lesznek. Ez nem feltétlenül egyezik meg a VHD állományunk helyével, itt a gép konfigurációját tároljuk XML formátumban, illetve a pillanatképeket. A következő lapon megadhatunk egy indítási memória mennyiséget, ami a virtuális gép indításához feltétlenül szükséges, illetve itt is engedélyezhetjük a dinamikus memóriakezelést:

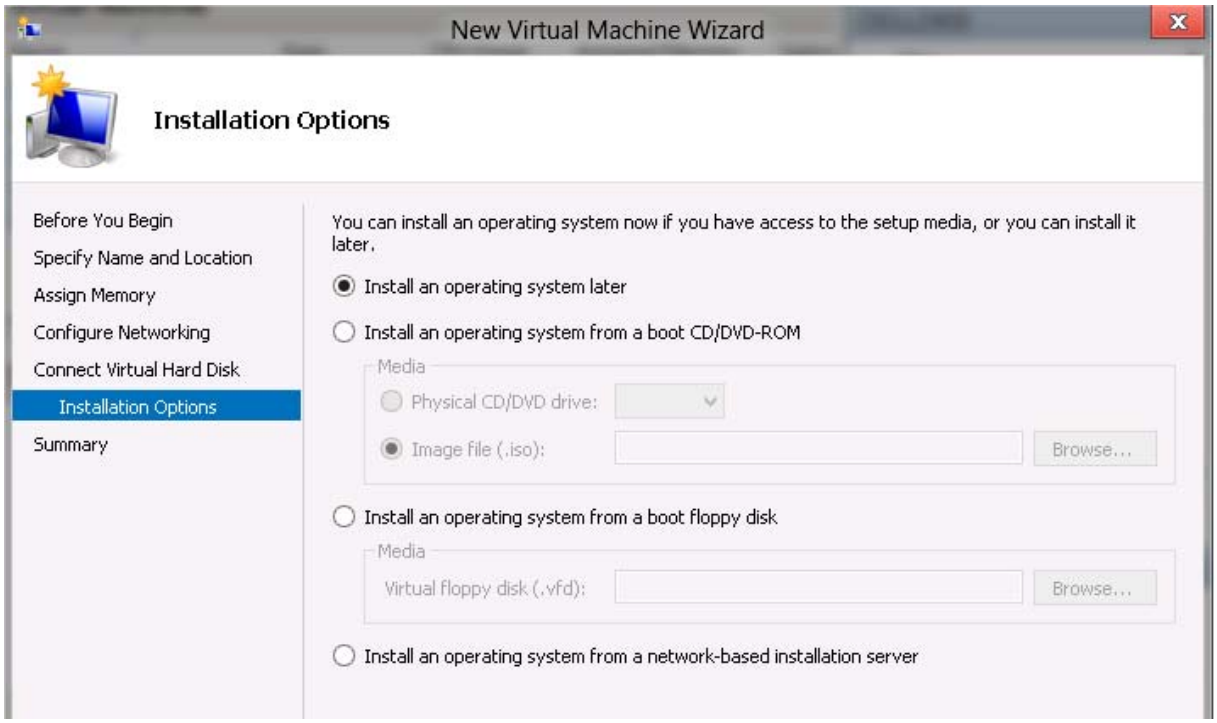


A hálózati kapcsolat kiválasztása után pedig virtuális lemezt konfigurálhatunk:



Létrehozhatunk új VHDX fájlt, csatolhatunk meglévő lemezt, ha pl. fizikai gépet virtualizálunk be, vagy csatolhatunk később is lemezt, ha pass-through diszket akarunk használni.

A telepítési opciónál csatolhatunk ISO állományt, fizikai DVD meghajtót, vagy választhatjuk a hálózati indítást (PXE) is:

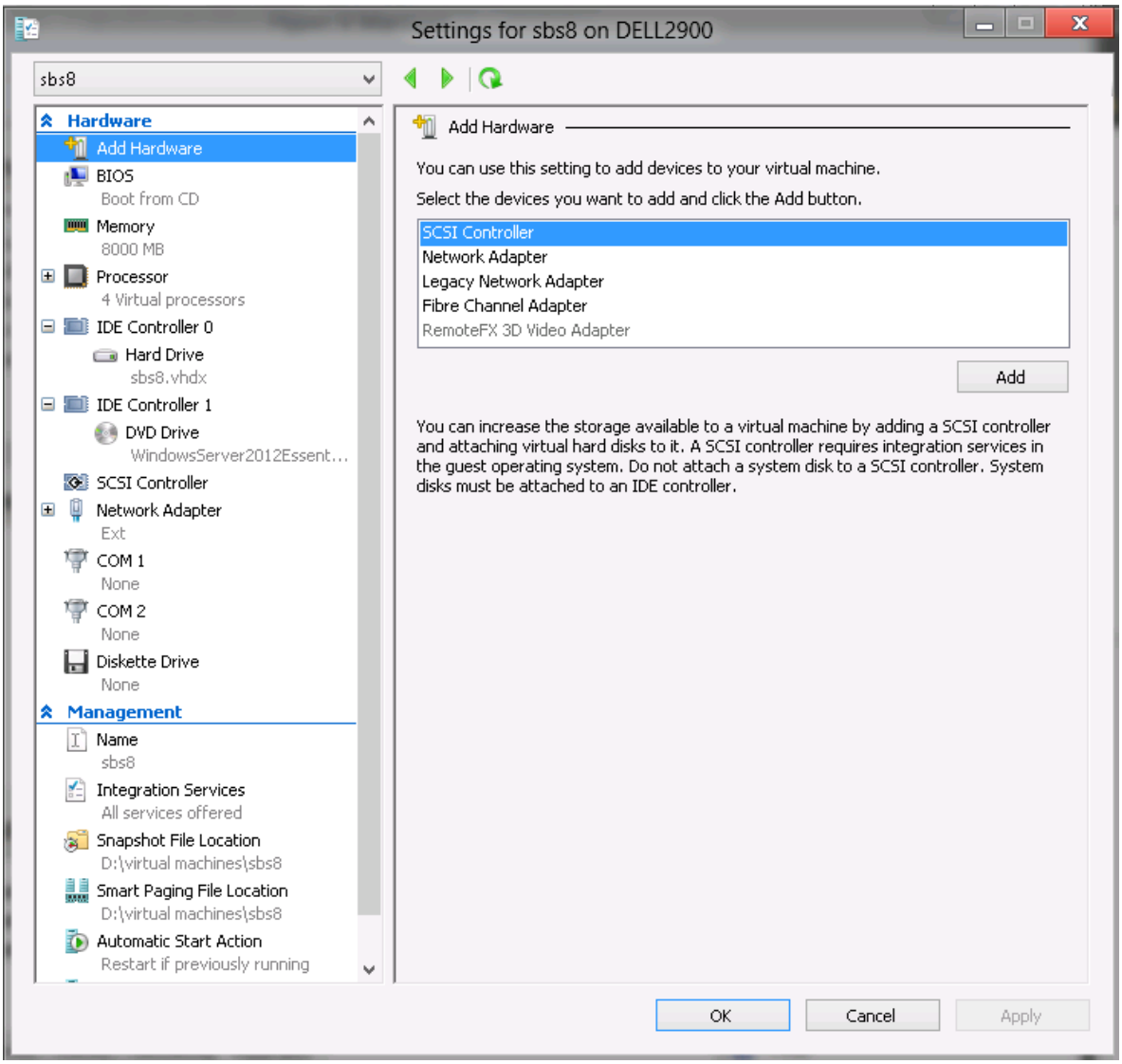


Network-based installation-nál a virtuális gépünk örökölt hálózati kártyát fog kapni, hiszen itt van lehetőségünk PXE boot-ra.

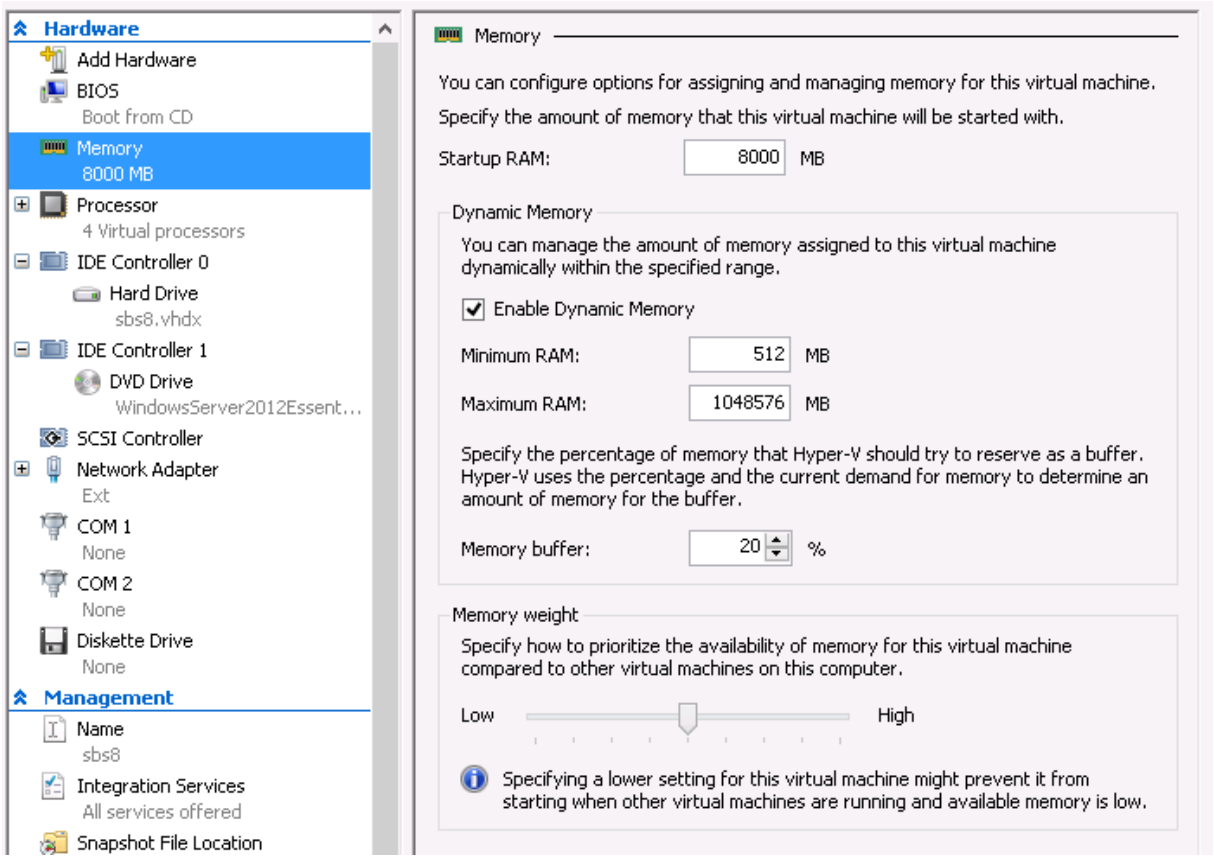
9.3 Virtuális gép beállítása

Miután létrehoztuk a virtuális gépünket, de még nem indítottuk el, további eszközöket is hozzáadhatunk, illetve egyéb beállításokat is megadhatunk. Nézzük ezeket:

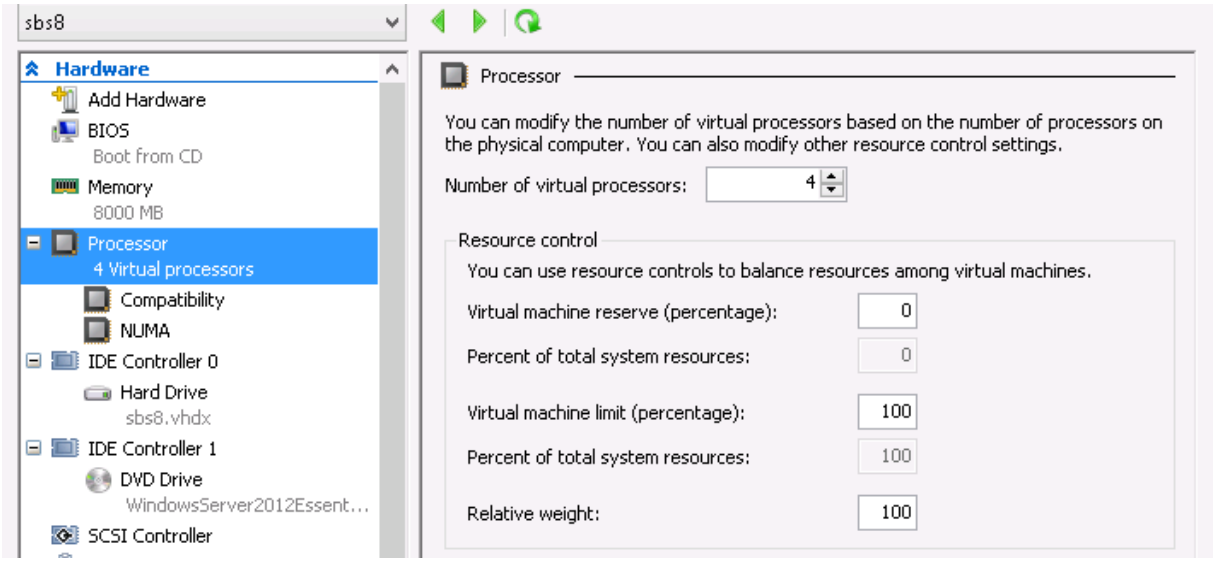
Az „Add hardware” résznél további eszközöket adhatunk hozzá, legyen az SCSI, LAN FC vagy RemoteFX videokártya.



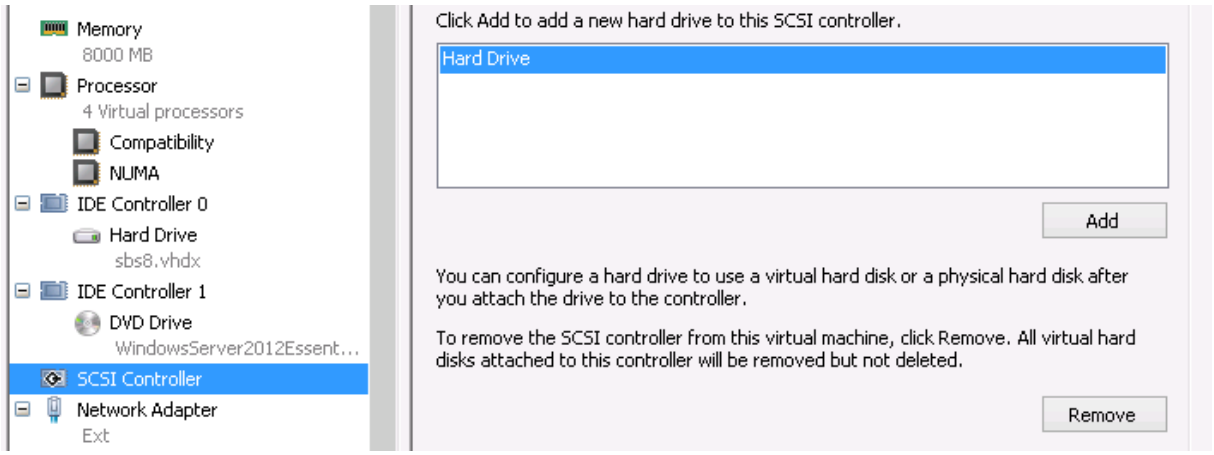
A memory résznél adhatunk dinamikus memóriát, illetve súlyozhatjuk a gépünket a többi virtuális géphez képest. Ha ez a gépünk az üzletileg kritikus vállalatirányítási rendszert futtatja, érdemes magas súlyozásra állítani. A gép aktuális memória-felhasználásáról a Hyper-V konzolban kapunk aktuális információt.



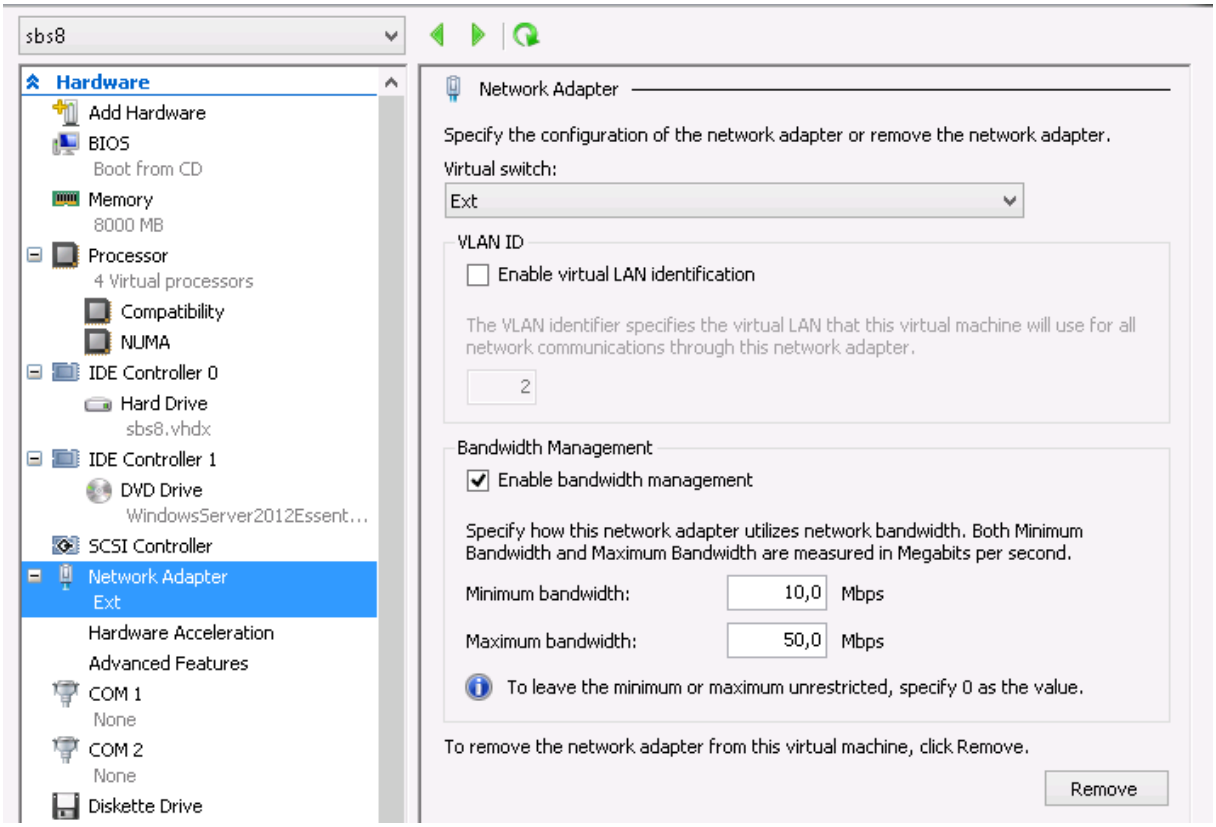
A CPU beállításoknál megadhatjuk, a virtuális mennyi magot használhat, illetve fenntartást, és felső limitet adhatunk a virtuális gépünknek. Itt is van lehetőségünk relatív súlyt adni a CPU használatra.



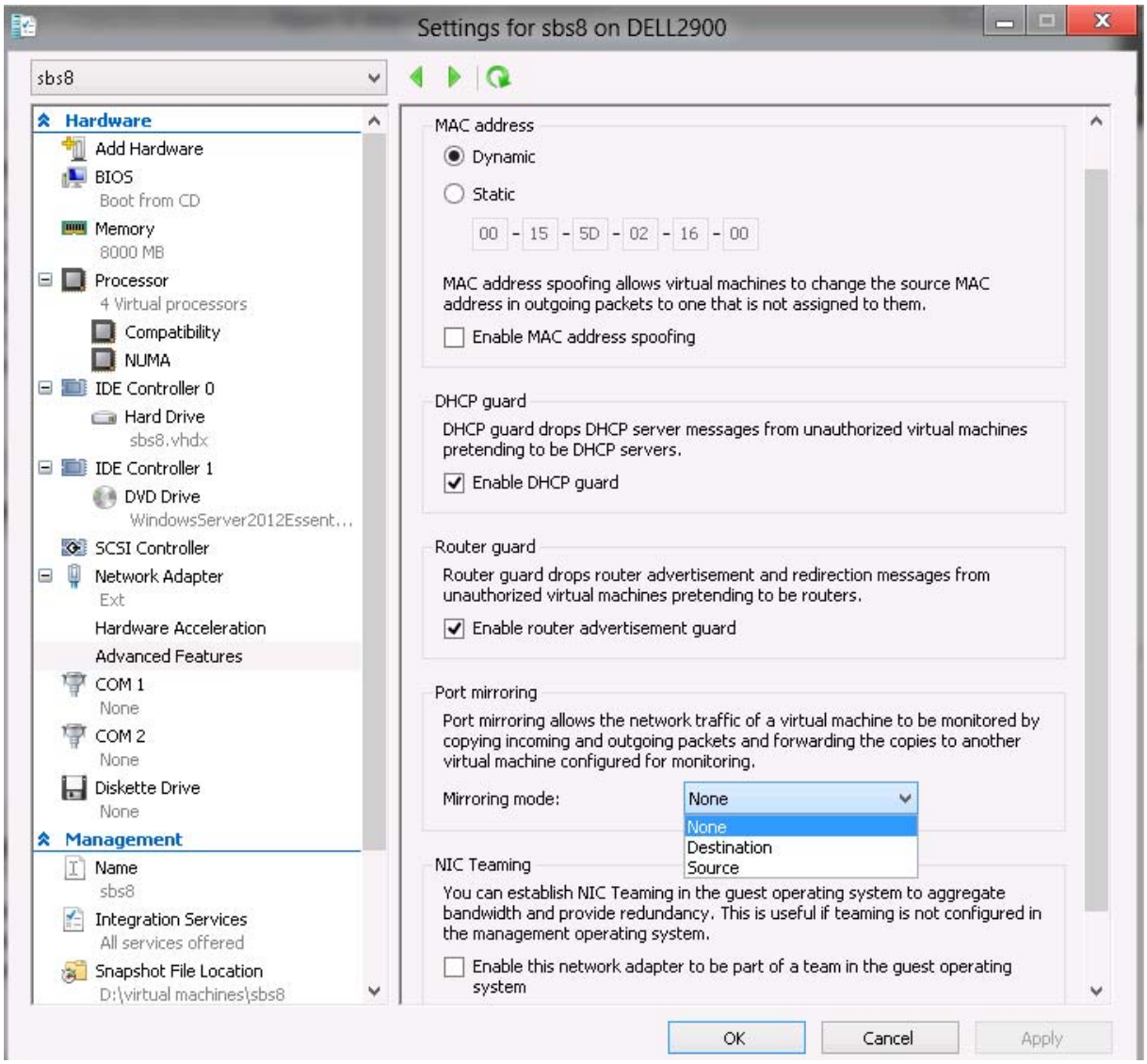
Az IDE és SCSI vezérlőknél tudunk további VHD lemezeket hozzáadni gépünkhöz, IDE csatornánként maximum 2-őt, SCSI kártyánként 128-at.



Az újdonság a Windows Server 2008-hoz képest a hálózat kezelés, ahol szintén adhatunk minimum fenntartott, és maximális sávszélességet. Ez különösen hasznos lehet, ha más cégeknek hosztolunk virtuális gépeket, vagy a webkiszolgálónknak allokálni szeretnénk a szükséges sávszélességet:



Itt tudjuk engedélyezni a VLAN azonosítást, a hardvergyorsítást, amennyiben a hálózati kártyánk ezt támogatja, illetve a speciális képességeket, ami szintén új a Windows Server 2012-ben:



A virtuális hálózati kártyának tudunk MAC címet adni, ha fizikai gépről migrálunk, és bizonyos szolgáltatások, vagy licencek MAC címhez vannak kötve. Ha nem adunk meg egyéni MAC címet, a Hyper-V egy dinamikus tartományból automatikusan kioszt egyet. Engedélyezhetjük a MAC spoofing-ot, ha bizonyos szolgáltatások több MAC címen működnek, vagy a virtuális gépnek cserélnie kell a MAC címét. Alapból ez a szolgáltatás biztonsági okokból le van tiltva.

A DHCP Guard letiltja a virtuális gépektől érkező DHCP üzeneteket. Ha a virtuális gépeket nem mi üzemeltetjük, hanem alkalmazás-gazdák, vagy hosztolunk virtuális gépeket, akkor érdemes bekapcsolni.

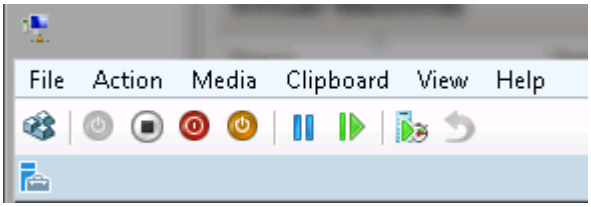
A Router Guard hasonló feladatot lát el, a virtuális gépek nem küldhetnek olyan üzeneteket a hálózatra, hogy ők a helyi hálózat átjárói (IPV6 Router advertisement)

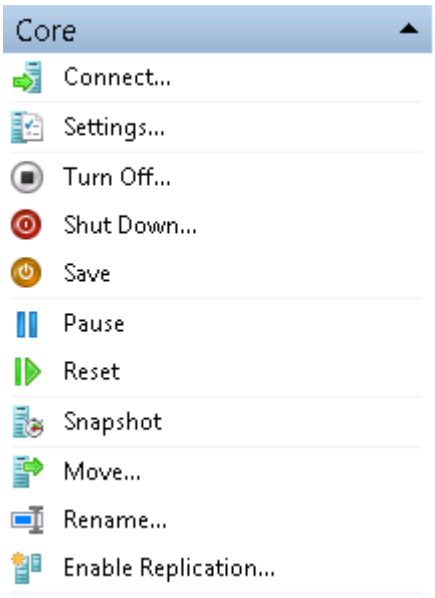
A Port Mirroring lemásol minden forgalmat, amit a source hálózati kártyára érkezik, és átküldi egy másik virtuális gépre, ahol a Destination értéket választottuk, így elemezhetjük a virtuális gép forgalmát egy másik gépen.

Ha NIC teaminget nem a gazdagépen, hanem a virtuális gépen szeretnénk használni, erre is lehetőségünk van, ilyenkor az összes virtuális hálózati kártyánál engedélyezni kell, hogy tagja lehessen NIC team-nek.

9.4 Virtuális gép üzemeltetése

A virtuális gépeinket a Virtual Machine Connection programmal érhetjük el. A VMC kliens RDP protokollt használ, hasonlóan a távoli asztali kiszolgálóhoz, de a 2179-es TCP portot használja. A gépeket ezen kívül a Hyper-V management console actions paneljéből is vezérelhetjük:





- Turn off: a számítógép kikapcsolása
- Shut down: az operációs rendszer szabályos leállítása. Néhány régebbi operációs rendszernél fel kell telepítenünk az integrációs szolgáltatásokat, hogy a hoszt gép utasítást tudjon küldeni a virtuális gépen futó operációs rendszernek
- Save: a virtuális gép mentése. Ilyenkor a memória tartalmát is mentjük, tehát bármikor el tudjuk indítani virtuális gépet, anélkül hogy újraindulna. Leginkább a hibernáláshoz hasonlít. Bizonyos szerepköröket, pl. Windows Server 2008 tartományvezérlőt nem szabad mentett állapotba helyezni, mert adatbázis-konzisztencia hibák léphetnek fel.
- Pause: hasonlóan a Save opcióhoz, lementi a virtuális gépet, de nem szabadítja fel a memóriát, csak a processzort. Ez nagyjából megegyezik az alvás funkcióval.
- Reset: újraindítja a virtuális gépet.

9.4.1 Pillanatfelvételek

Snapshot, vagy pillanatfelvétel készítésével a virtuális gépünk aktuális állapotát tudjuk menteni, beleértve a VHD és a memória tartalmát. Erre a pillanatfelvételre bármikor visszaállhatunk, sőt, mindegyik virtuális gépről akár 50 pillanatfelvételt is készíthetünk. Különböző funkciók telepítésekor, vagy bonyolultabb, többlépéses teszteléskor érdemes használni, de bizonyos kiszolgálókon akár patchelés előtt is készíthetünk snapshotot. Fontos, hogy tartományvezérlőnél, SQL, vagy Exchange kiszolgálónál a visszaállítás nem várt eredményeket hozhat, például a pillanatfelvétel készítése óta érkezett levelek elvesznek, vagy a számítógép

elveszti tartomány-tagságát. Szintén fontos, hogy a pillanatfelvétel készítése nem helyettesíti a rendszeres biztonsági mentést.

A pillanatfelvételek AVHD vagy AVHDX fájlban tárolódnak, vagyis amikor készítünk egyet, az eredeti VHD állományunkat a rendszer lezárja, és a módosításokat egy új AVHD fájlba írja. A visszaállítás (revert) tehát az AVHD törlését jelenti, és visszaállást az eredeti AVHD-ra. Amennyiben több snapshotot készítünk, a rendszer külön-külön AVHD fájlokat köt egymás után sorba. Ezeket a fájlokat úgy tudjuk egyesíteni az eredeti VHD-ba, ha exportáljuk a gépet, majd visszaimportáljuk. Ha töröljük a pillanatfelvételeket, a Windows Server 2012 azonnal törli az AVHD fájlt, és felszabadítja a szabad területet, szemben a Windows Server 2008-al, ahol le kellett állítanunk a virtuális gépet, hogy az AVHD törlődjön, vagy esetleg összefésüljük az eredeti VHD-val.

9.4.2 Virtuális gépek exportálása és importálása

Virtuális gépeinket exportálhatjuk, importálhatjuk, és mozgathatjuk Hyper-V kiszolgálók között. Amikor virtuális gépet importálunk, akkor betöltjük nem csak a VHD állományt, de a komplett konfigurációt, a hálózati beállításokat, és az esetleges pillanatfelvételeket is, illetve megőrizhetjük a virtuális gép azonosítóját. Szemben a Windows Server 2008-al, importálni nem csak egy másik gépről exportált gépet tudunk, de megadhatunk egy mappát is, ahonnan az importálás varázsló behelyezi a gépet a Hyper-V konzolba. Ez a varázsló kijavítja a konfigurációs XML esetleges hibáit, a lemezek útvonalait, stb. Így könnyebben tudunk gépeket importálni egy meghibásodott Hyper-V hosztról. Importáláskor arra is lehetőségünk van, hogy egy exportált gép másolatát importáljuk vissza, így az eredeti exportot később bármikor felhasználhatjuk.

Exportáláskor megadhatjuk, hogy a virtuális gép legutolsó állapotát szeretnénk exportálni, vagy az összes régebbi pillanatképre is szükségünk lesz. Az exportálás semmilyen hatással nincs az eredeti virtuális gépre.

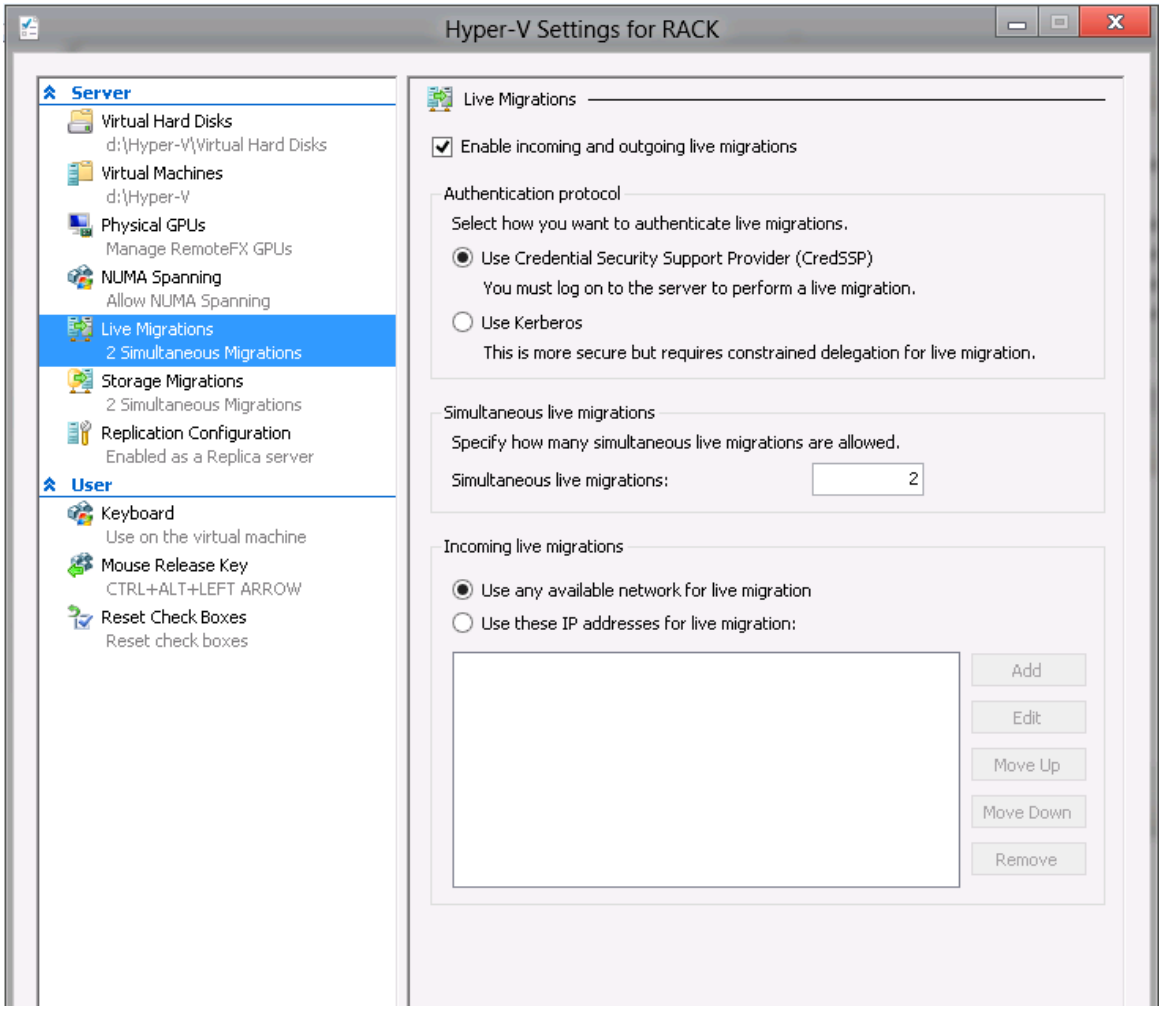
Mozgatáskor két lehetőség közül választhatunk:

- Virtuális gépek mozgatása hosztok között: Windows Server 2012-őt futtató Hyper-V 3-as hosztok között mozgathatunk gépeket Live Migration használatával, vagyis a virtuális gépek leállítása nélkül
- Adatok mozgatása hoszton belül: különböző kötetek között mozgathatjuk a teljes virtuális gépet, vagy csak bizonyos komponenseit, pl. VHD-t, a pillanatfelvételeket vagy a konfigurációs állományokat.

9.4.3 Live Migration

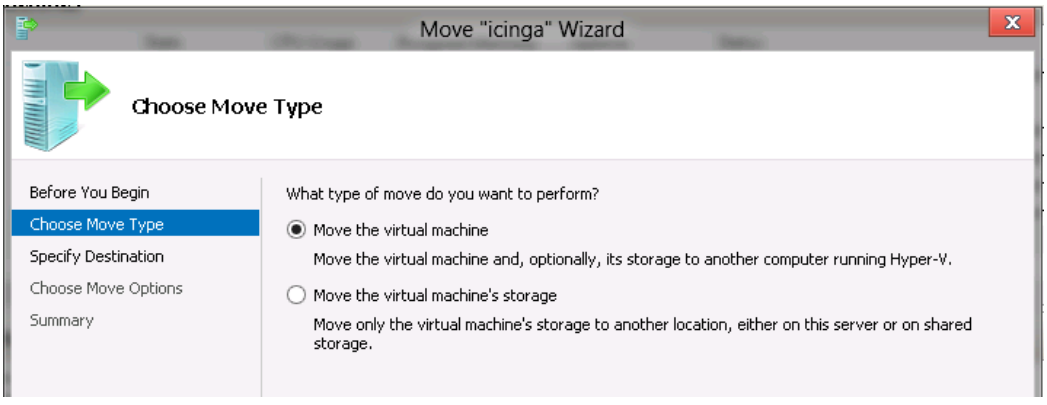
Az egyik legérdekesebb fejlesztés a továbbfejlesztett Live Migration szolgáltatás. A Windows Server 2008 R2-ben is volt lehetőségünk virtuális gépeket futó állapotban mozgatni, de kizárólag Hyper-V fürtön belül, magas rendelkezésre állású rendszereken, ahol közös storage-ot kellett használnunk. A Windows Server 2012-ben viszont virtuális gépet mozgathatunk fürtről különálló gépre, különálló gépről fürtre, és különálló gépről különálló gépre, tehát bárhonnan bárhová, amennyiben mindegyik Hyper-V 3.0-ás verziót használ

A Live Migrationt engedélyezni kell a hoszt gépeken. A Hyper-V Managerben nyissuk meg a Hyper-V Settings részt:



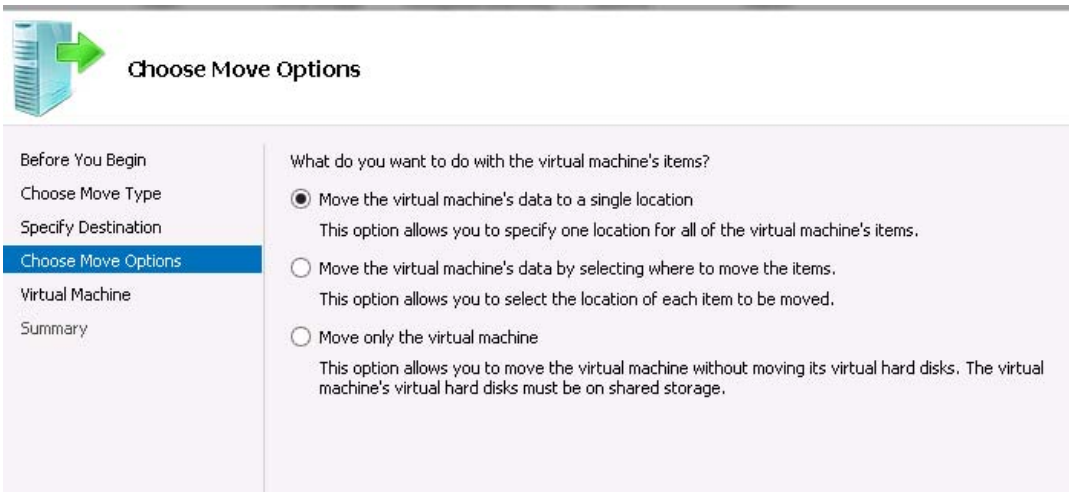
A Live Migration résznél engedélyezzük a migrálást mindkét hoszton. Lehetőségünk van egy időben több Live Migration-t engedélyezni, így gyorsabban tudunk költözni egyik hosztról a másikra.

Majd válasszunk ki egy tetszőleges gépet, és a helyi menüben válasszuk a Move opciót:



Az első lehetőség a virtuális gépet migrálja hosztok között, a második a hoszton belül helyezi át.

A „Move virtual machine” résznél meg kell adnunk a célszámítógépet, majd meg kell adnunk, hogy milyen mappákba szeretnénk helyezni a virtuális gépünket:



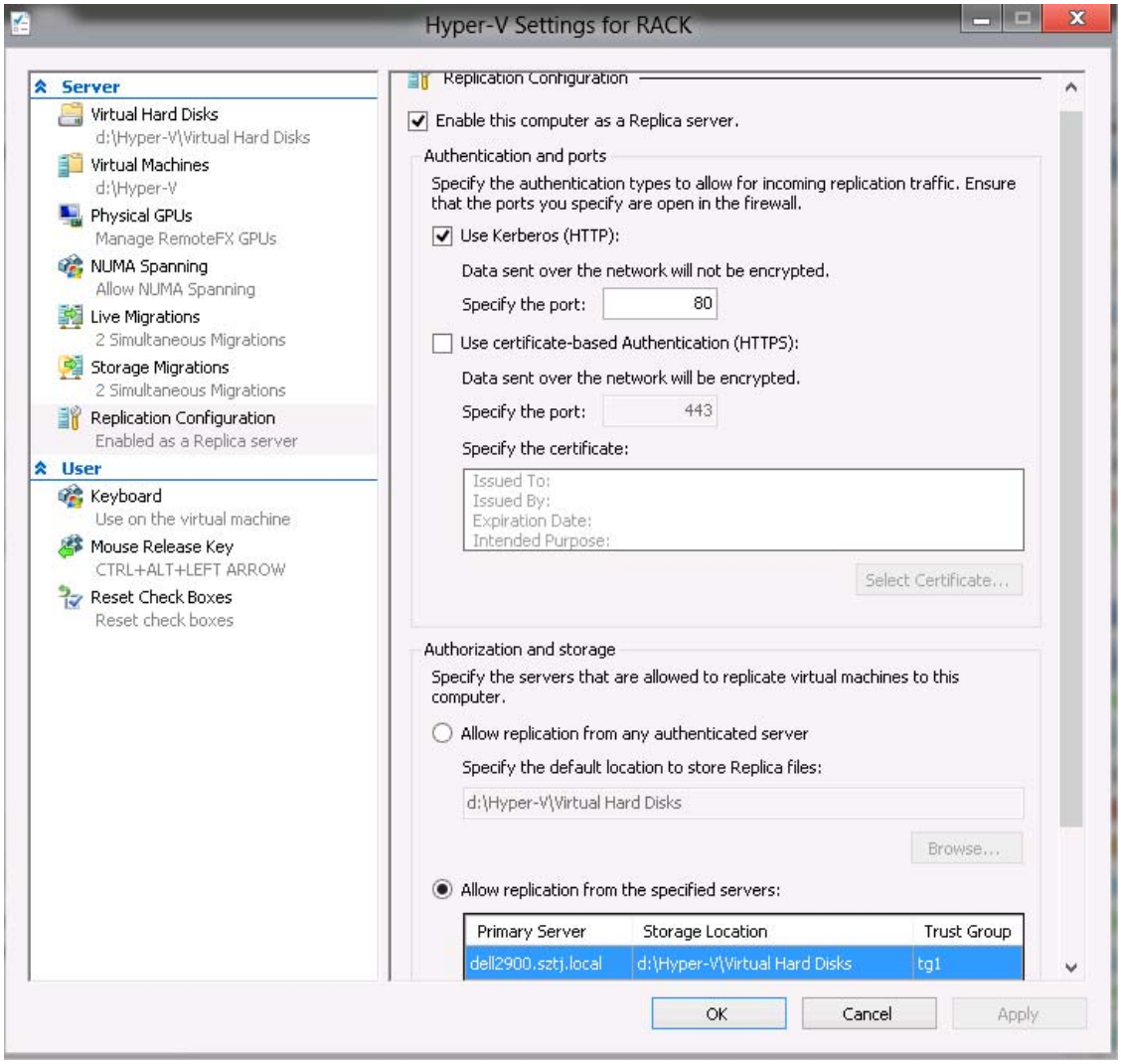
Az utolsó lehetőséget (Move only the virtual machine) akkor tudjuk használni, ha a virtuális gépeinket közös storage-on tároljuk. Ilyenkor az Offloaded Data Transfer (ODX) használatával nem a hosztok között költözik a gép, hanem a storage belsejében, ezzel nem terheli a hosztokat, a hálózat, és sokkal gyorsabban mozgathatjuk gépeinket.

A célmappa megadása után pedig el is kezdhetjük a virtuális gépünk mozgatását. Ez a funkció nem működik különböző processzorral rendelkező gépek között, tehát nem tudunk AMD-ről Intel hosztra migrálni.

9.4.4 Hyper-V replikáció

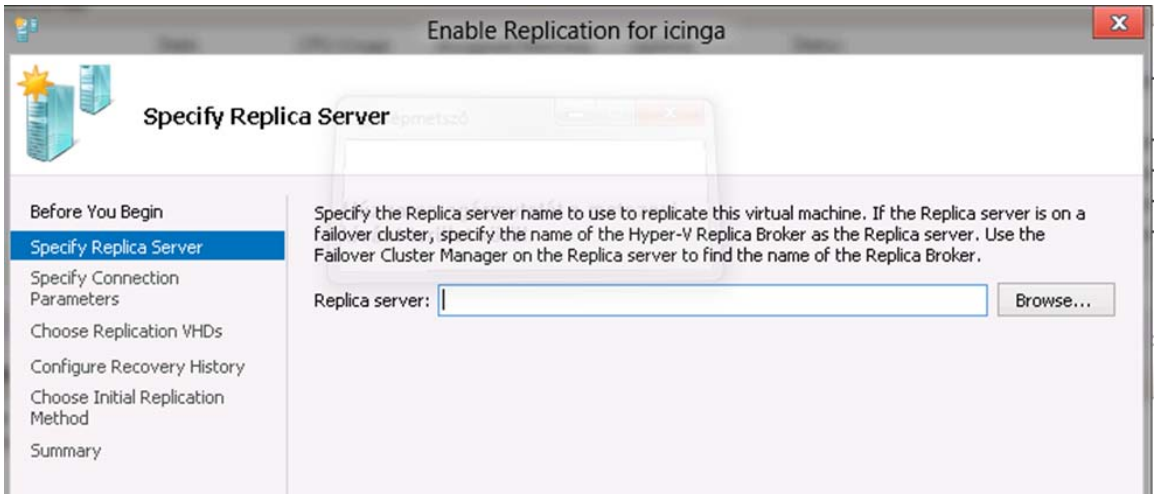
A Hyper-V replika lehetővé teszi, hogy ugyanazt a virtuális gépet két különböző hoszton futtathassuk, az egyik gépen egy on-line, a másikon egy offline példányban, így egy esetleges leálláskor a másik gépen futó másolat elindítható, és képes kiszolgálni a hálózati kéréseket. Replikáció esetén különböző típusú hosztokat és külön storage-okat használhatunk, sőt a két kiszolgáló lehet akár külön telephelyen is. A virtuális gép két példánya folyamatos szinkronban van, és bármikor átterhelhető a másik hosztra. A replikáció kiépítése után tesztelhetjük a tervezett és a nem tervezett költözést is.

A replikációt engedélyeznünk kell mindkét kiszolgálón, majd meg kell adnunk, hogy HTTP-n, vagy HTTPS-en szeretnénk a replikációt futtatni. Az első esetben az adataink titkosítatlanul mennek át a hálózaton, a második esetben viszont tanúsítványokat kell konfigurálnunk. Tesztelésnél használhatunk HTTP-t is, de éles környezetben erősen javasolt a titkosított csatorna használata.

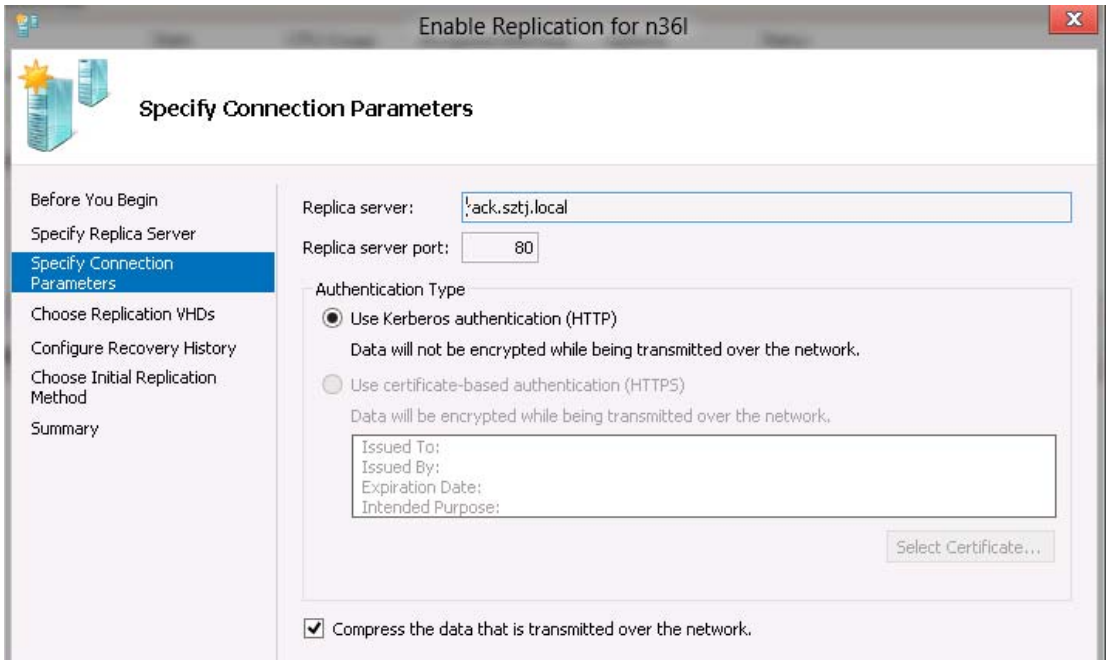


A fogadó hoszton engedélyeznünk kell a bejövő replikációt, meg kell adnunk, hogy milyen protokollt szeretnénk használni, illetve honnan fogadunk el bejövő replikációt, illetve, hogy a replikált gépeket hol szeretnénk tárolni.

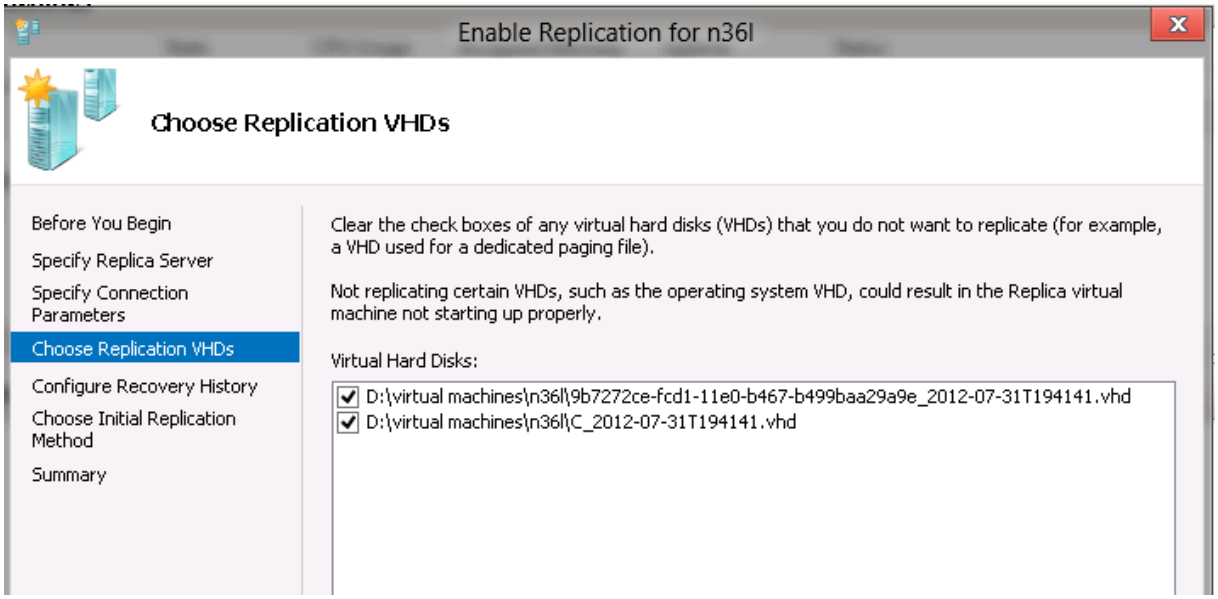
Ezután a küldő hoszton ki kell választanunk a replikálandó gépet, majd „Enable replication”.



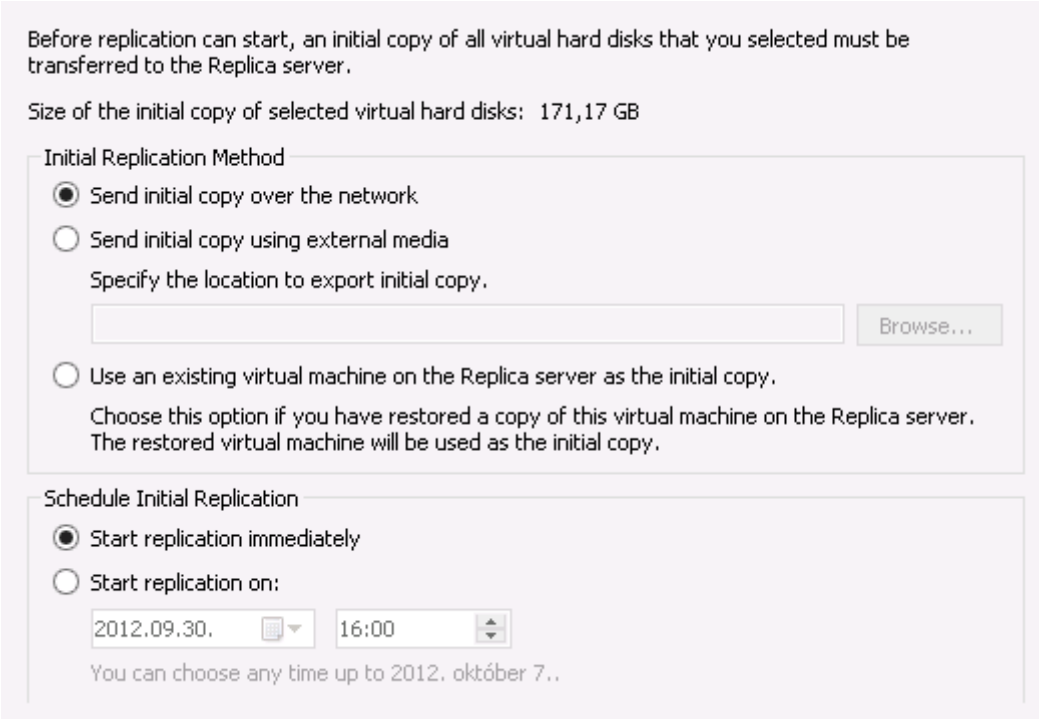
A varázslóban meg kell adnunk a replika szervert, ahová replikálni szeretnénk, a kapcsolathoz használni kívánt protokollt:



Kiválaszthatjuk a replikálni kívánt VHD-kat:



A visszaállítási pontok kiválasztása után pedig meg kell adnunk, hogy a kezdeti replikációt a hálózaton szeretnénk átküldeni, vagy külső adathordozón juttatjuk el a másik gépre. Ha másik telephelyre replikálunk, érdemes a második opciót választanunk:



Ezután kezdetét veszi a kezdeti replikáció, majd egy idő után a gépek szinkronizált állapotba kerülnek. Ekkor van lehetőségünk a virtuális gép Replication gyorsmenüjében tesztelni a replikációt, egy esetleges failovert, vagy tervezett átállást.

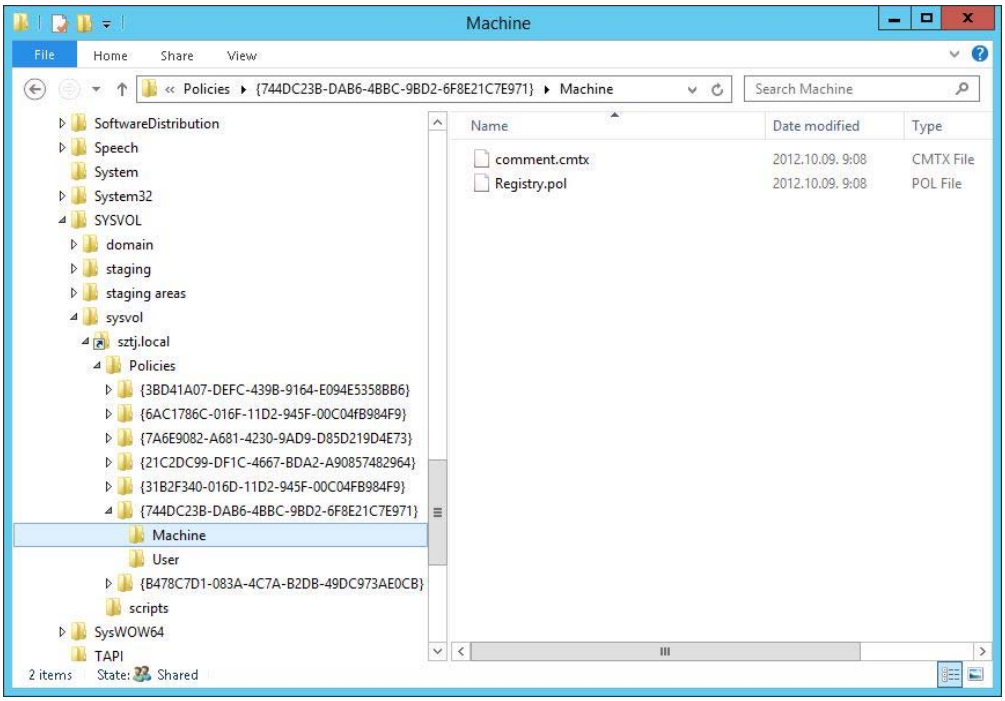
10 Csoportházirend

A csoportházirend (Group Policy) a Windows Server operációs rendszereinek egy funkciója, amivel megoldható a felhasználók, a számítógépek és a felhasználói munkakörnyezetek viselkedésének és jogosultságainak szabályozása. Ha egy felhasználóra vagy számítógépre több, esetleg egymással ütköző házirend-beállítás vonatkozik, a következő sorrendben kerülnek végrehajtásra (a később végrehajtott felülírja a korábbit):

- helyi számítógép
- hely (site)
- tartomány
- szervezeti egységek (OU)

A csoportházirend objektumokat megtaláljuk a tartományvezérlő SYSVOL mappájában, a kliensek ehhez a mappához fordulva töltik le beállításaikat. A SYSVOL mappa változásait a tartományvezérlő automatikusan továbbítja (replikálja) a többi tartományvezérlőre, így a mappa tartalma mindig konzisztens marad. Az adatátvitelre a Windows Server a Distributed File System Replication (DFSR) technológiát használja. Zárójelben megjegyzendő, hogy ez a technológia használatos még nagyméretű fájlkiszolgálók szinkronizálására is, akár WAN hálózaton keresztül is megőrizve adataink konzisztenciáját.

A Csoportházirend objektumok listáját a fájlstruktúrában a tartománynév alatt találjuk, ezeket egy 16 karakterből álló GUID szám azonosítja. Ha ezeket megnyitjuk, előtűnnek a számítógép és a felhasználói beállítások.



A számítógép indulásakor először a számítógép (Computer Configuration) alatti, rá vonatkozó csoportházrend objektumokat olvassa be, majd amikor erre a számítógépre a felhasználó bejelentkezik, akkor az ő személyére vonatkozó (User Configuration) beállításokat tölti be. Az érvényesítésre kerülő házirendek, a felülről történő öröklődés miatt több csoportházirendnek az összességét jelenti.

Az öröklődést lehet kikényszeríteni (enforcement vagy no override), illetve blokkolni (block inheritence). Kikényszerítés (enforcement) esetén az öröklés a legutolsó szintig megtörténik. A Blokkolás során szervezeti egység vagy tartomány esetén megszüntetjük egy felső szintről történő öröklődést, de csak abban az esetben, ha nincs kikényszerítve.

A fenti két lehetőség alkalmazása eléggé kétséges, hiszen az öröklődések erőltetése és megszakítása folyamán egy idő után már nem látjuk át, hogy bizonyos csoportházirend elemek miért nem hajtódnak végre, vagy honnan kapunk bizonyos beállításokat. A csoportházirend struktúrájának tervezése során törekedni kell arra, hogy a fentieket csak kivételes, valóban indokolt esetekben használjuk.

A csoportházirend egyik fontos eleme az Intellimirror technológia. Ez a technológia lehetővé teszi, hogy egy számítógép meghibásodása esetén, egy új üzembeállítása után a rendszer telepítése automatikusan megtörténjen. Ennek három része a következő:

- User Data Management: Minden olyan fájl, dokumentum, táblázat elérhetővé tétele, amely a felhasználó napi munkájához tartozik. Ez csoportházirend szinten azt jelenti, hogy a felhasználó számítógépét úgy állítjuk be, hogy pl. a munkáját egy központi megosztásból végezze, amelyen mi rendszeres mentést végzünk.
- Software Installation and Maintenence: Megtehetjük, hogy egy alkalmazást hozzárendelünk (assign) a felhasználóhoz, amely akkor települ, amikor a felhasználónak valóban szüksége van rá. Megtehetjük azt is, hogy egy alkalmazást kiadunk a felhasználó részre, amit, amikor szüksége van rá, önállóan telepíthet. Az így publikált alkalmazásokat a Control Panel Programs and Features részben találjuk meg.
- User Settings Management: Itt visszaállíthatjuk a felhasználó korábbi beállításait. Csoportházirenddel szabályozzuk a felhasználó, illetve a számítógép beállításait. Itt olyanokat találunk, mint pl.:
    - Felhasználó szinten: Internet Explorer kedvencek, Outlook Express, Outlook beállítások.
    - Számítógép szinten: Energiagazdálkodási lehetőségek, számítógép beállításai a fájlok offline használatára vonatkozóan, személyes tűzfal beállítások.

Az operációs rendszer automatikus telepítésére használható a Windows Deployment Services (WDS) vagy a System Center termékcsalád Configuration Manager alkalmazás.

10.1 Group policy editor felépítése

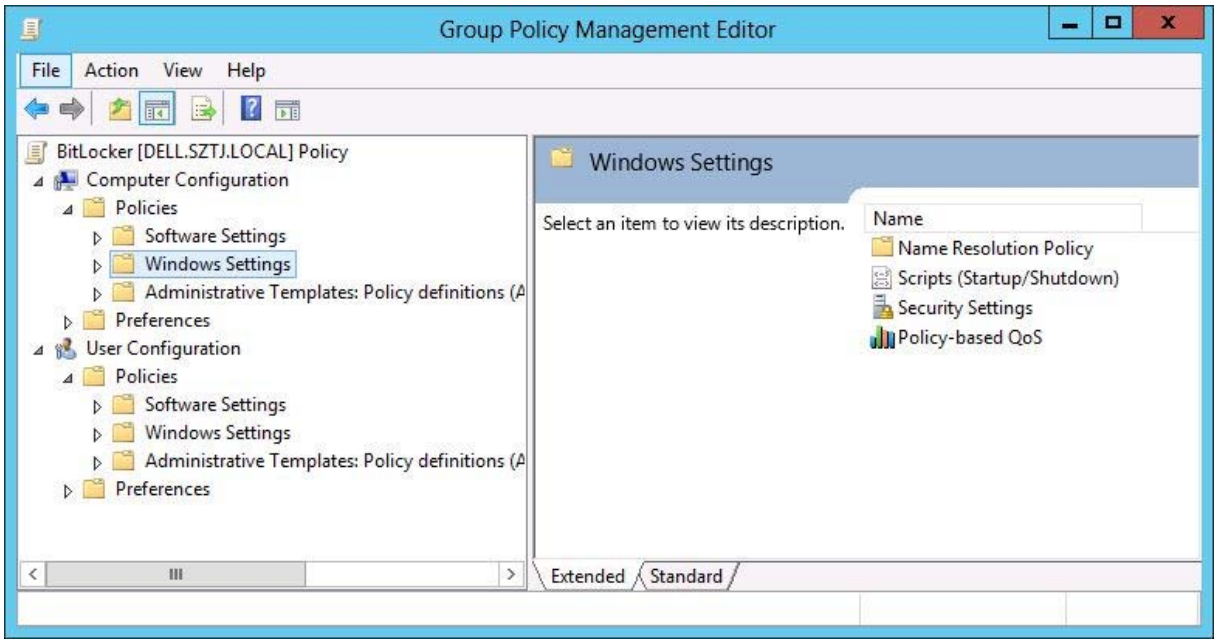
A csoportházirendek két fő részből állnak: az egyik a számítógépre, a másik a felhasználóra vonatkozik. Ezek a következők:

- Computer Configuration
- User Configuration

Mind a Computer, mind a User Configuration-ben megtaláljuk a következőket:

- Software Settings: Ennek a segítségével alkalmazásokat tudunk kiküldeni a kliensekre, alapértelmezés szerint .msi csomagként, de van lehetőség .exe kiterjesztésű fájl terjesztésére is. A programok telepítése csak akkor történik, amikor a felhasználónak erre ténylegesen szüksége van. Ugyanakkor itt megtehetjük, frissíthetjük az alkalmazásokat, de akár el is távolíthatjuk.

- Windows Settings: Itt tudjuk beállítani a Folder redirection-t, scripteket és biztonsági beállításokat.
- Administrative Templates: Operációs rendszer és komponensei, alkalmazások beállításai.
- Preferences: A Group Policy Preferences a Windows Server 2008-as verziójában mutatkozott be először, nagyrészt azon feladatok ellátására szolgál, amelyekre a korábbiakban bejelentkezési és rendszerindítási parancsfájlokra volt szükségünk. A felhasználók, a többi házirenddel ellentétben szabadon megváltoztathatják a Preferences-ben kapott konfigurációt.



Ha változtatni szeretnénk az egyik házirend elemén, akkor kattintsunk rá kétszer az egérrel, majd lépjünk az "Engedélyezve" (Enabled) rádiógombra. Ha a "Letiltva" ("Disabled") rádiógombot jelöljük ki, akkor kikapcsolást (Disabled) valósítunk meg. A "Nem konfigurált" (Not Configured) beállításnak akkor van jelentősége, ha több csoportházirend öröklődés van beállítva, ezen beállítás mellett ez a házirend nem fogja befolyásolni az öröklődést.

10.2 Group policy frissítése

A csoportházirendek frissítése a következő esetekben történik meg:

- A számítógép elindul
- A felhasználó bejelentkezik
- Alkalmazás vagy a felhasználó kér egy frissítést
- A csoportházirend automatikusan frissítődik alapértelmezett vagy módosított beállítások szerint.

A csoportházirend-kliens „pull” modell alapján dolgozik. Alapértelmezésben a csoportházirend a tartományvezérlők esetében 4 percenként, számítógépek esetében minimum 90, maximum 120 percenként hajtódik végre automatikusan. A vállalat aktív klienseinek a számától függően az időintervallumot kisebbre is vehetjük, stílusosan mindezt csoportházirendből. A Computer Configuration\Administrative Template\System\Group Policy alatt találhatjuk a Set

group policy refresh interval for computers lehetőséget. Itt a választási lehetőség elég széles, hiszen 0-tól 44641 percig állíthatunk. A 0 tulajdonképpen azt jelenti, hogy 7 másodpercenként frissítődik a csoportházirend. Bár a kliensek számától erősen függ, de nem érdemes nagyon rövid időintervallumot használni a hálózat terhelése miatt.

A Group policy frissítése a kliens oldalról kikényszeríthető, ha a megadott automatikus végrehajtást nem szeretnénk kivárni. A parancs neve gpupdate, és mind a számítógép, mind a felhasználói részt frissíti. PowerShellben használhatjuk az Invoke-Gpupdate parancsot.

10.3 Biztonsági beállítások

10.3.1 Auditálás

A csoportházirendben lehetőségünk van a felhasználók tevékenységeit naplózni. Az event logban alapértelmezetten beállítva már megtalálhatjuk a security log-ot, viszont elképzelhető, hogy sokkal több információkra van szükségünk, mint amit ott megtalálunk. Milyen esetek fordulhatnak elő egy vállalat életében, amelyeket érdemes lehet naplózni?

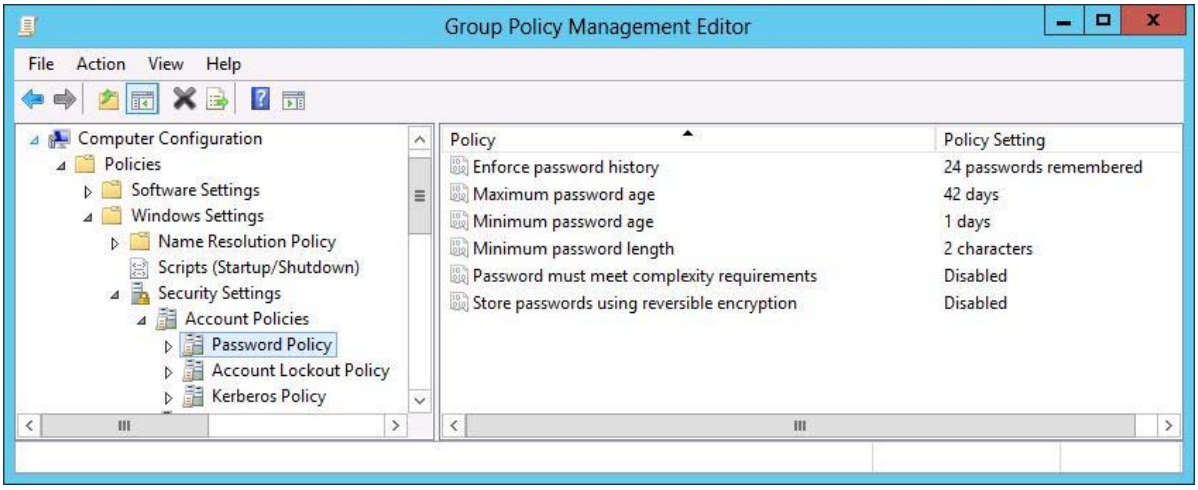
- Egy rendszergazda, aki módosítja az adatokat egy fájlszerveren lévő pénzügy megosztásban.
- Egy felhasználó, aki egy titkos mappát nyit meg és módosít.
- Egy felhasználó, aki többször próbál belépni egy szerverre, de hozzáférés hiányában ezt nem tudja megtenni.

Navigáljunk el a Group Policy Management-ben a következő útvonalra: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit policy. Itt a következő fontosabb lehetőségeket találjuk:

- Audit account logon events (fiókbejelentkezés naplózása): Akkor naplóz, amikor a hálózatunkban történt egy sikeres vagy sikertelen ki- vagy bejelentkezés.
- Audit accounting management (fiókkezelés naplózása): fiókok vagy csoportok létrehozása, módosítása, törlése, átnevezése, engedélyezése, tiltása, jelszavak beállítása vagy megváltoztatása.
- Audit object access (objektum-hozzáférés naplózása): A rendszer objektumai a fájlok, mappák, nyomtatók stb. Minden objektum hozzáféréssel kapcsolatos ténykedés eseményt vált ki, ami bejegyzésre is kerül a naplóba.
- Audit system events. (rendszeresemények naplózása): Az operációs rendszer elindulása, leállása és minden rendszerbiztonsági esemény feljegyzésre kerül.

10.3.2 Felhasználói fiókházirend

A felhasználói fiókházirendet (Account policy) tartományi szinten határozzuk meg. Az adott policy áll a felhasználók jelszavának házirendjéből, zárolás és kerberos házirendből. Windows Server 2012 a Fine-grained password segítségével több felhasználói jelszó házirendet határozhatunk meg. Ezeket a beállításokat ajánlatos közvetlenül a felhasználóra vagy a globális csoportra érvényesíteni nem pedig a tartományra. A beállításokat itt találjuk a Group Policy Management Console-ban: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies.



10.3.3 Korlátozott csoportházirend

A korlátozott csoportházirendbe (Restricted Groups Policy) lokális vagy globális csoportok tagjaira is tudunk házirendet rendelni. A csoportok tagságát általában a rendszergazda adja meg, de a Restricted Group házirenddel meg tudjuk határozni, hogy mely csoportok azok, amelyeknek tagságát nem lehet megváltoztatni. Amint érvényre juttatjuk a házirendet, a csoportba nem lehet tagokat felvenni, vagy a meglévőeket eltávolítani.

A beállítást itt találjuk: Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups.

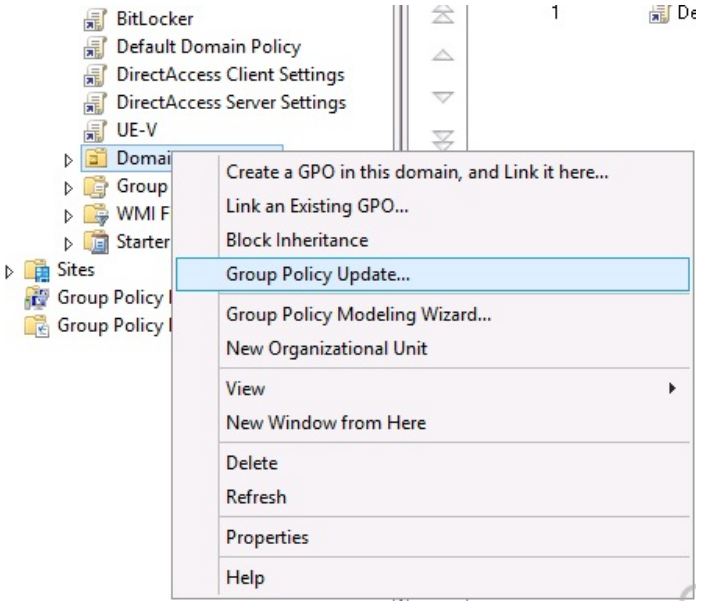
10.3.4 Windows tűzfal házirend

A felhasználók számítógépén lévő Windows tűzfalat tudjuk szabályozni. Itt megadhatjuk a be- és kimenő forgalmi szabályokat, meghatározhatjuk a kommunikációs beállításokat (pl. IPSec). A beállításokat itt alkalmazhatjuk: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security.

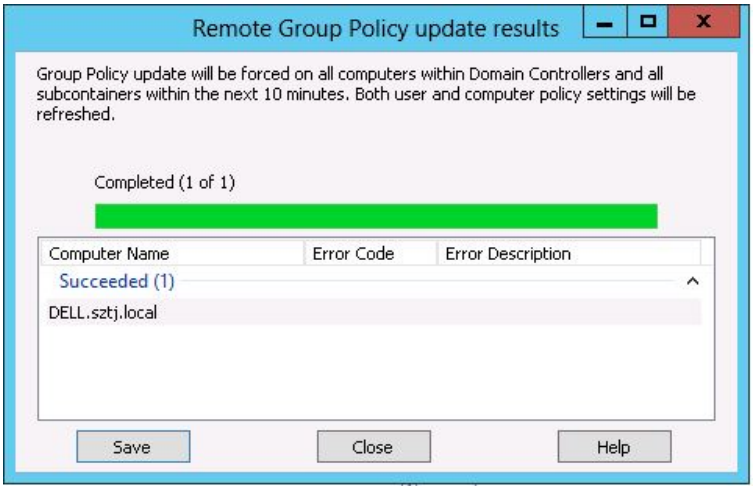
10.4 Újdonságok

Ahogy eddig szinte minden Windows Server 2012 komponensnél, itt is történtek változások, melyek mellesleg igen hasznosak.

Az előző változatban, ha létrehoztunk egy csoportházirend objektumot, azt nem tudtuk elérni, hogy ez a közeljövőben végre is hajtódjon. Jelenleg is az operációs rendszerek részét képezi a `gpupdate` parancs, amelynek segítségével ki tudjuk „erőszakolni” a kliens gépen a policy végrehajtását, viszont ez olyankor problémát okozhat, ha egy szervezeti egység (OU) több ezer felhasználót és/vagy számítógépet tartalmaz. Ennek a problémának a megoldására jött létre a Force Update, amely 10 percen belül végrehajtja az adott szervezeti egységre kiadott csoportházirendet. A parancs a Group Policy Management Console-ból érhető el, jobb klikk a szervezeti egységre és előtűnő menüből már láthatjuk is a lehetőséget.



A parancs végrehajtásának hatására láthatjuk, hogy az adott szervezeti egységben lévő házirend végrehajtódott-e a benne lévő összes objektumon. A képernyőn megjelenő listát elmenthetjük egy csv fájlba.



Ugyanezt a lehetőséget megtaláljuk PowerShellből is. A Windows Server 2012-ben új Invoke-Gpupdate paranccsal lehetővé válik távoli számítógépek házirendjének frissítése. A következő utasítás frissíti a COMPUTER-02 nevű számítógépet, annak is csak felhasználói házirendjét:

```
Invoke-GPUpdate -computer COMPUTER-02 -Target user
```

A másik újdonság a Status detection, ezt szintén a Group Policy Management Console-ban érjük el. Csak válasszuk ki a tartományunkat, és a jobb oldalon megjelenő status alatt a Detect Now-t megnyomva, a tartományvezérlőnk nyit egy kommunikációt az összes többi tartományvezérlő felé azzal a céllal, hogy megvizsgálja a SYSVOL könyvtár tartalmát és replikáció sikerességét.

Természetesen az új csoportházirendben számos Windows 8 policy-t is találunk. Így az új Windows 8 számítógépeinket is tudjuk szabályozni a csoportházirend alól.

A Group Policy Result kibővült, és a hibajavítások egyik fő célpontja lesz. Ha egy felhasználóra vagy egy számítógépre nem hajtódik végre egy házirend, itt könnyen beazonosíthatjuk a hiba okát. A Group Policy Result varázsló megkérdezi a számítógép, majd a felhasználó nevét, és a rájuk érvényes csoportházirendeket kiértékeli. Az összefoglalón csak a legfontosabb státuszok jelennek meg, ellenben a Details-en már alaposabb vizsgálatra van lehetőségünk. A Component Statusban láthatjuk, hogy az egyes összetevők, mint pl. a Group policy infrastruktúra, a registry vagy security settings, a vonal sebességének függvényében mennyi idő alatt hajtódtak végre, illetve mikor történt az utolsó végrehajtás. Events fül egy csoportházirend esemény napló, amelyben az idő tekintetében láthatjuk a csoportházirendek végrehajtásának sikerességét mind számítógép, mind felhasználó tekintetében.

Az AppLockert már ismerhetjük a Windows Server 2008 R2-es verzióból. Az AppLocker segítségével tudjuk szabályozni, hogy a vállalatunknál milyen programokat (executable rules), telepítési forrásokat (Windows Installer rules), PowerShell, Visual Basic, JavaScript scripteket (Script rules) tudunk futtatni.

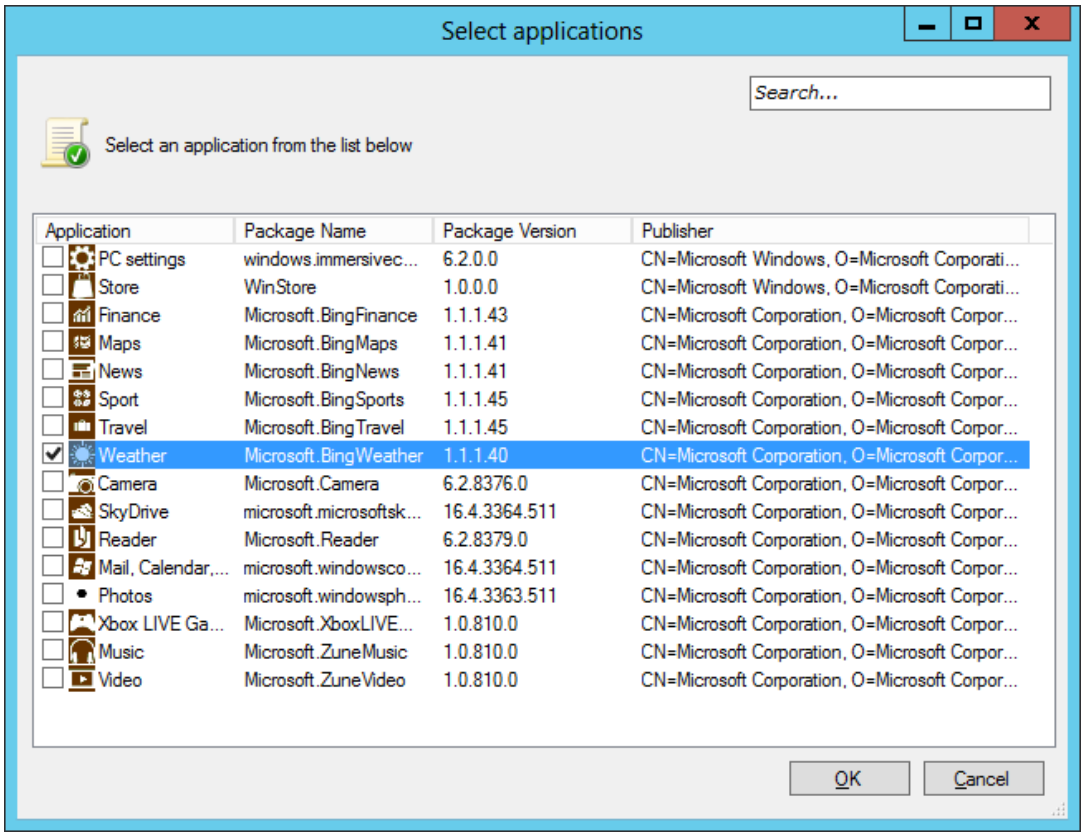
Szűrési lehetőségünk adódik a következőkre:

- Gyártó neve
- Termék neve
- Fájl neve
- Fájl verziója

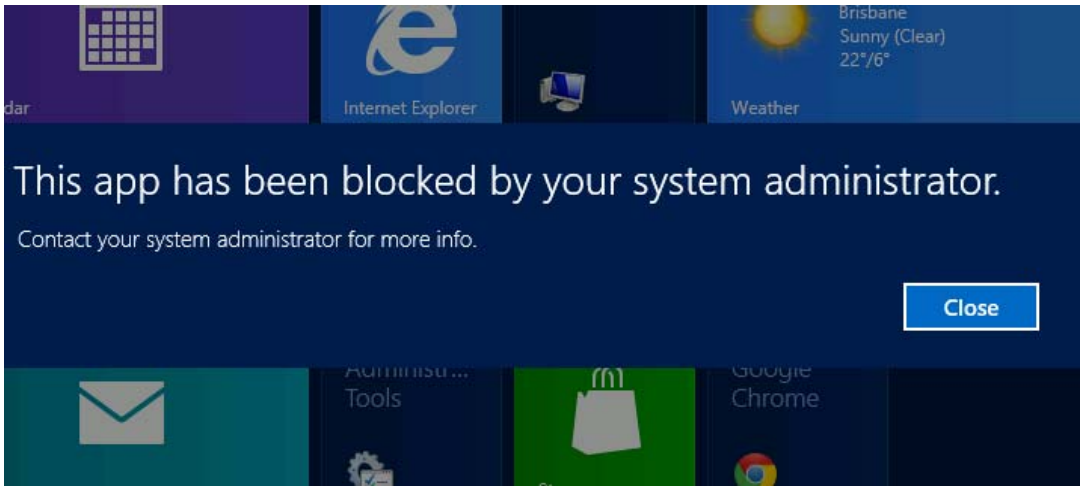
Szabály végrehajtása

- Engedélyező szabály
- Tiltó szabály
- Kikényszerítés, vagy csak a naplózás bekapcsolása

A Windows Server 2012-ben az említett három lehetőségen kívül találunk egy negyediket is: Packaged App Rules. Ennek segítségével tudjuk engedélyezni vagy éppen tiltani a Windows App Store-ról letöltött alkalmazástípusokat. A varázslóban meg kell adnunk a felhasználók körét, az engedélyező vagy tiltó szabályt. Referenciaként meg kell adnunk egy aláírt appx telepítő referencia fájlt, amely alapján a csoportházirend létrehozza a szükséges szabályt. A házirendet itt találjuk Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\Applocker.



A Bing Weather telepítését és indítását tiltjuk. Ha már telepítve van a gépünkre, akkor indításakor a lenti üzenetet kapjuk.



11 Távelérés

A felhasználók munkastílusa alapvetően változott meg az elmúlt években. A távmunka, a több eszköz használata, és az állandóan úton lévő felhasználók folyamatos hozzáférést igényelnek a cég belső erőforrásaihoz, legyen az kis- közép- vagy nagyvállalat. A Windows Server 2008 R2-ben bemutatott DirectAccess ezt a feladatot hivatott megvalósítani, a Windows Server 2012-ben pedig kiköszörültek minden olyan hiányosságot vagy bonyolultságot, ami miatt a 2008-as rendszerben nem álltunk neki a bevezetésnek.

Természetesen a Windows Server 2012-ben a tradicionális VPN megoldások is elérhetőek, mint a PPTP, L2TP, SSTP vagy az IKEv2. Ezek a szolgáltatások viszont kevesebb funkcióval bírnak, ezen keresztül a kliens gépek nem menedzselhetőek, nem esik rájuk csoportházirend, nem épül fel a kapcsolat automatikusan a gép bekapcsolásakor, stb.

Az egységes üzemeltetői felületen, egy helyen konfigurálhatjuk a DirectAccess és a VPN beállításokat is.

11.1 DirectAccess

A Windows Server 2012-ben található DirectAccess szolgáltatás segítségével a távoli számítógépeken felhasználók beavatkozása nélkül, a kliens bekapcsolásakor automatikusam bejelentkezik a központi kiszolgálóra, elérik az infrastruktúraszolgáltatásokat (AD, DNS, Group Policy, stb.) Ez üzemeltetői oldalról könnyíti meg a dolgunkat, hiszen a frissítések, csoportházirend beállítások kikerülnek a távoli gépekre, és menedzselhetőek a megszokott felügyeleti rendszerrel, pl. SCCM. A DirectAccess alapja az IPv6 protokoll, így minden olyan alkalmazás képes DA-n keresztül kommunikálni, ami támogatja az IPv6-ot

11.1.1 A DirectAccess a következő szolgáltatásokat nyújtja:

- Azonnali kapcsolódás a cég belső hálózatához, ahogy a kliens Internetre csatlakozik
- Többféle protokollon képes csatlakozni, akár HTTPS-en is, ahol az IPv6-os forgalmat HTTPS alagútba csomagoljuk. Ez a megoldás létezett a Windows Server 2008-ban is, de teljesítmény-problémák miatt nem javasolták. A 2012-es verzióban ezeket a problémákat kijavították, hangoltak a teljesítményén, így kifejezetten javasolják az IPv6-HTTPS módot
- IPSec alapú titkosítás
- Központilag menedzselhető távoli számítógépek
- Teljes körű Network Access Protection (NAP) támogatás

11.1.2 Újdonságok a Windows Server 2012-ben

Ha üzemeltünk be DirectAccess szolgáltatást a Windows Server 2008-ban, akkor látni fogjuk, hogy a 2012-es verzió mennyi könnyítést hozott a bevezetésben:

- DA és VPN együttműködés.
- Továbbfejlesztett naplózási és monitorozási felület a DirectAccess konzolon
- Server Core és PowerShell támogatás
- Egyszerű telepítés varázsló, ami minden komponenst beállít
- Egy hálózati kártyával és 1 külső IP címmel is működik, vagy akár NAT-olt hálózat mögött is.

- A belső hálózaton nem kötelező IPv6-ot használnunk
- Több telephelyes környezetnél a Windows 8-as kliensek automatikusan a legközelebbi végpontra csatlakoznak. (a Windows 7-es klienseknél kézzel kell megadnunk a megfelelő végpontot)

11.1.3 DA komponensek

A DirectAccess infrastruktúra kiépítéséhez a következő komponensekre lesz szükségünk:

- DA Server: bármelyik, tartományba léptetett Windows Server 2012. Ez a gép lesz a hitelesítési kiszolgáló, illetve az IPSec csatorna végpontja
- DA kliens: bármelyik Windows 8, Windows 7 Enterprise, vagy Windows 7 Ultimate Edition-t futtató kliensgép
- Network Location Server: egy webszolgáltatás, ami alapján a kliensek eldöntik, hogy a belső vagy a külső hálózaton tartózkodnak. Ha HTTPS-el elérik az NLS kiszolgálót, akkor belső hálózaton vannak, és kikapcsolják a DA szolgáltatást, ha nem érik el, akkor megpróbálják felépíteni a DA csatornát.
- Belső erőforrások: bármilyen, IPv6-ot támogató belső kiszolgálót megadhatunk, amit a DA kliensek elérnek. Ha az erőforrások nem támogatják az IPv6-ot, a Windows Server 2012 képes átfordítani a protokollt NAT64 segítségével, illetve a névfeloldást is DNS64-el
- Active Directory: A DA használatához mindenképpen AD-re van szükségünk, a minimum tartományi működési szint Windows Server 2008 R2. A 2012-es DA támogatja a több tartományos működést is.
- Csoportházirend: a kliens beállításokat csoportházirenden keresztül tudjuk kiküldeni. A DirectAccess beállítása varázsló létrehozza a szükséges csoportházirend-objektumokat, mind a kliensek, mind a kiszolgálók számára.
- PKI: nem kötelező komponens, de ha beüzemeljük, egyszerűsíthető a tartományi hitelesítési folyamat.
- DNS: A DNS kiszolgálónknak legalább Windows Server 2008R2-nek kell lennie
- NAP kiszolgáló: ha szeretnénk a kliens gépek egészségügyi állapotát ellenőrizni DA csatlakozáskor, esetleg bizonyos biztonsági beállításokhoz kötni a csatlakozást, javasolt a NAP infrastruktúra használata.

11.1.4 NRPT

Ahhoz, hogy el tudjuk választani a belső hálózati és az Internetes kommunikációt a kliens gépeinken, Name Resolution Policy Table-t (NRPT) kell szerkesztenünk. Ez a szolgáltatás előre meghatározott házirend alapján szétválasztja a DNS kéréseket külső és belső kérésekre. Ha a DNS kérés belső névre hivatkozik, akkor a cég belső hálózatán lévő DNS server válaszol, és a forgalom is a DA csatornára terelődik. Ha a kérés nincs rajta az NRPT táblán, akkor a kliens az Internet-kapcsolat DNS kiszolgálóját kérdezi meg.

11.1.5 Kliensek csatlakozása

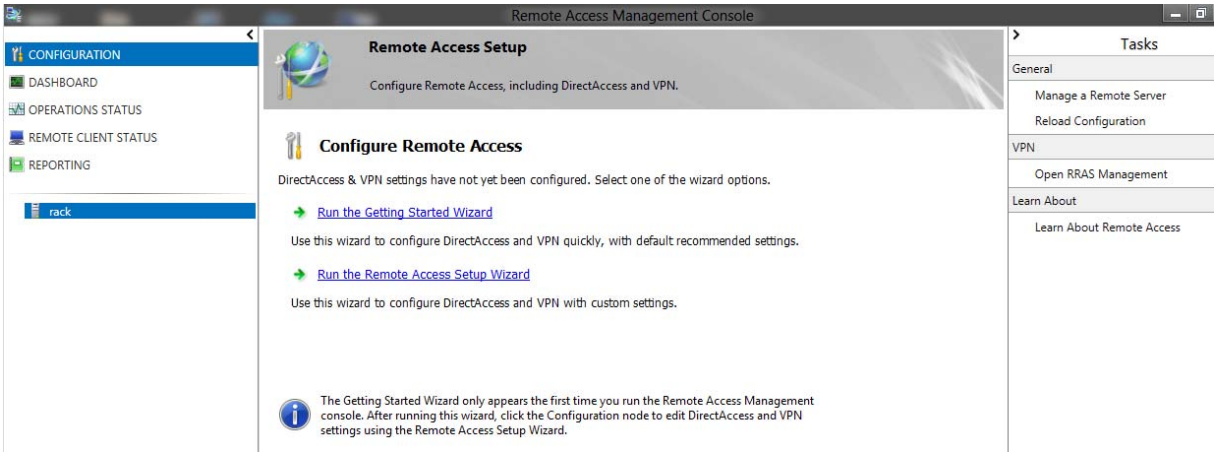
Amikor a kliensek csatlakoznak az Internethez, először megpróbálják eldönteni, hogy céges, vagy külső hálózaton vannak: megpróbálják elérni az NLS URL címet. Ha nem éri el az NLS címét, akkor elindítja az NRPT és DA-hoz kapcsolódó IPSec szabályokat, amellyel csatlakozik a belső hálózathoz. Csatlakozás után megkeresi a tartományvezérlőt, DNS kiszolgálót, majd bejelentkezik a tartományba. Ezután a felhasználó, függetlenül attól, hogy belső vagy

külső hálózaton van, be tud jelentkezni a tartományba, lefut a bejelentkezési parancsfájl, érvényesül a csoportházirend, felveszi a kapcsolatot az infrastruktúra kiszolgálókkal, stb.

11.1.6 DirectAccess telepítése, konfigurálása

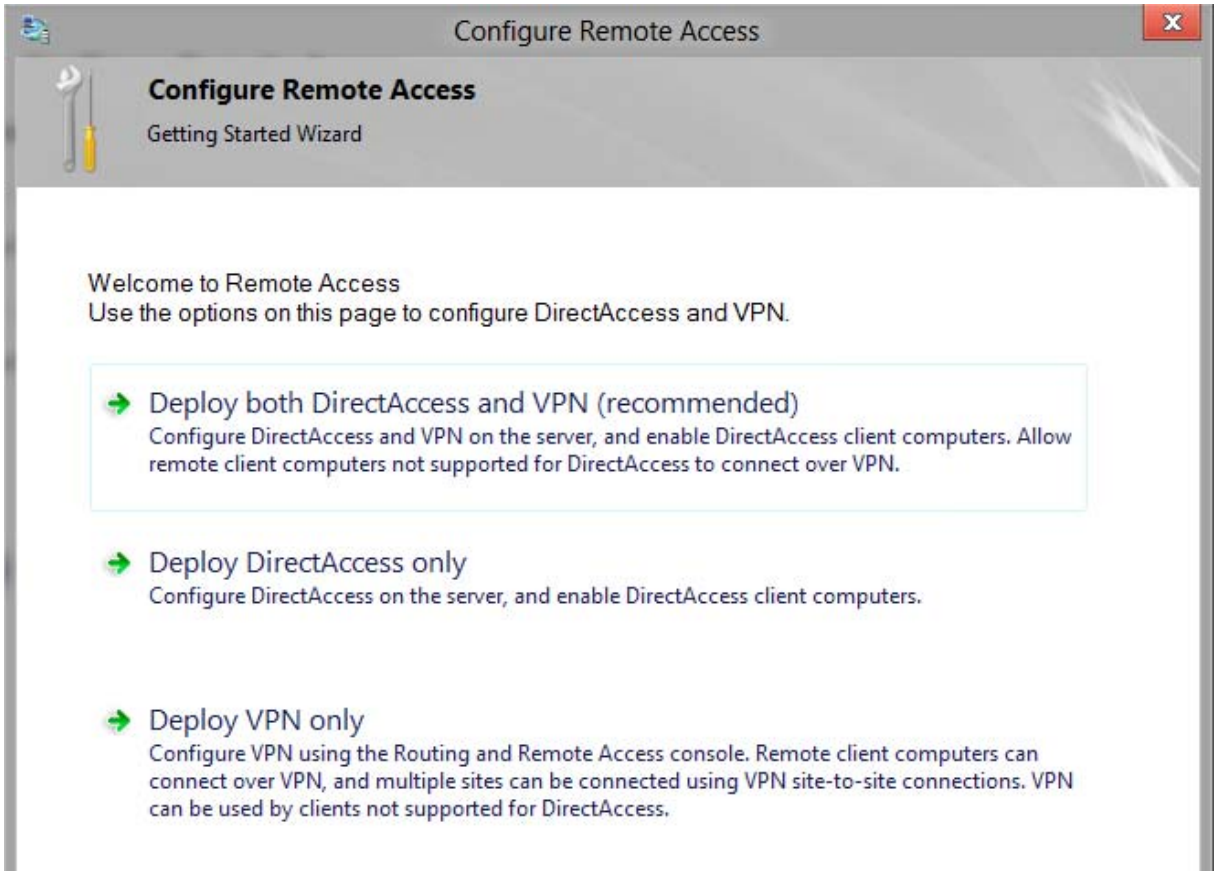
A DirectAccess infrastruktúra kiépítéséhez tehát kiszolgáló oldalon szükségünk lesz egy Windows Server 2012-re, felkonfigurált AD-vel (lehet tartományvezérő vagy tartománytag is), DNS-el, kliens oldalon pedig Windows 8, Windows 7 Ultimate, vagy Enterprise verziókra. Tanúsítvány kiszolgáló csak abban az esetben kötelező, ha NAP infrastruktúrát is szeretnénk használni. Az Active Directoryban célszerű létrehozni egy számítógép-csoportot azon gépek számára, amelyeket be szeretnénk engedni a DA kiszolgálónkon. A tűzfalunkon pedig publikálni kell a 443-as és 80-as portokat a DA szerver felé.

A konfigurálás a Server Manager/Add Roles menüjében kezdődik. Telepítés után indítsuk el a Remote Access Management Console-t:

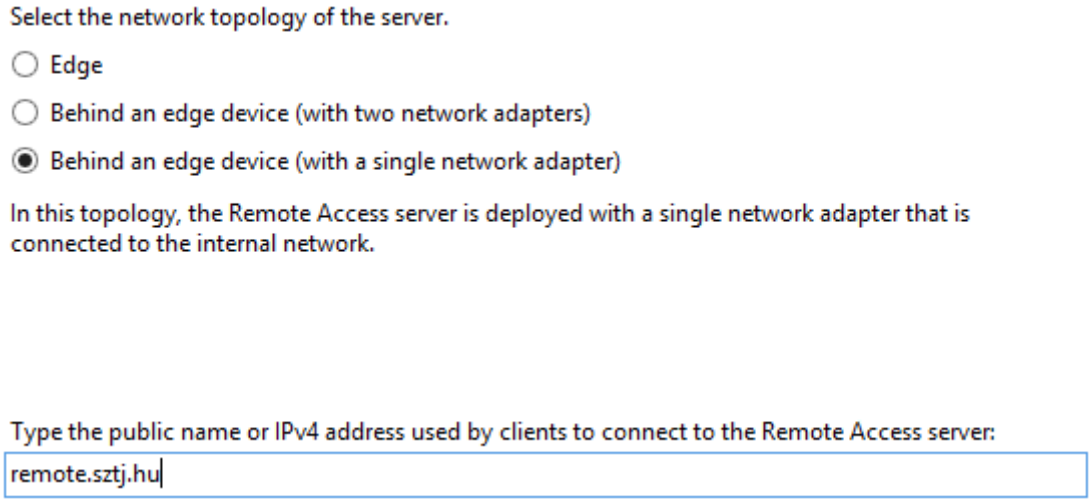


A Getting Started Wizardban három lehetőségünk van:

- DirectAccess és VPN konfigurálása, így minden kliensünk be tud jelentkezni távolról, a Windows bármelyik verzióját használva
- Csak DirectAccess
- Csak VPN



Válasszuk a DirectAccess és VPN beállítást, majd az előfeltételek ellenőrzése után válasszuk ki a számunkra megfelelő topológiát:



Az Edge topológiánál két hálózati kártyára van szükségünk, egy Internetes csatlakozással, egy pedig a belső hálózat felé.

A második opciónál a DA szerver tűzfal mögött van, egyik lába a belső hálózatra, a másik a DMZ hálózatra csatlakoztatva

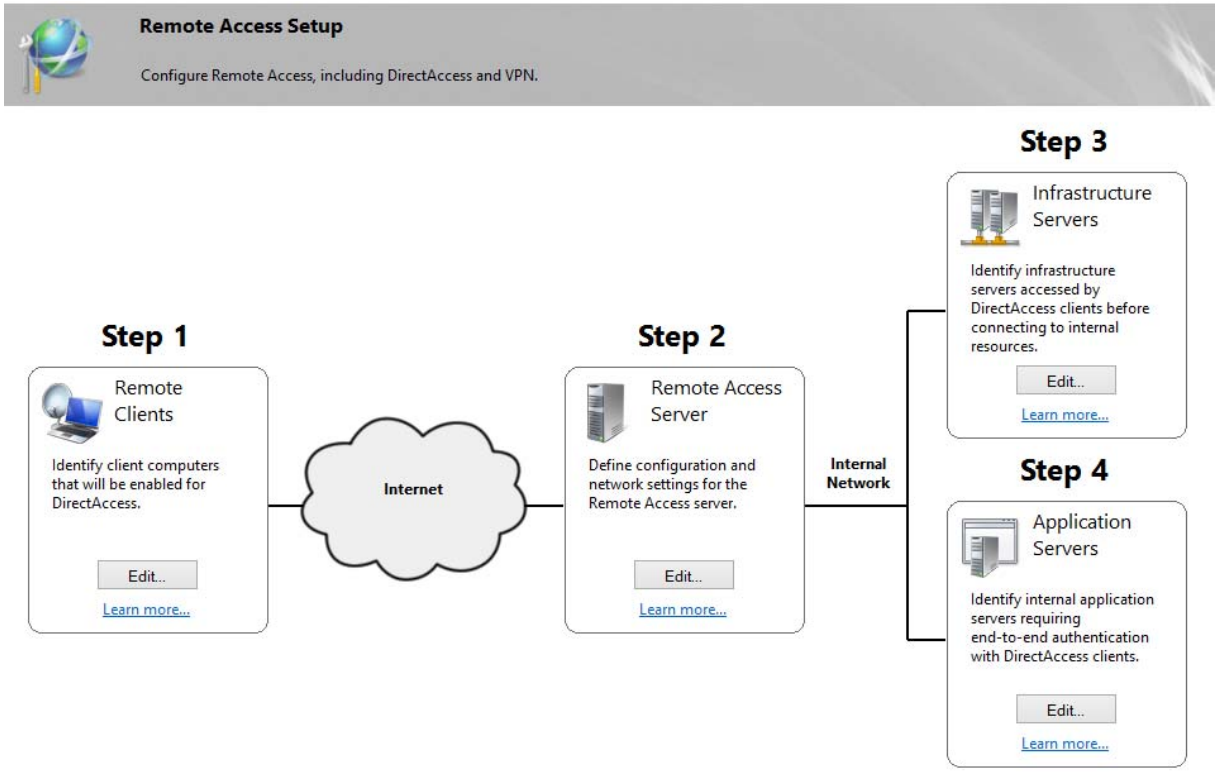
A harmadik opció egy hálózati kártyát és egy IP címet igényel, itt viszont csak IP-HTTPS technológiát használhatunk.

Ha kiválasztottuk a számunkra megfelelő topológiát, meg kell adnunk a kiszolgáló külső nevét, ahová az Internetes kliensek csatlakoznak. Egy, erre a névre szóló tanúsítványt a rendszer automatikusan legenerál, majd csoportházirendből kiküldi a kliensgépekre, mint megbízható tanúsítvány.

Az egyszerű beállítási varázsló ezzel készen is van, a következő beállításokat végzi el:

- létrehoz 2 házirendet, a kliens és a kiszolgáló beállítására, megadva az NRPT, NLS beállításokat
- Beállítja a távelérési jogosultságot a „Domain Computers" tartományi csoportra, ez később módosítható, ha az általunk létrehozott csoportot szeretnénk engedélyezni
- A DA-t nem támogató eszközök számára engedélyezi a VPN hozzáférést, Windows hitelesítéssel. Alapértelmezésként a VPN kliensek a belső DHCP kiszolgálótól kapnak IP címet.
- Beállítja az infrastruktúra kiszolgálókat, amelyek a hitelesítést fogják végezni

A konfigurálás befejezése után egy összefoglaló képernyőt kapunk a DA infrastruktúránkról, illetve módosíthatunk is a beállításainkon:



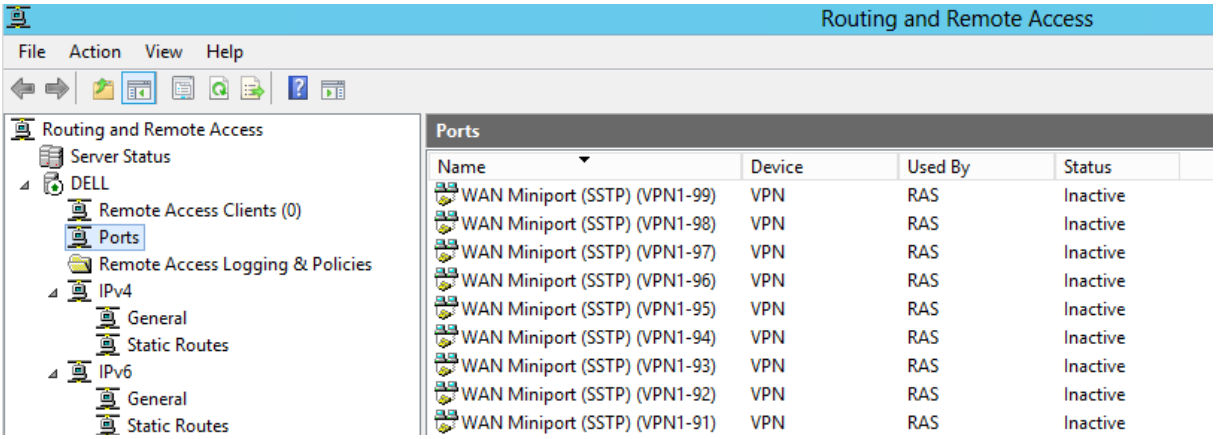
11.2 VPN Kiszolgáló

A DirectAccess mellett a Remote Access kiszolgálónk alkalmas VPN kapcsolatok kezelésére is, legyen az PPTP, L2TP, SSTP vagy IKEv2 protokoll. Ezeket a távelérési protokollokat használhatjuk akár Windows XP-n, Windows 7-en vagy 8-on is, illetve kiépíthetünk telephelyek közötti Site-to-Site VPN kapcsolatot. Ha már telepítettük a Remote Access Szerepkört, akkor a Server Managerből indítsuk el a Routing and Remote Access-t:

Az RRAS konzolon felügyelhetjük a VPN kiszolgálónkat:

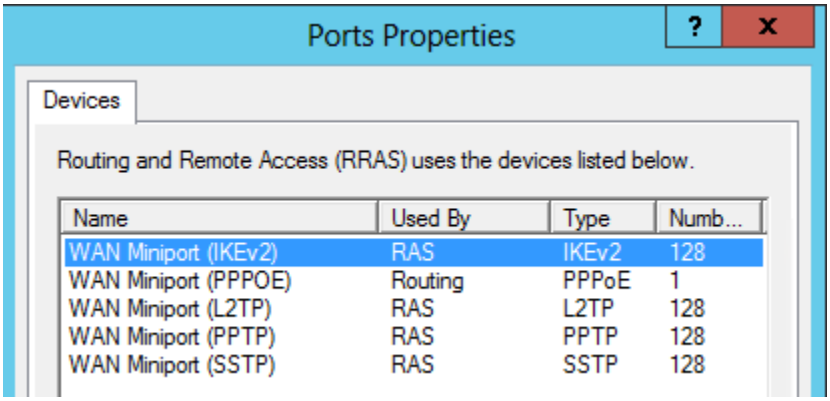
- Távelérési protokollokat engedélyezhetünk/tilthatunk
- IP beállításokat definiálhatunk
- Felügyelhetjük a csatlakozott ügyfeleket

A felhasználók hozzáférését viszont nem itt, hanem a Network Policy Serveren vagy az Active Directoryban tudjuk szabályozni, de erről majd később. Először lássuk az RRAS üzemeltetési felületét:



A Remote Access Clients menüben láthatjuk az aktuálisan csatlakozott ügyfeleinket, illetve meg tudjuk szakítani a kapcsolatokat

A Ports résznél láthatjuk, hogy ha a Remote Access Server konfigurálásakor DirectAccess és VPN beállítást választottuk, akkor az RRAS engedélyezte az összes VPN protokollt, mindegyik protokollra maximum 128 egyidejű kapcsolattal:



Ezt érdemes korlátozni az általunk igényelt protokollokra, illetve a kapcsolatok számát is az általunk használtra. A Windows Server 2012-ben támogatott távelérési protokollok a következők:

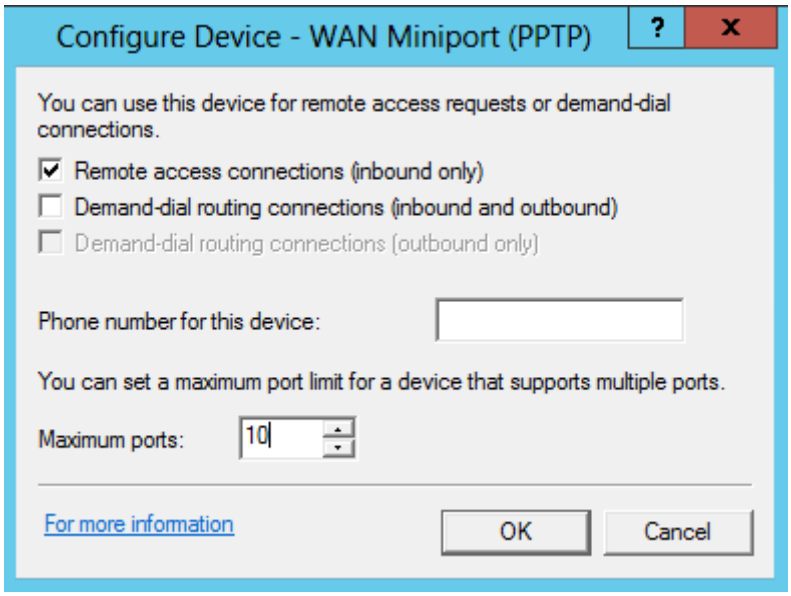
- PPTP: Egyszerű, közepesen biztonságos távelérési protokoll, a TCP 1723-as portot használja. Hitelesítése és titkosítása is korlátozott, ezért általános célokra használhatjuk, de magasabb biztonsági szinten érdemes kerülni. Speciális beállítást nem igényel, és telephelyek összekötésére is alkalmas.
- L2TP alapesetben nem titkosítja a forgalmat, viszont bármilyen titkosítással felvértezhetjük. Általában IPSec-el titkosítjuk a forgalmat, akár tanúsítvány alapon, akár előre megosztott kulccsal. A Windows XP-től támogatott protokoll.

- Az SSTP a forgalmat HTTPS alagútban viszi át a két végpont között a 443-as TCP porton, így bárhol tudjuk használni, ahol a PPTP és L2TP technológiákat esetleg korlátozzák. SSL titkosítást használ, hitelesítéshez pedig konfigurálhatunk akár magasabb biztonságú EAP-TLS-t is.
- Az Internet Key Exchange version 2 (IKEv2) IPSec alagutat használ az 500-as UDP porton. Főleg olyan helyeken használjuk, ahol a távoli felhasználók sűrűn váltanak átviteli közeget, WIFI-ről mobilinternetre, vagy kábeles kapcsolatra. Az IKEv2 MOBIKE támogatása miatt képes ezeket a változásokat észrevétlenül kezelni, és folyamatos hozzáférést biztosítani.

A fenti VPN protokollok használatához a tűzfalon a következő portokat kell engedélyezni:

- A PPTP eléréséhez a TCP 1723-as portját kell konfigurálnunk
- Az L2TP használatához az UDP 500-as, UDP 1701-es, UDP 4500-as portokat, és az 50-es IP opciót kell engedélyeznünk
- Az SSTP használatához mindössze a 443-as portot kell kinyitnunk
- Az IKEv2 az UDP 500-as portot használja

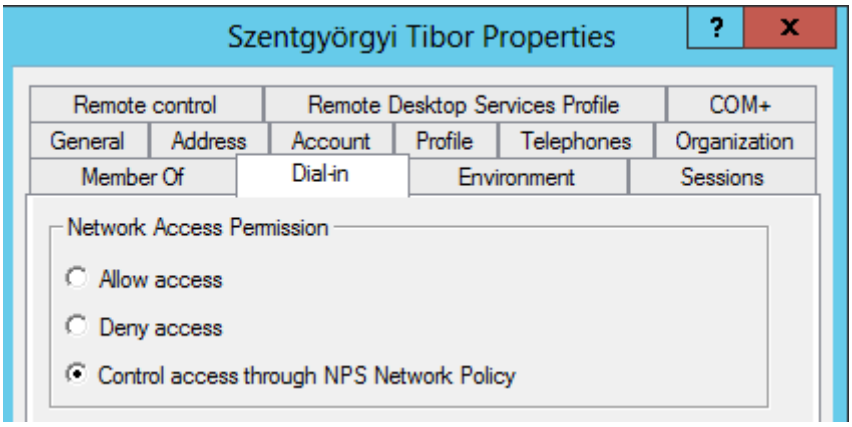
Ha megnézzük egy adott protokoll beállításait, a következő beállításokkal találkozunk:



Megadhatjuk, hogy a protokollt milyen irányban szeretnénk használni, távelérésre, vagyis bejövő hívások fogadására, mindkét irányba, vagy csak tárcsázni szeretnénk kifelé. A PPPoE protokollt például csak kifelé tárcsázásra tudjuk használni, pl ADSL kapcsolatnál. Az SSTP protokoll viszont csak bejövő hívások fogadására alkalmas, ezért is nem lehet telephelyek közötti VPN kapcsolatot kiépíteni, csak PPTP vagy L2TP/IPsec csatornán.

11.2.1 Felhasználók engedélyezése

Miután engedélyeztük a VPN hozzáférést, és beállítottuk a használni kívánt alagút-protokollt, a felhasználóknak engedélyeznünk kell a távelérést. Ezt megtehetjük felhasználónként is az Active Directory Users and Computers részben is, ha a felhasználó Dial-in hozzáférését engedélyezzük:

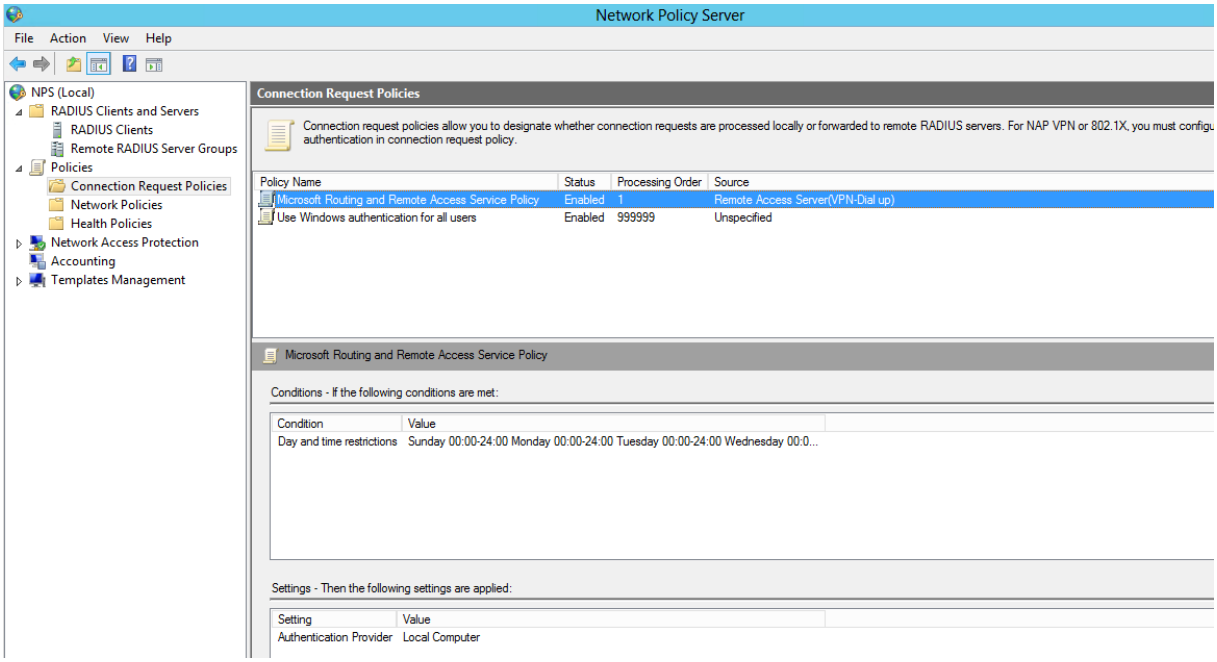


A Network Access Permission résznél három beállítás közül választhatunk:

- Allow Access: a felhasználó hozzáférést kap a VPN kiszolgálóhoz, függetlenül a távelérési házirendektől. Ez a beállítás nem javasolt, mert üzemeltetési szempontból nehezen nyomon követhető, hogy kinek van hozzáférése.
- Deny Access: a felhasználó explicit tiltást kap, függetlenül a házirendektől.
- Control access through NPS Network Policy: A hozzáférést távelérési házirendből, központilag szabályozzuk.

11.2.2 Házirendek

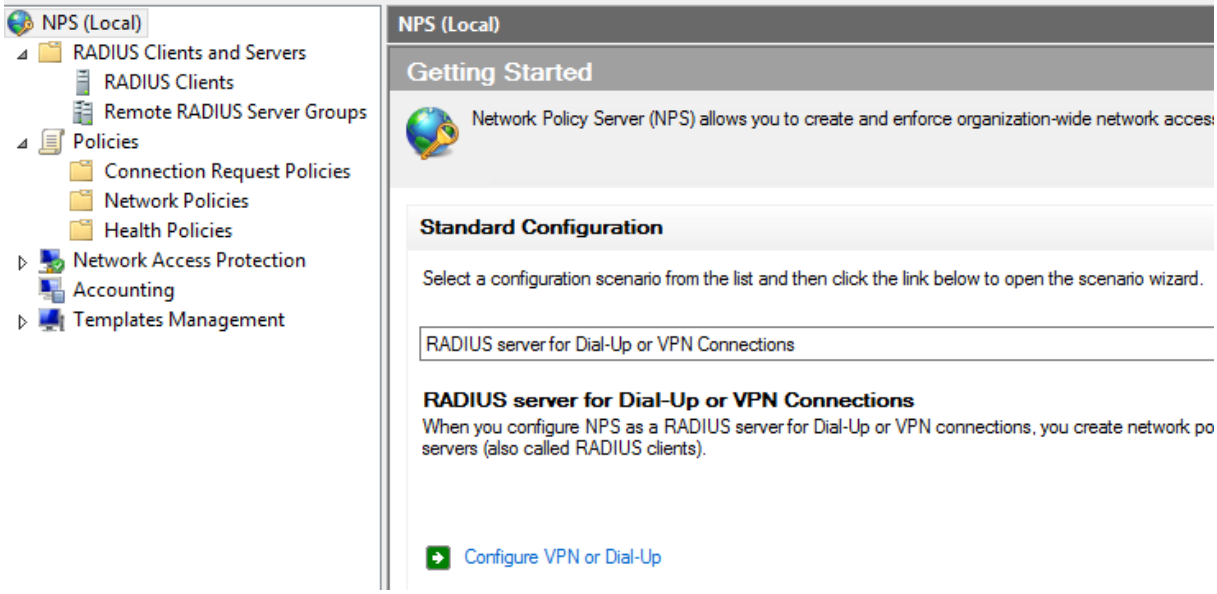
VPN és egyéb távelérési házirendeket, pl. NAP vagy 802.1x szabályokat a Network Policy Serveren (NPS) hozhatunk létre.



A távelérés engedélyezéséhez a következő házirendeket kell létrehoznunk:

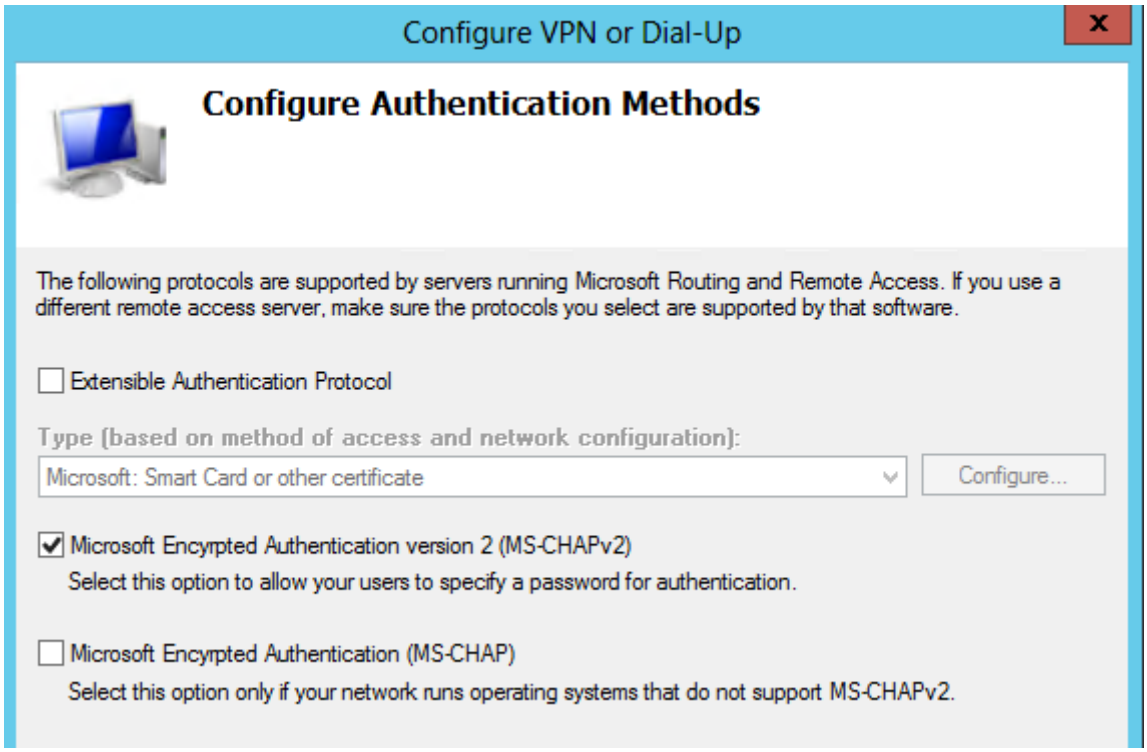
- Connection Request Policy: ez a házirend definiálja, hogy a hitelesítés a helyi gépen történik, vagy egy másik NPS kiszolgálón
- Network Policy: hozzáférési engedélyt adhatunk csoportoknak, illetve titkosítási, hitelesítési és egyéb beállításokat szabályozhatunk.

A szükséges házirendeket a varázslóból is létrehozhatjuk, ha a bal felső sarokban az NPS (local) kiszolgálón a „Radius Server for Dial-up or VPN Connections” konfigurációt választjuk:



Ha elindítjuk a Configure VPN or Dial-Up varázslót, akkor válasszuk a VPN kapcsolatot, majd a RADIUS kliens részen lépjünk tovább. Erre akkor lenne szükségünk, ha a VPN kiszolgáló és a hitelesítési kiszolgáló külün számítógépeken van, vagy ha több VPN kiszolgálót szeretnénk egy NPS-ről szabályozni.

A következő lépésnél az alábbi hitelesítési módszerek közül választhatunk:



- EAP: bővíthető hitelesítés, akár intelligens kártyával, akár tanúsítvánnyal, de akár jelszóval is azonosíthatjuk a felhasználóinkat. Részletesebb leírás: http://technet.microsoft.com/en-us/network/bb643147.aspx
- MS-CHAPv2: kétirányú, Windows jelszavas hitelesítés. Leírás: http://technet.microsoft.com/en-us/library/cc957983.aspx
- MS-CHAP: régebbi klienseken használható hitelesítés

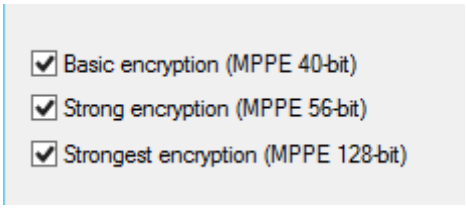
Ha lehetőségünk van, használjuk az EAP alapú hitelesítési módszert, itt is több opció közül választhatunk:

- Smart Card or Other Certificate: intelligens kártyás vagy egyéb tanúsítvánnyal azonosítjuk a felhasználóinkat, használatához PKI infrastruktúra szükséges
- PEAP: TLS-el titkosított csatorna, használatához kiszolgálói tanúsítványra van szükségünk. A csatornán belül használhatunk jelszavas vagy tanúsítvány alapú hitelesítést
- EAP-MSCHAPv2: szintén kiszolgálói tanúsítvány szükséges a hitelesítéshez. Kevésbé biztonságos, mint a PEAP protokoll

A következő lépésben ki kell választanunk egy felhasználói csoportot, akik VPN hozzáférést kapnak. Javasolt egy külön erőforrás-csoportot létrehozni (pl. távelérési felhasználók), és ebbe a csoportba behelyezni a felhasználóinkat vagy csoportjainkat.

Az IP filternél korlátozhatjuk, hogy a VPN felhasználók a hálózat mely részéhez férhetnek hozzá, kimenő és bejövő szűrők használatával.

A VPN titkosításnál kiválaszthatjuk, milyen kulcshosszúságú biztonsági szintet szeretnénk használni:



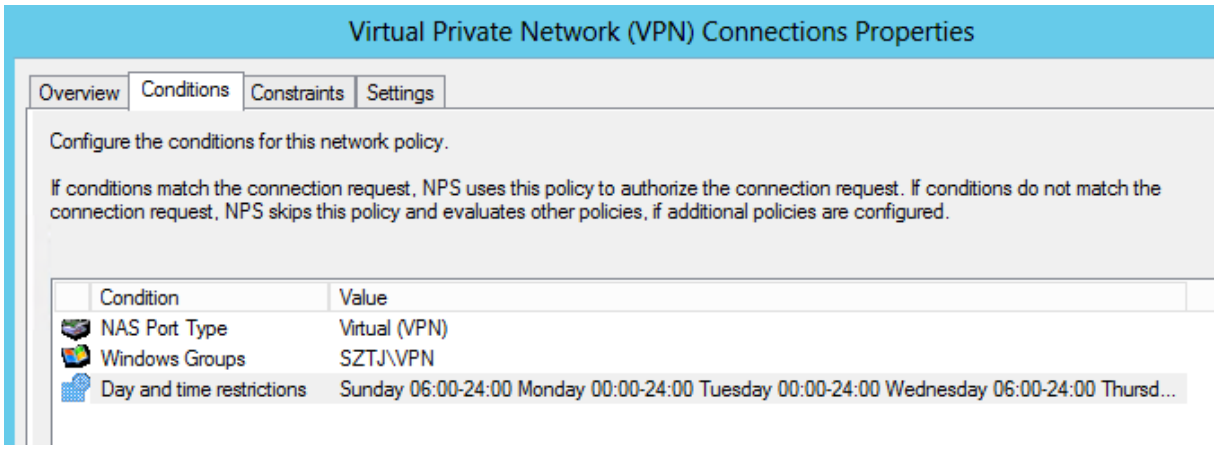
Ha mindhármat bekapcsolva hagyjuk, a VPN kiszolgáló először a legnagyobb kulcsú titkosítással próbálkozik, és ha a kliens ezt nem támogatja, csökkenti a titkosítást. Bizonyos kliensek csak 40-bites titkosítást képesek használni, tehát érdemes mindhárom opciót engedélyezni.

A realm name kihagyása után (ezt csak bizonyos szolgáltatók igénylik) az összefoglaló képernyőn láthatjuk, hogy létrehoztunk egy kapcsolatkérelmi házirendet (connection request policy) és egy hálózati házirendet (Network policy) is.

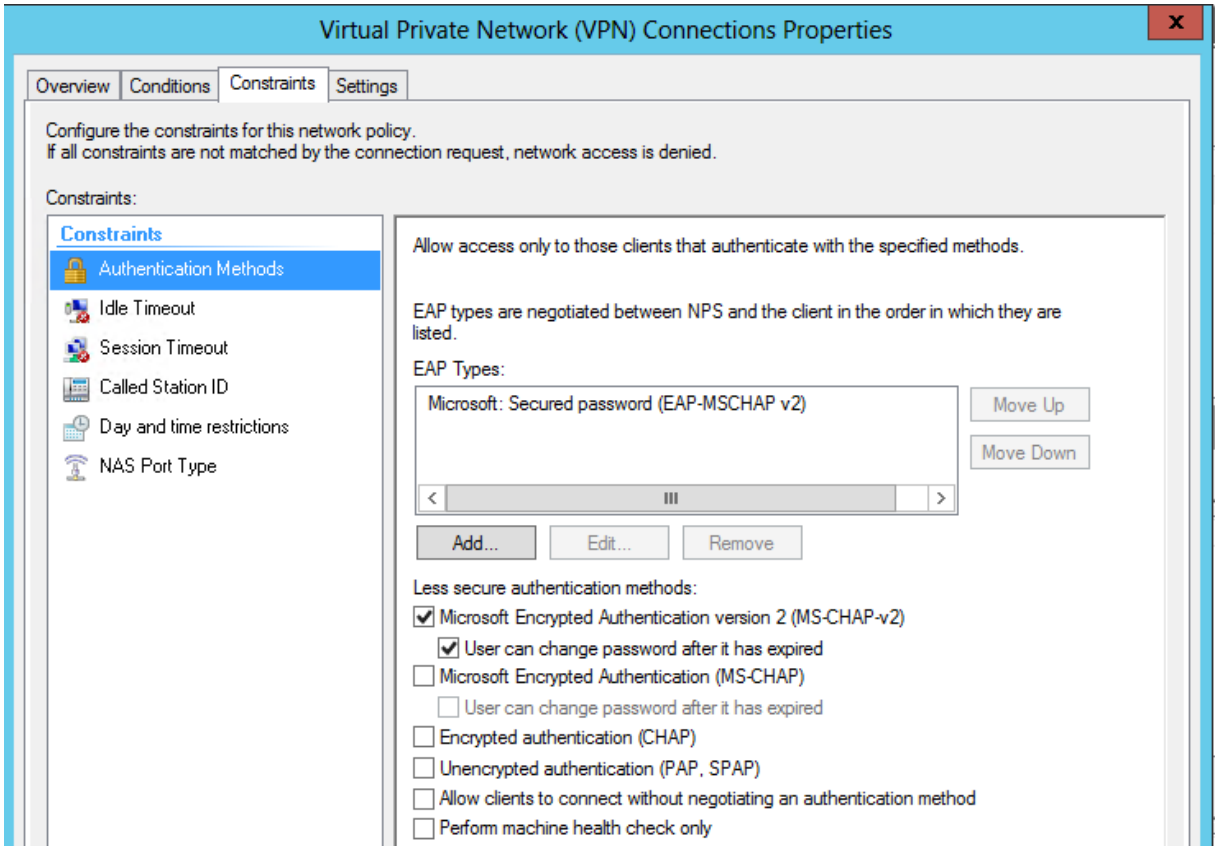
Ezzel készen is vagyunk a házirendek létrehozásával, nézzük is át a Network policy-t:

A szabály tulajdonságait megnyitva, az Overview fülön kapcsolhatjuk ki/be a szabályt, illetve megadhatjuk, hogy engedélyező/tiltó szabályról van szó – pl. munkaidőben tiltjuk a VPN-t – illetve felülbírálhatjuk az AD-ben beállított engedélyezést.

A Conditions fülön további feltételeket adhatunk meg, pl. mikor jelentkezhetnek be a felhasználóink:



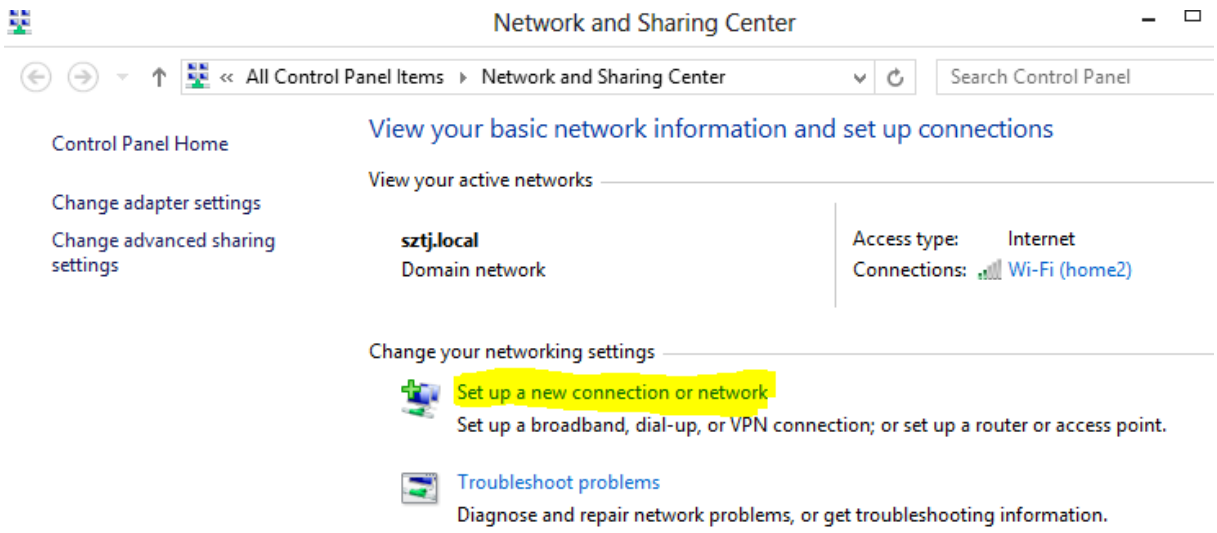
A constraints fülön a megadott hitelesítési módszereken tudunk változtatni, korlátozhatjuk a VPN kapcsolat idejét, illetve beállíthatjuk, hogy bizonyos tétlenségi idő után a server bontsa a kapcsolatot.



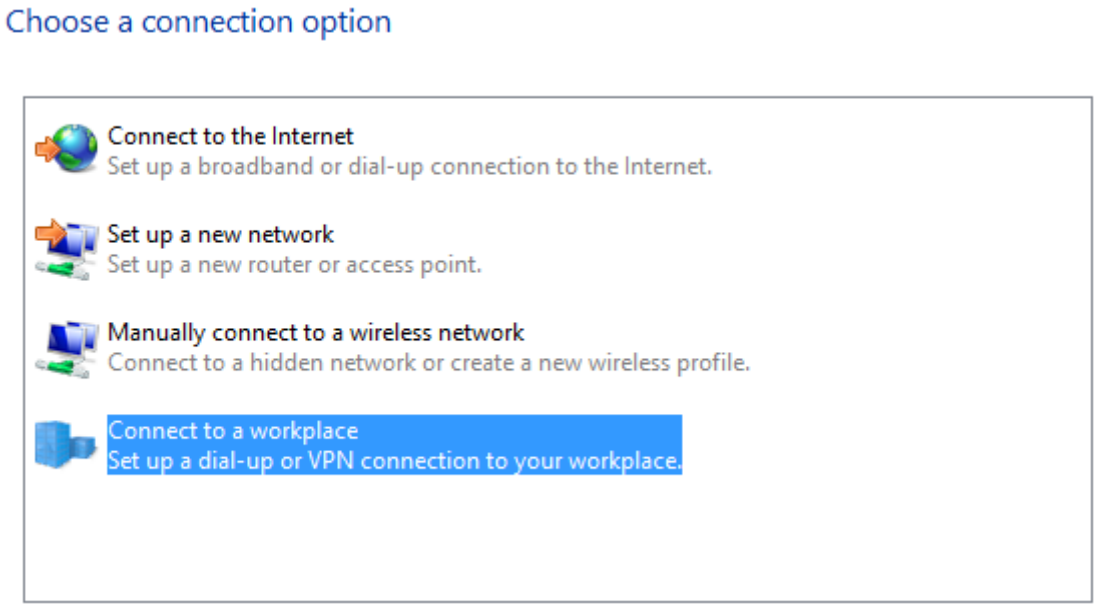
Ezzel a kiszolgáló oldallal készen vagyunk, nézzük a VPN kliens oldali beállítását.

A VPN kapcsolatot létrehozhatjuk kézzel, csoportházirendből, vagy a Connection Manager Administration Kit (CMAK) használatával is. Nézzük a kézi beállítást:

- A Windows 8-on nyissuk meg a Hálózati és Megosztási Központot (Network and Sharing Center)
- Nyissuk meg a set up a new connection or network varázslót:

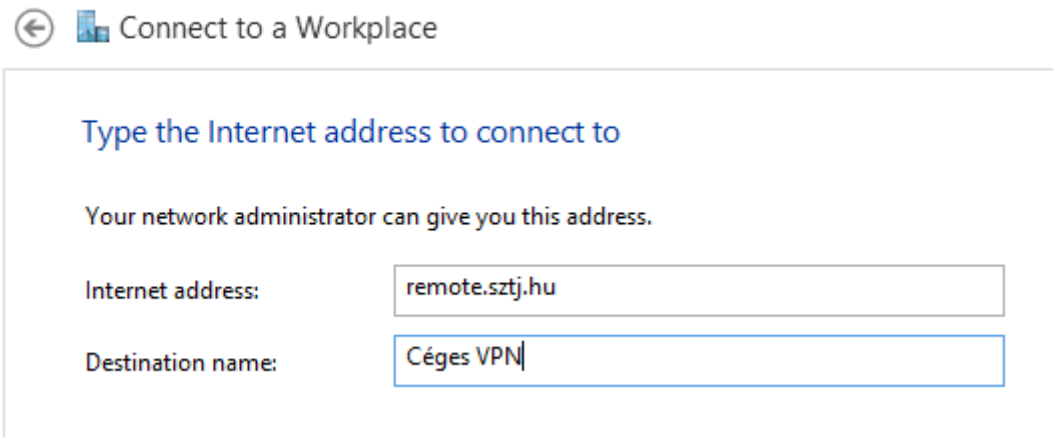


Válasszuk a csatlakozás a munkahely hálózatához opciót:

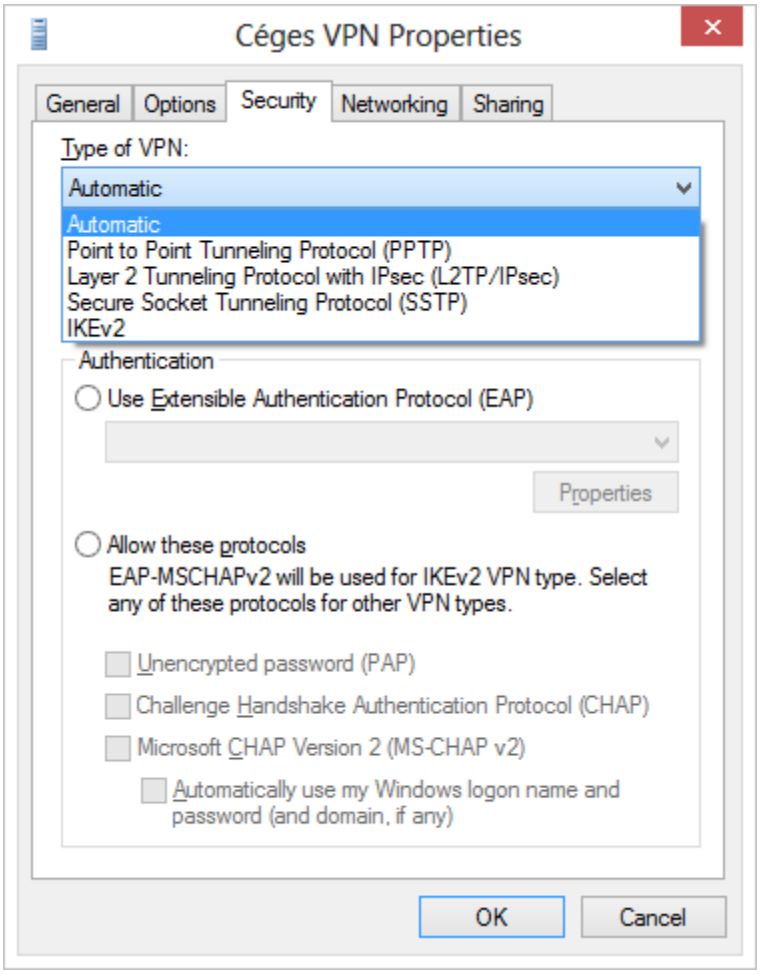


Majd a VPN kapcsolatot:

Adjuk meg a kiszolgálónk Internetes nevét, illetve egy megjelenítési nevet:



Létrehozás után a VPN kliensünk megpróbál csatlakozni a kiszolgálóhoz. A VPN protokollt automatikusan próbálja megállapítani, először próbálkozik IKEv2-vel, SSTP-vel, L2TP-val, majd PPTP-vel. Ha nem szeretnénk végigvárni, érdemes kézzel megadni a használt protokollt a VPN kapcsolat tulajdonságainál:



12 Windows Server Biztonsági Másolat

Ebben a fejezetben megnézzük, milyen stratégiával érdemes menteni az adatainkat és rendszereinket, hogyan tudunk felkészülni az esetleges adatvesztés elkerülésére. Megismerkedünk a Windows Server Backup programmal és vetünk egy pillantást a Microsoft Azure alapú online mentési felületére.

A Windows Server Backup használatával a következő mentéseket végezhetjük el:

- Teljes mentés: a számítógép összes adatának mentése, beleértve az összes kötetet, a rendszer beállításait, és a különböző alkalmazásokat. Ha lehetséges, mindig érdemes ilyen mentést készítenünk, visszaállításkor pedig el tudjuk dönteni, milyen állományokra van szükségünk.
- Adott kötetek mentése: ha a rendszer konfigurációja nem változik túl sűrűn, érdemes lehet a napi mentésbe csak néhány kötetet bevonni, ahol pl. a megosztott dokumentumok találhatók
- Adott fájlok és könyvtárak mentése: ha kézi mentést szeretnénk végezni, vagy csak bizonyos fájlokat szeretnénk menteni a Microsoft online backup segítségével.

A Windows Server Backup lehetőséget ad arra is, hogy ún. Bare Metal Restore-t (operációs rendszer nélkül visszaállítás) hajtsunk végre, amennyiben a mentett számítógép teljesen tönkremegy, a Windows Recovery Enviroment segítségével egy másik gépre a komplett feltelepített Windows-t képesek vagyunk visszaállítani.

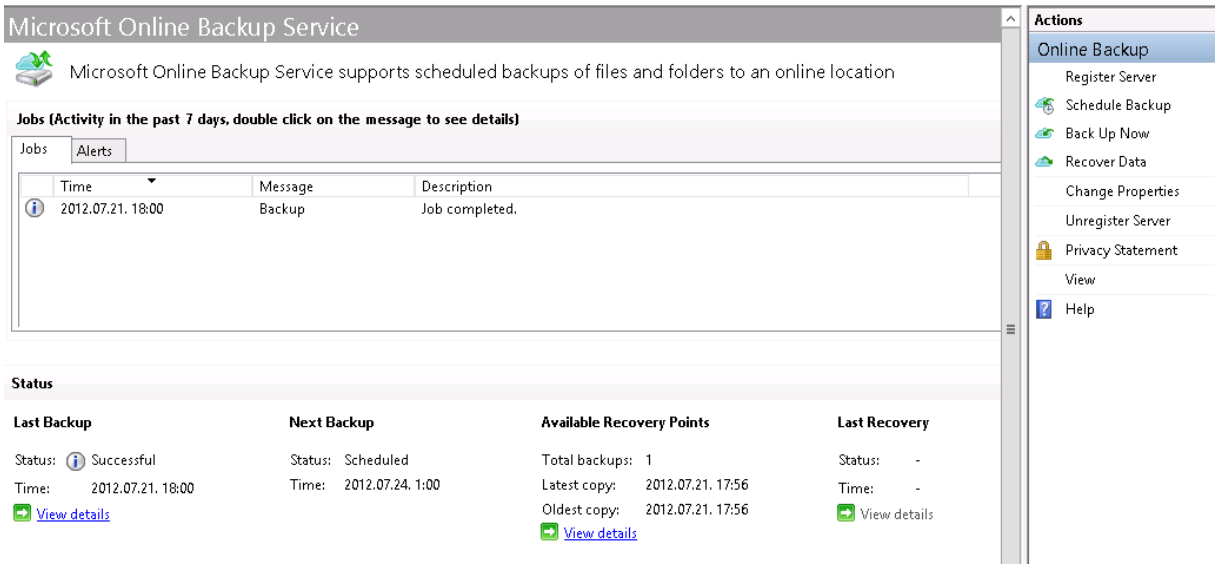
12.1 Windows Online Backup

A Microsoft új, felhő alapú mentési megoldása, mely a Windows Azure platformot használja az adatok tárolására, a következő előnyöket nyújtja:

- Egyszerű felület, a szolgáltatás beépül a Windows Server Biztonsági Mentés konzolba
- Blokk-szintű különbözeti mentés
- Adatok átvitele tömörített és titkosított formátumban
- Adatmegőrzési házirend segítségével megadhatjuk, meddig szeretnénk megőrizni a mentéseket
- Adatintegritás ellenőrzése a felhőben.

A Windows Online Backup mint előfizetés vásárolható, és kizárólag fájlokat és mappákat képes menteni, pl. rendszer-állapotot, Exchange vagy SQL adatbázist nem. Ezért ez a megoldás inkább kiegészíti a Windows Server Biztonsági Másolatot, nem helyettesíti.

Használatához először regisztrálnunk kell a szolgáltatásra, majd a kapott felhasználónév és jelszó segítségével regisztrálnunk kell kiszolgálónkat a Microsoft Online Backup felhőbe. A rendszer jelenleg tesztelési fáziban működik, ingyenesen kipróbálható, de maximum 10GB-nyi adatot tölthetünk fel. Sikeres regisztráció után a felület ugyanúgy működik, mintha helyi mentést végeznénk.



A Windows Online Backup felülete beépül a Windows Biztonsági mentés programba

Az on-line mentés beállításánál megadhatunk egy 16 karakteres jelszót, amivel a titkosítást végzi a rendszer, így a felhőben tárolt dokumentumokhoz mások nem férhetnek hozzá, megadhatunk proxy kiszolgálót a szinkronizáláshoz, illetve korlátozhatjuk a mentéshez használt sávszélességet is. A mentések végrehajtásához szükségünk lesz a Microsoft Online Backup Agent-re, mely a Connect oldalról érhető el:

http://connect.microsoft.com/site1277/Downloads/DownloadDetails.aspx?DownloadID=40629

12.2 Rendszerállapot mentése

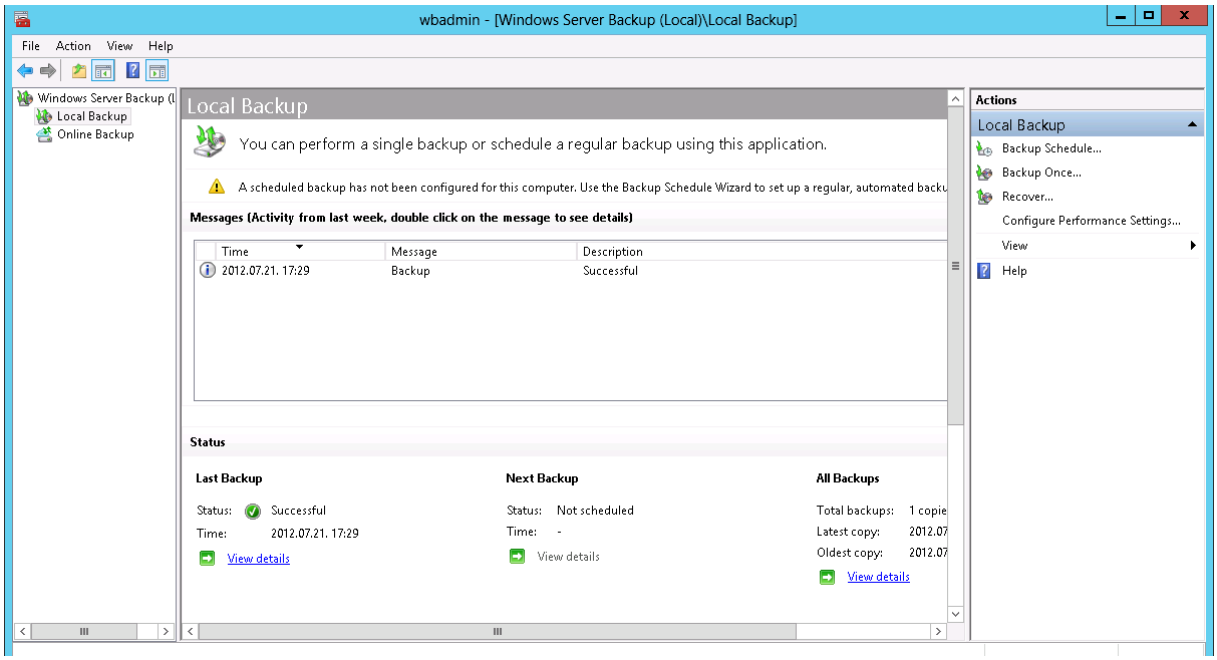
A rendszerállapot mentése, mint különálló komponens választható a mentés ütemezésekor vagy kézi mentéskor. Ez a következő elemeket tartalmazza:

- Active Directory
- DNS
- DHCP
- Fájl- és nyomtatószolgáltatások
- Tanúsítvány kiszolgáló
- IIS
- Útválasztás és távelérés

Segítségével a rendszer meghibásodása esetén könnyen visszaállhatunk egy régebbi, még működő állapotra.

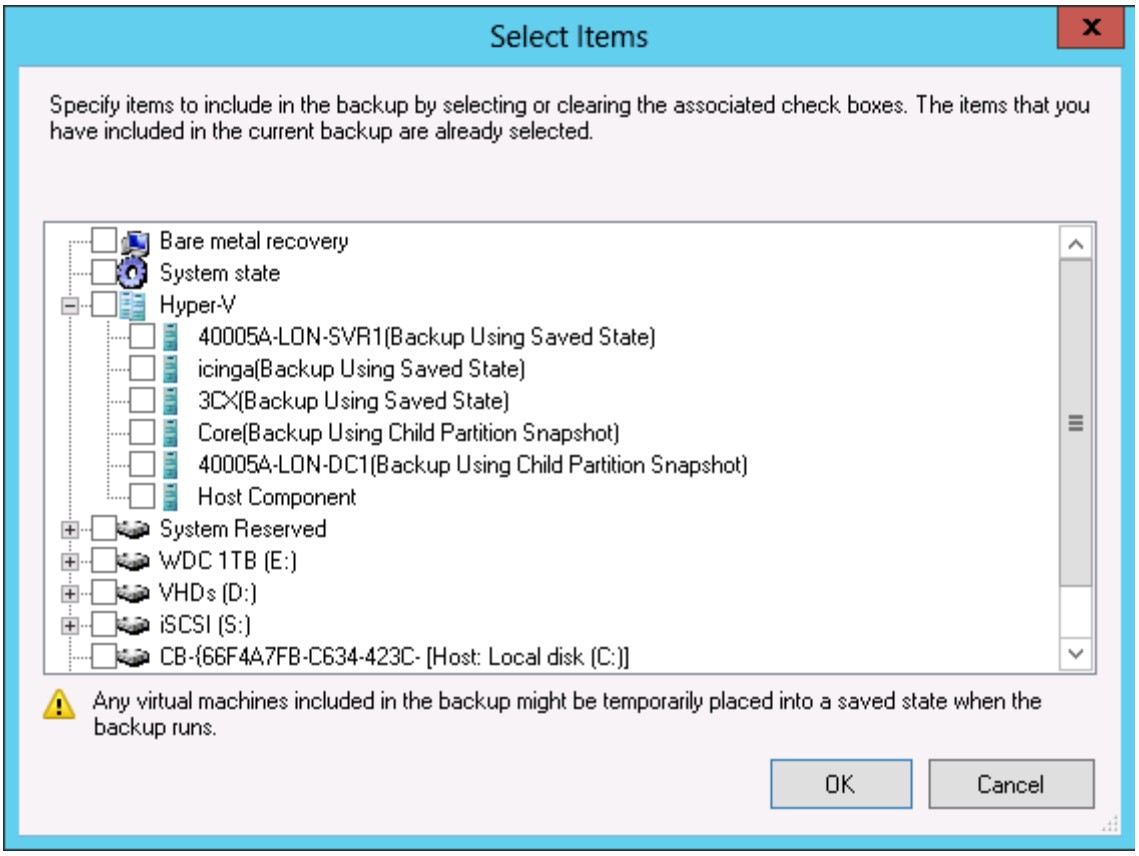
Biztonsági mentés ütemezése

A mentés ütemezéséhez indítsuk el a Windows Server Biztonsági Mentés programot:



A mentés ütemezése gombra klikkelve elindul a biztonsági mentés varázsló, ahol a következő paramétereket kell megadnunk:

- Teljes mentés vagy egyéni mentést szeretnénk időzíteni
- Az egyéni mentésnél megadhatjuk, milyen meghajtókat szeretnénk menteni, illetve szeretnénk-e bare metal restore-t vagy system state mentést végezni
- Az időzítésnél megadhatjuk, milyen napokon és órákban szeretnénk futtatni a mentést.



(Érdemes megfigyelni, hogyan tudunk virtuális gépeket menteni a Hyper-V hoszton.)

A mentés helyének választhatunk dedikált háttértárat, (helyileg csatolt vagy iSCSI lemezt), meglévő kötetet vagy hálózati megosztást. A hálózati megosztásnál nem tudunk több mentést megtartani, az aktuális mentés mindig felülírja a legutóbbit. A javasolt megoldás a dedikált háttértár, így nem követhetünk el olyan hibát, hogy pl. ugyanazon a lemezen vannak a mentéseink, ahol az adatokat tároljuk. A legbiztosabb megoldás, ha egy másik gépen lévő iSCSI target-re végezzük a mentést, erről a lemezkezelés részben olvashat részletesebben.

Miután megadtuk a céllemezt, ahová a mentéseink készülni fognak, egy összefoglaló képernyőn ellenőrizhetjük a beállításokat, majd a rendszer létrehozza az ütemezett feladatot.

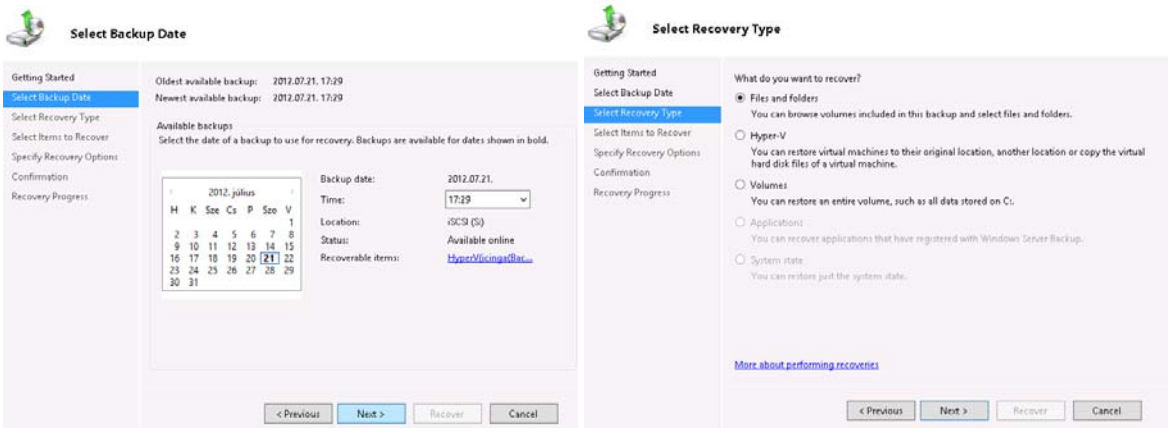
Fontos tudni, hogy a biztonsági mentés eltárolja a fájlok és mappák biztonsági beállításait is, így egy visszaállítás után nem szükséges újra beállítani a jogosultságokat. Ez akkor is igaz, ha a visszaállítást egy másik kiszolgálóra végezzük.

12.3 Fájlok visszaállítása

Esetleges adatvesztés után a visszaállítás menüvel tudjuk elindítani az adatok visszaállítását:

- A mentés forrása lehet a helyi számítógép vagy egy másik kiszolgáló
- Ütemezett mentés esetén ki tudjuk választani, melyik időpontra szeretnénk visszaállni
- Ezután ki kell választanunk, milyen adatokat szeretnénk visszaállítani
- A visszaállítás helyénél ki tudjuk választani az eredeti helyet is, vagy másik mappába is visszaállíthatjuk adatainkat

- A biztonsági beállításoknál megadhatjuk, hogy szeretnénk-e visszaállítani a mappák és fájlok jogosultságait (ACL bejegyzéseit) is.



A biztonsági mentés visszaállítása varázsló

12.4 Kiszolgáló helyreállítása

Bizonyos esetekben szükségünk lehet a teljes kiszolgáló visszaállítására, ha pl. a kiszolgáló leégett, ellopták, vagy egyéb módon teljesen megsemmisült. Ilyen esetekre a biztonsági mentés a következő lehetőségeket nyújtja:

- Operációs rendszer nélkül helyreállítás eredeti hardverre vagy másik gépre
- Virtuális gép visszaállítása eredeti helyre vagy másik Hyper-V hosztra
- Mivel a mentés VHD formátumot használ, így a fizikai gépmentést visszaállíthatjuk Hyper-V környezetbe is, így virtualizálva a fizikai gépet.

12.5 Parancssori eszközök

Ugyan a biztonsági mentés programhoz vannak PowerShell Cmdlet-ek, de van saját parancssori alkalmazása, a wbadmin.exe:

- wbadmin start backup: egyszeri mentés készítéséhez
- wbadmin start systembackup: rendszerállapot mentést hoz létre
- wbadmin get status: a folyamatban lévő mentés állapotát kérdezi le

13 Távtelepítés

A Windows Deployment Services használatával hálózaton keresztül tudunk operációs rendszert teríteni a fizikai és virtuális gépeinkre. A hálózati telepítéshez nincs szükségünk DVD lemezekre, USB eszközökre, illetve egy időben akár több gépet is telepíthetünk.

Előnyei:

- Kliens és kiszolgáló gépek gyorsabb, egyszerűbb telepítése
- Mixed módban telepíthetünk Windows XP, 2003, Windows 7, Windows 8, és Windows Server 2008, 2012-es operációs rendszereket
- Egységes környezetet alakíthatunk ki
- A beépített Windows PE szolgáltatásokat használja, így hardver függetlenül telepíthetünk
- Egy időben több gépet telepíthetünk multicast címzés segítségével
- Létrehozhatunk céges referencia operációs rendszert, amit később terjeszthetünk WDS-el
- Illesztőprogramokat tudunk illeszteni a telepítési környezetünkbe.

13.1.1 Újdonságok a Windows Server 2012-ben

Az új WDS már működik Active Directory nélkül is, ha egy ad-hoc hálózatot szeretnénk telepíteni, támogatja a VHDX formátumot, így a 2TB-nál nagyobb lemezképeket is ki tudunk szórni, teljes körűen támogatja az Ipv6-os infrastruktúrát, az UEFI alapú gépeket, illetve telepítéskor nem kell letároltunk a .WIM állományunkat a helyi gépen (erről részletesebben később)

13.1.2 Feltételek

A Windows Deployment Services telepítéséhez szükségünk lesz egy AD címtárra (kivéve standalone server mode), DNS, DHCP kiszolgálóra, és javasolt egy külön NTFS partíciót fenntartani a telepítés fájloknak. A WDS kiszolgáló lehet tartományvezérlőn vagy tartománytagon, és telepíthetjük fizikai vagy virtuális gépre is.

13.1.3 Működés

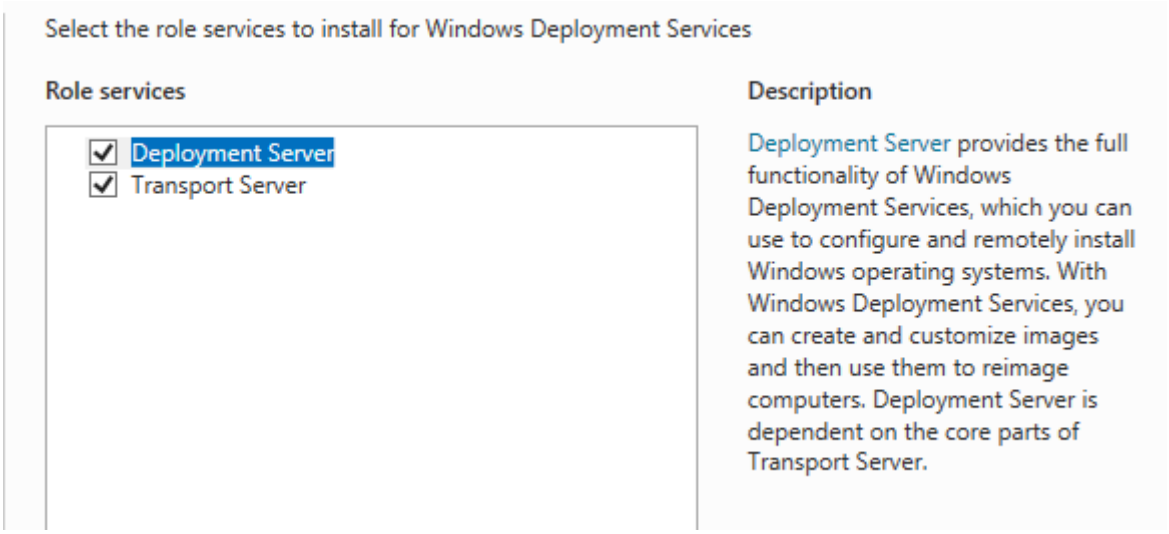
A WDS környezet hálózati bootolási környezetet (PXE) igényel. A telepíteni kívánt gép PXE-ről indul, majd első lépésben a DHCP kiszolgálótól kér IP címet, illetve információt a TFTP (trivial FTP) kiszolgálóról. Miután felvette a kapcsolatot a TFTP kiszolgálóval, letölt egy kiválasztott Windows PE-t, ami lehet telepítés környezet, x86 vagy x64-es, lemezkép készítő, vagy akár testreszabott, karbantartó Windows PE is akár.

Ha telepítési Windows PE-t választunk, akkor a PE betölti a hálózati és lemezkezelő meghajtó-programokat, és elindítja a Windows telepítőt. A WDS alapértelmezésként belépteti a gépet az Active Directory tartományba, és automatikusan elnevezi a számítógépet.

13.1.4 WDS telepítés

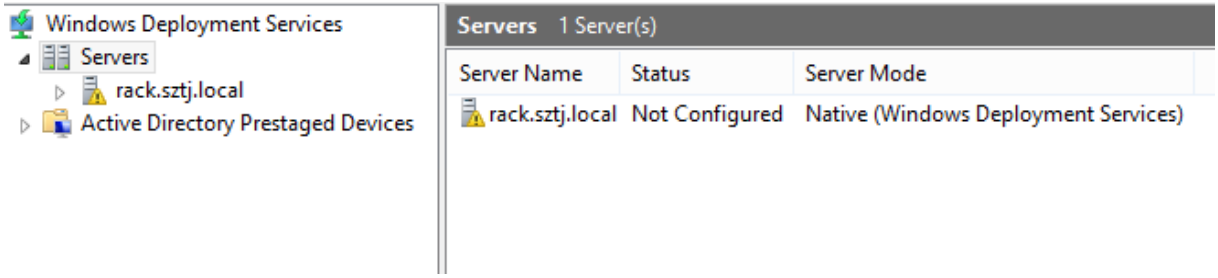
A WDS telepítése előtt tehát kell, hogy legyen egy működő címtárunk, DNS és DHCP kiszolgálónk. Ha ezek a feltételek adottak, nekiláthatunk a telepítésnek. A WDS telepítése PowerShellből nem indítható, a grafikus felületet kell használnunk.

Telepítésnél két komponenst választhatunk:



- Deployment Server: alapkomponens, operációs rendszerek telepítése, testreszabására. Tartalmazza a TFTP kiszolgálót és minden szükséges fájlt a gépek egyéni telepítéséhez
- Transport Server: használatával multicast telepítést indíthatunk, tehát akár egy komplett számítógép-termet telepíthetünk egy időben. Ez a szerepkör külön gépre is telepíthető.

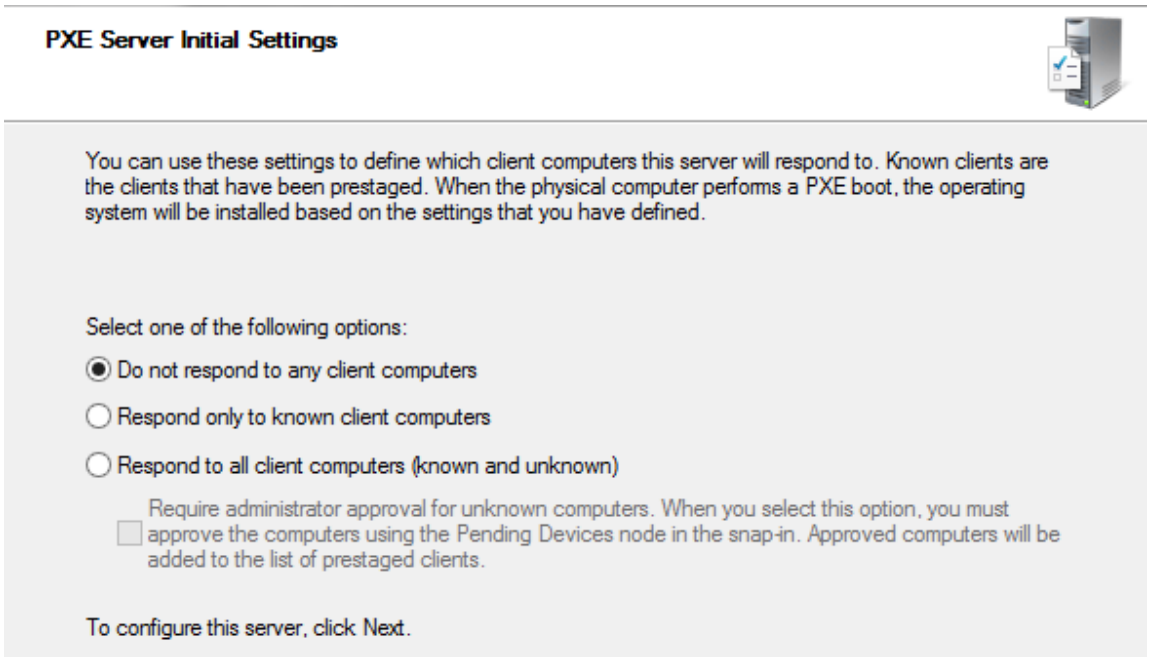
Telepítés után testre kell szabnunk a WDS kiszolgálónkat, akár a konzolból, akár a WDSUtil parancssori eszköz használatával. Mi most a grafikus felületet nézzük végig:



A testreszabás során meg kell adnunk, hogy AD integrált, vagy standalone WDS kiszolgálót szeretnénk-e konfigurálni, majd meg kell adunk egy NTFS partíciót, ahol a telepítési fájlokat tároljuk. A következő beállítás a DHCP-re vonatkozik:

Amennyiben a DHCP kiszolgáló a helyi gépünkön fut, a WDS-t úgy kell beállítanunk, hogy ne ütközzön a DHCP-vel, tehát ne figyeljen a DHCP és DHCPv6 portokon, illetve állítsa be a helyi DHCP servert, hogy ossza ki a 60-as PXE beállításokat, így a PXE-vel induló DHCP klienseink megtalálják a TFTP kiszolgálót.

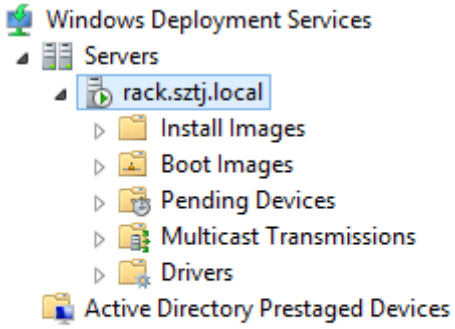
A WDS kiszolgálónkat telepíthetjük úgy, hogy csak az előre megadott klienseknek válaszoljon, ilyenkor a kliens gépeink GUID azonosítóját előre fel kell konfigurálnunk, vagy választhatjuk azt, hogy minden kliensnek válaszoljon, ami azonban biztonsági kockázattal jár: ebben az esetben bárki telepítheti a céges Windows lemezképeket, akár a saját notebookjára is. Ebben az esetben megadhatjuk, hogy rendszergazdai beavatkozás szükséges a telepítés elkezdéséhez:



Ezután a WDS elindítja a szükséges szolgáltatásokat, majd hozzá kell adnunk az indítási és telepítési WIM állományt.

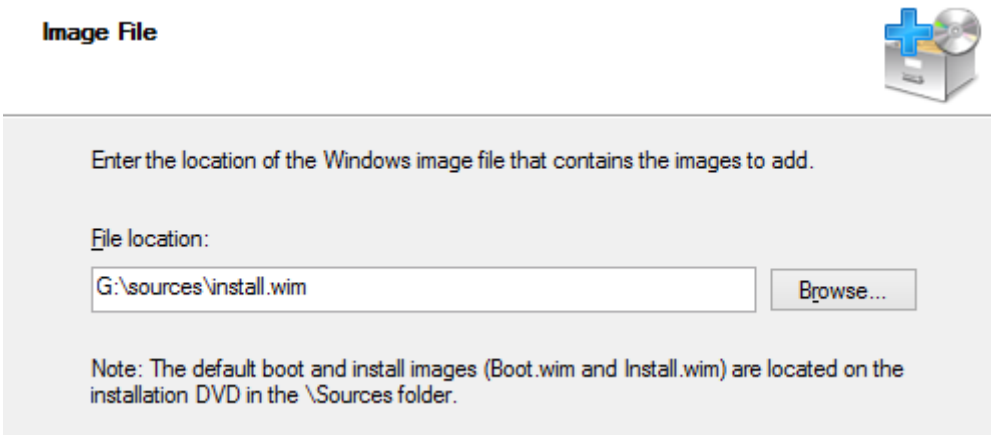
A WIM fájlformátum, hasonlóan a VHD formátumhoz, egy komplett lemezképet tárol. A Windows telepítési médián is két WIM állomány található, az első a BOOT.WIM, ami a Windows PE előtelepítési lemezképet tartalmazza, illetve az INSTALL.WIM, ami magát a telepítendő operációs rendszer lemezképét tárolja. Ezeket a WIM állományokat kell bemásolnunk a WDS kiszolgálóra.

13.1.5 A WDS kiszolgáló felülete

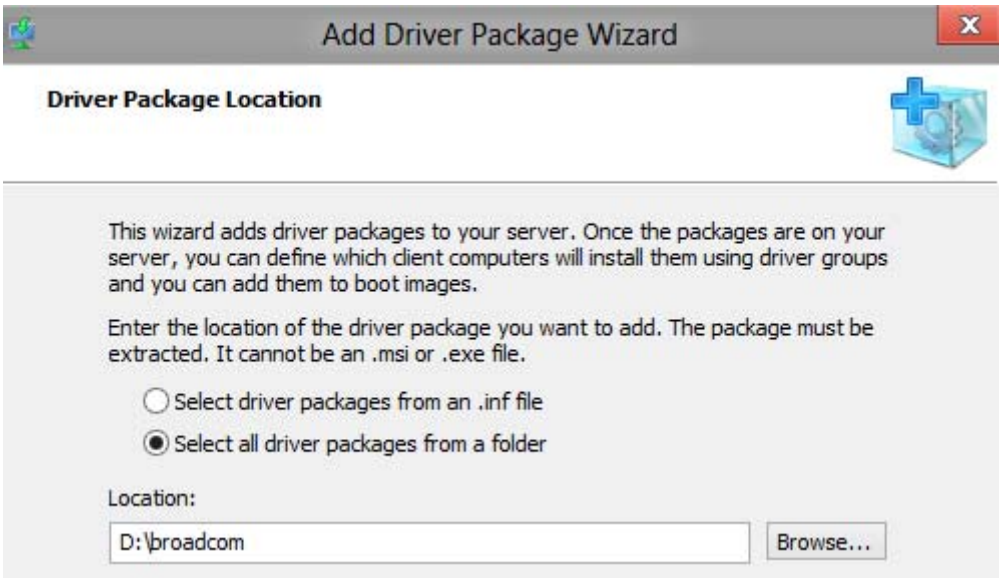


A WDS konzolon tudjuk felvinni az indítási lemezképeinket, a Boot Images résznél, az Add Image segítségével. Indítási lemezképből mindig érdemes a legújabbat használni, például a Windows 7 SP1 vagy Windows 8-as boot állományt, illetve a kliens gépeinktől függően érdemes felvenni az x86-os és x64-es WIM állományokat egyaránt. A felvett lemezképekből tudunk majd ún. Capture Image-et létrehozni, amellyel egy már előre feltelepített operációs rendszert tudunk visszamásolni a telepítési kiszolgálónkra.

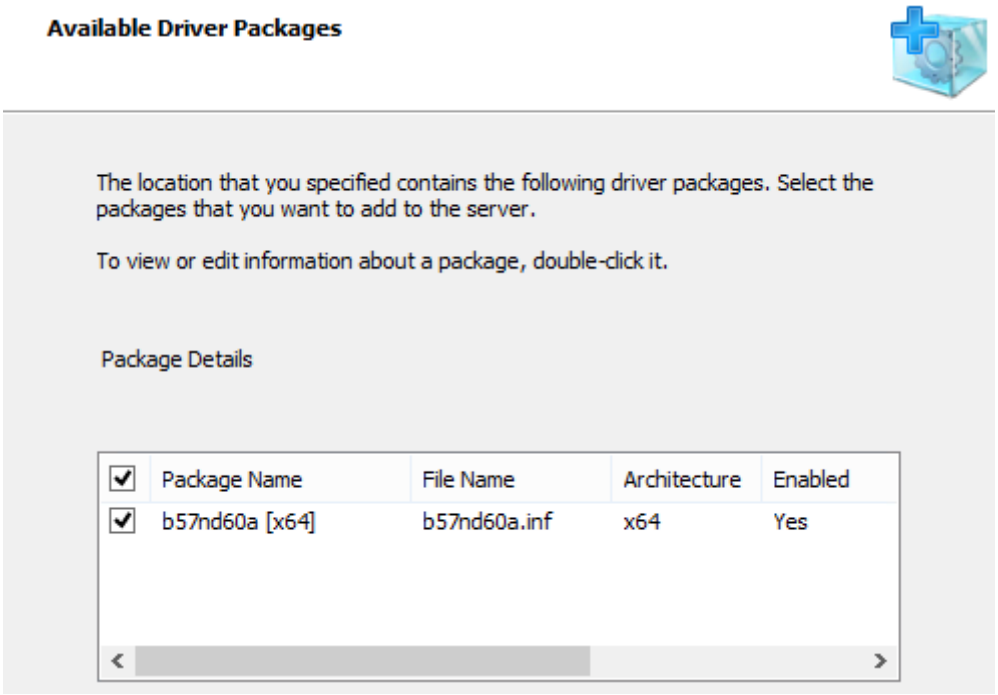
Az Install Image résznél, először érdemes megfelelő mappákat vagy image group-okat létrehozni a különböző operációs rendszereinknek, majd fel kell másolnunk a Windows telepítő DVD-ről az install.wim állományunkat. A telepítési lemezkép általában adott operációs rendszer több verzióját is tartalmazza, és ki tudjuk választani, mely verziókat szeretnénk használni cégünknél.



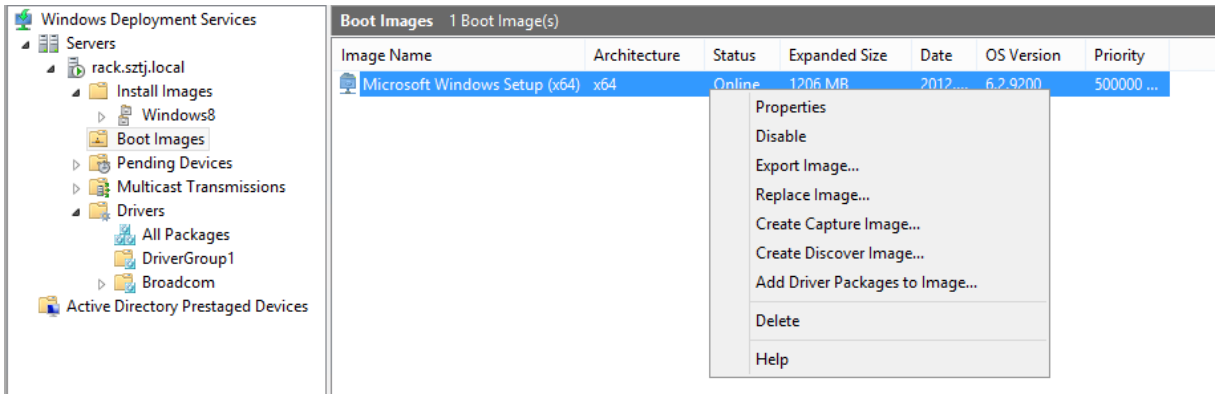
Miután hozzáadtuk az indítási és telepítési WIM állományunkat, ha szükséges, hozzáadhatunk további illesztőprogramot a Drivers résznél. A hozzáadott drivereket később beágyazhatjuk az indítási lemezképbe, így újabb hálózati kártyával vagy speciális merevlemez-vezérlővel szerelt gépeinket is tudjuk telepíteni WDS-ből:



Driver hozzáadásakor megadhatjuk közvetlenül az INF állományt, vagy rábízhatjuk a WDS konzolra, hogy adott mappában keresse meg az összes használható driver csomagot. EXE és MSI fájlokat nem tud hozzáadni, ezért fontos, hogy kicsomagolt illesztőprogramjaink legyenek.



Ha az összes szükséges driver csomagot hozzáadtuk a WDS-hez, a csomagokat be kell helyeznünk a telepítési BOOT.WIM állományunkba az „add driver package to Image” menüben:

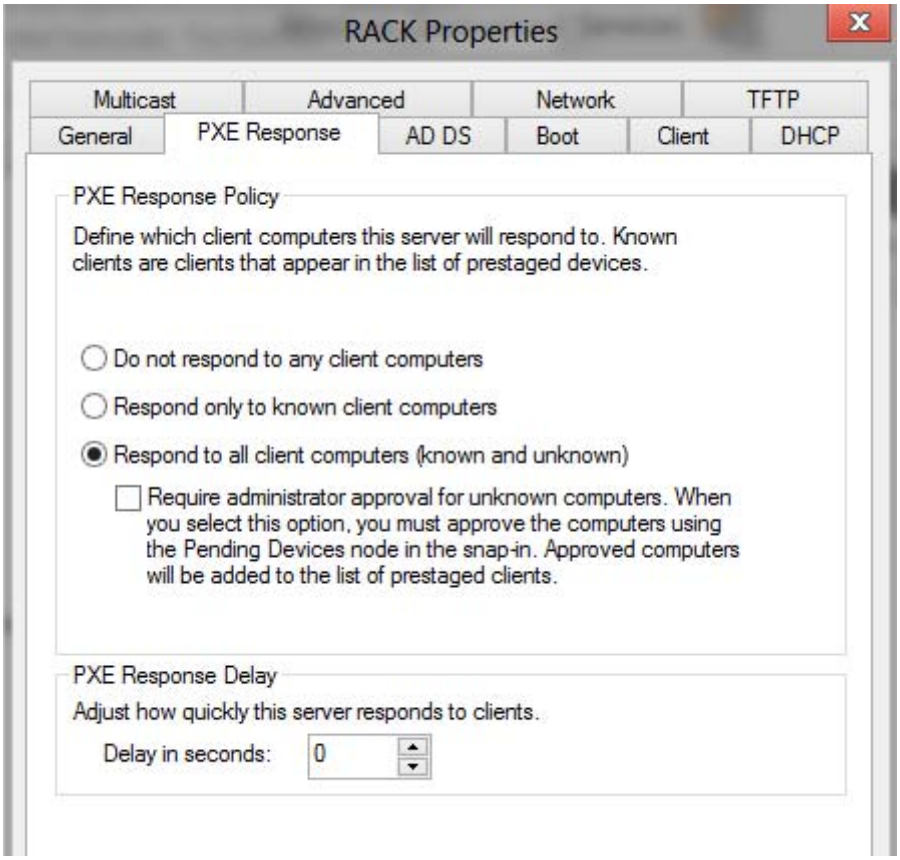


Ezután bármilyen típusú gépen el tudjuk indítani a WDS kliens környezetünket, és tudjuk telepíteni a kiválasztott operációs rendszert

13.1.6 A WDS kiszolgáló beállítása

A kiszolgáló tulajdonságainál a következőket állíthatjuk be:

- PXE válasz a kliensek kéréseire (PXE response)
- AD DS fül: a számítógép neve testreszabható, bármilyen fix és változó értéket beleírhatunk, illetve kiválaszthatjuk, melyik szervezeti egységbe kerüljenek a gépeink
- A Boot résznél megadhatjuk, hogyan reagáljon a WDS az ismert és ismeretlen gépek kéréseire. Ismert gépek azok a számítógépek, amiket egyszer már telepítettünk WDS-ből, vagy kézzel felvettük az AD-be a gépek egyedi azonosítóit (GUID) Megadható, hogy az ismert gépek ne induljanak PXE-vel, az új gépeknél viszont automatikusan
- A Client résznél válaszfájlt adhatunk a kliensgépeknek, illetve kikapcsolhatjuk az automatikus tartományba léptetést.

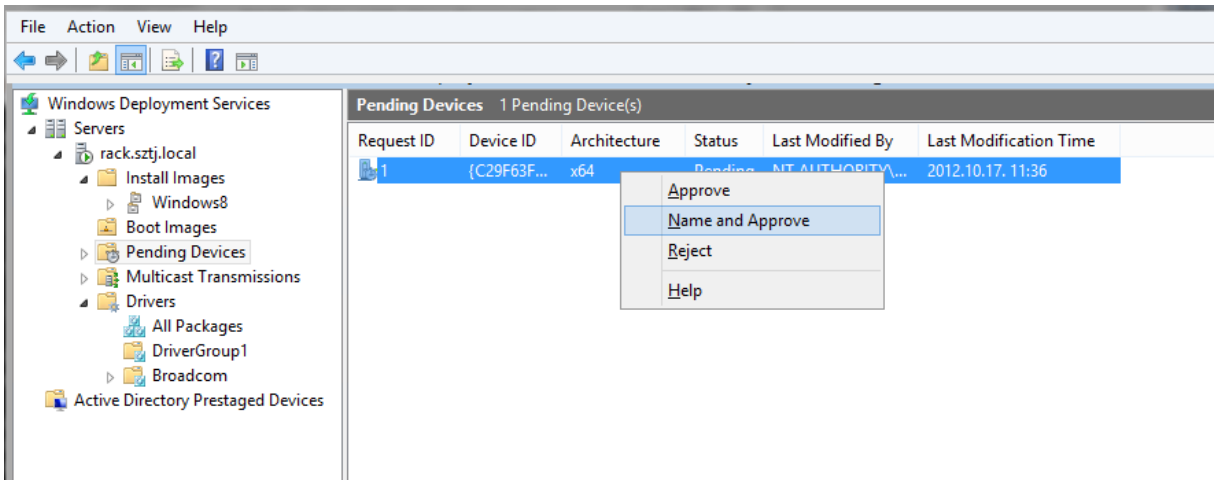


13.1.7 Számítógépek telepítése WDS-ből

Miután bekonfiguráltuk a WDS kiszolgálónkat, nekiláthatunk a kliens gépek telepítésének:

- A gép BIOS-ában engedélyeznünk kell a PXE Boot opciót
- A boot options-nál ki kell választanunk a network boot-ot
- Ezután a kliensgépünk megtalálja a DHCP kiszolgálót, és megkapja a TFTP server adatait

Ha a WDS kiszolgálót úgy állítottuk be, hogy az ismeretlen gépekre csak rendszergazdai engedélyezéssel lehet telepíteni, akkor ennél a lépésnél engedélyeznünk kell a gépet a WDS konzol pending devices résznél:



- A name and approve opcióval a gépet engedélyezzük, el is tudjuk nevezni, illetve megadhatjuk, hogy melyik szervezeti egységbe kerüljön, de azt is megadhatjuk, hogy a gépet ne léptesse be tartományba
  Visszatérve a kliens gépre, a Windows indítási képernyőn ki kell választanunk, hogy melyik indítási lemezképet szeretnénk elindítani, 32 vagy 64 bites verziót.
- A hálózaton letöltődik a Boot.wim állományunk, és tartományi hitelesítés után el tudjuk kezdeni az operációs rendszer telepítését.

13.1.8 Testreszabott operációs rendszer telepítése

A WDS-ben nem csak szűz Windows-t telepíthetünk, de lehetőségünk van céges, testreszabott operációs rendszert kiküldeni. Ehhez a következő lépésekre van szükségünk:

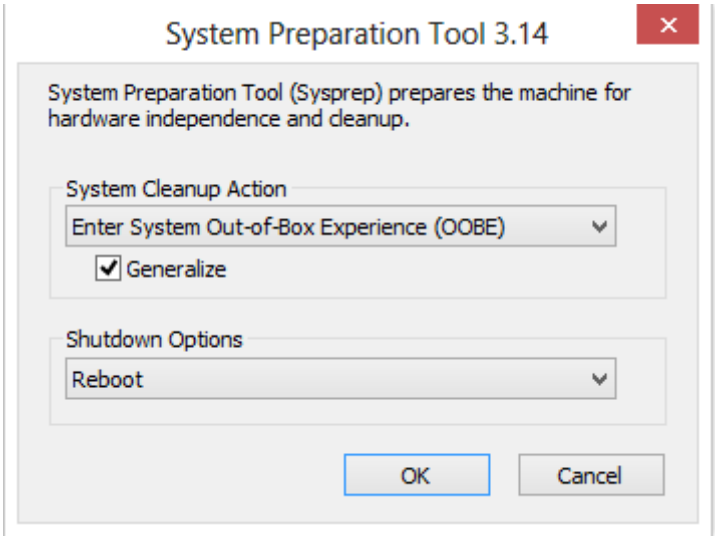
- Referencia gép telepítése
- Testreszabás
- Driverek, patchek, frissítések telepítése
- Referencia gép lezárása
- WIM állomány létrehozása és visszamásolása a WDS kiszolgálóra.

Nézzük végig ezeket a lépéseket:

A referencia gép vagy Master image egy testreszabott Windows, ezt általában a virtuális környezetünkben futtatjuk, és adott időközönként frissítjük. Az aktuális referencia gép mindig tartalmazza a legfrissebb programokat, drivereket, Windows frissítéseket, és az esetleges egyéni alkalmazásainkat. A referencia gépet is WDS-ből érdemes telepíteni.

Az üres referenciagép telepítése után tehát testre kell azt szabnunk, minden olyan alkalmazást fel kell telepíteni, amit az ügyfélgépeken szeretnénk használni. Ha különböző hardverekre szeretnénk teríteni, akkor az adott hardverek illesztőprogramjait fel kell telepíteni a referenciagépre

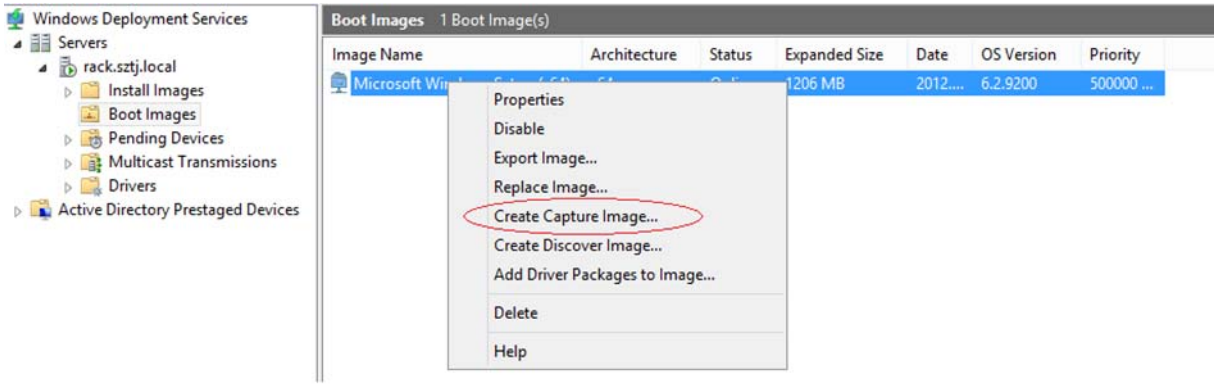
Ezután el kell távolítanunk minden egyéni beállítást a gépről, pl. számítógépnév, termékkód, egyéb azonosítók, és vissza kell zárnunk a telepítés utáni állapotra. Ezt a kliens gép c:\windows\system32\sysprep mappában található sysprep.exe-t kell lefuttatnunk, majd kiválasztanunk a generalize opciót:



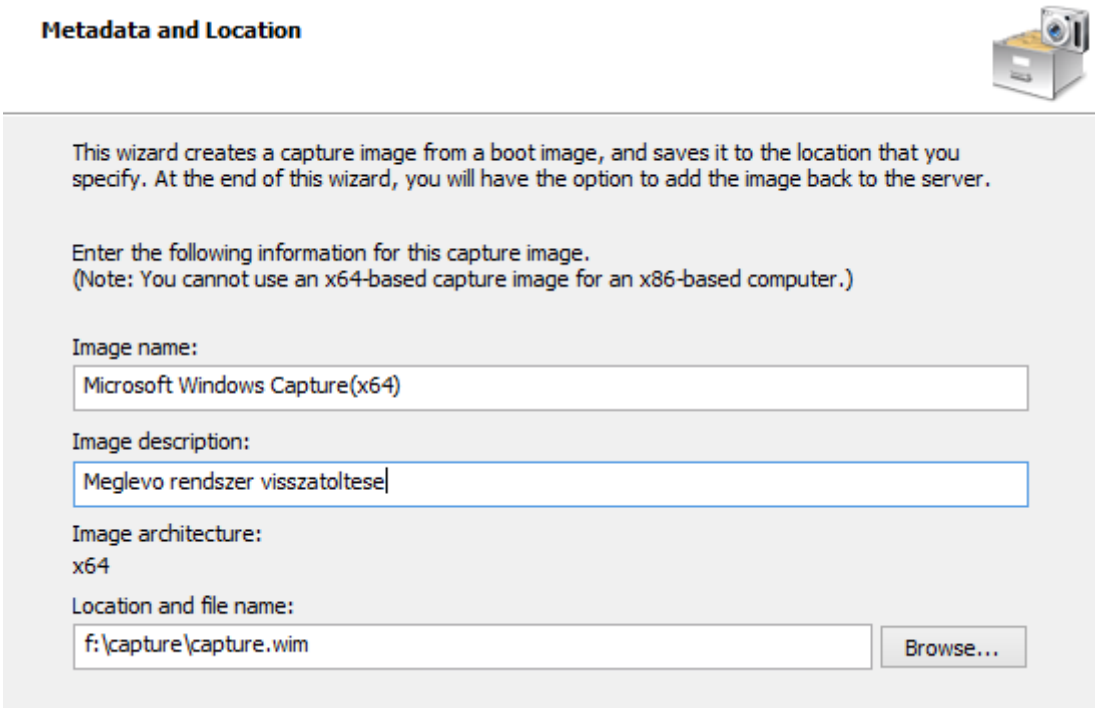
Ha a sysprep sikeresen lefutott, akkor a WDS kiszolgálón létre kell hoznunk egy ún. capture image-et. Ez a „begyűjtő” lemezkép fogja felmásolni a már meglévő operációs rendszerünket a WDS kiszolgálóra.

13.1.9 Capture image készítése

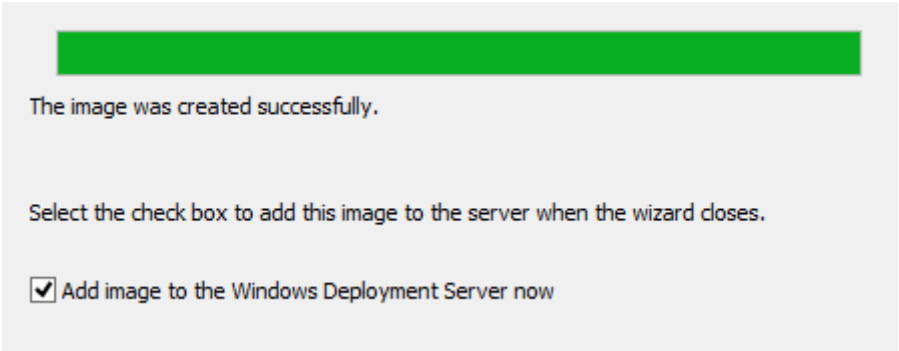
A Capture image alapja az indítási lemezkép, amit a WDS konzol megfelelően módosít, így nem telepítése, hanem visszamásolásra tudjuk használni. A WDS konzolon válasszuk a boot image-ünket, majd válasszuk a create capture image opciót:



A capture fájlt le kell mentenünk egy átmeneti helyre, illetve meg kell adni a nevét és a leírását:



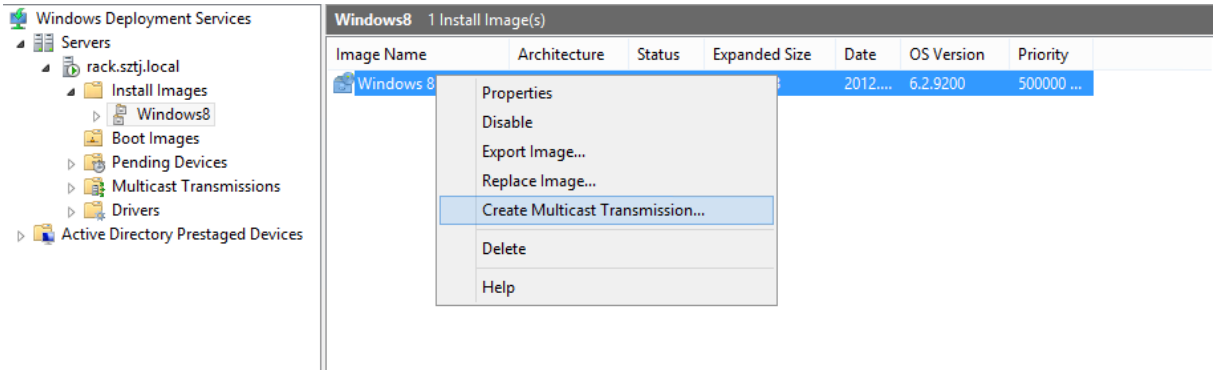
Miután a WDS konzol elkészítette a capture lemezképünket, vissza kell töltenünk a WDS kiszolgálóra:



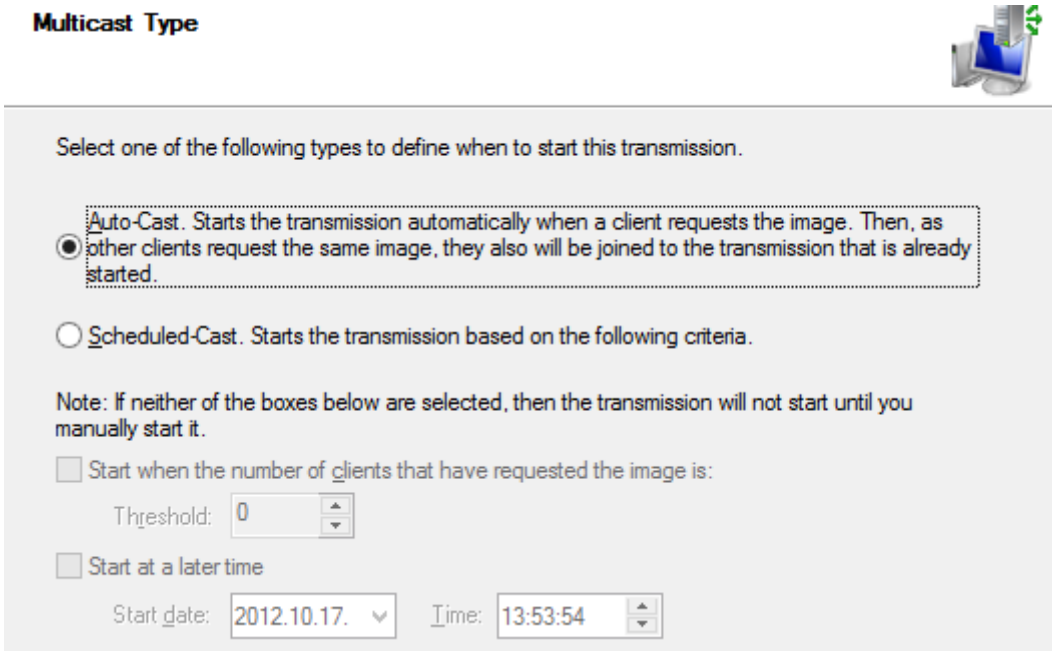
Sikeres visszatöltés után a felhasználók PXE induláskor már ki tudják választani a capture opciót is, és a megfelelően előkészített operációs rendszer partíciót a capture betömöríti egy új WIM állományba, majd feltölti a távtelepítési kiszolgálóra, ahol az install image-ek között meg is jelenik.

13.1.10 Csoportos küldés

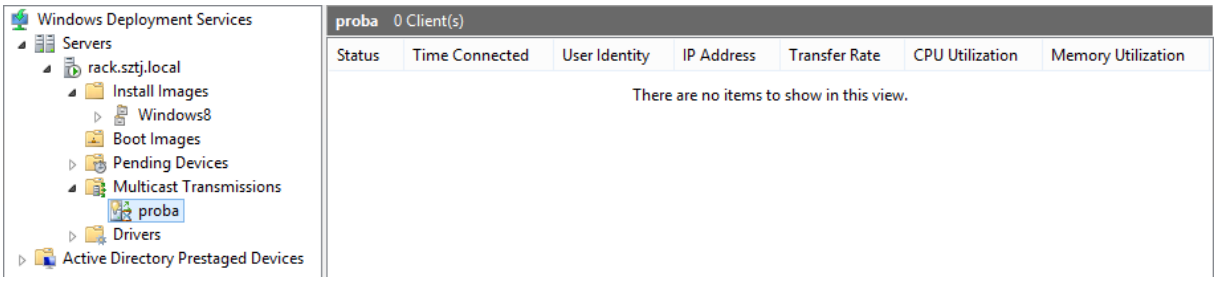
A WDS Transport Server használatával multicast címzés alapú csoportos küldést is indíthatunk, ha egy meglévő image-ből létrehozunk egy multicast transmission-t:



A multicast típusoknál választhatunk auto-cast módszert, ilyenkor mindegyik gép becsatlakozik menet közben a telepítésbe, illetve Scheduled-Cast-ot, amikor bizonyos feltételek teljesülésekor (időpont vagy gépszám) a telepítés automatikusan és egyszerre indul el. A második lehetőségbe a később indított kliensek már nem képesek becsatlakozni.



A multicast átvitel elindítása után a konzol láthatjuk az aktuálisan bejelentkezett klienseket, illetve kézzel el tudjuk indítani a Scheduled-Cast átvitelt is, ha esetleg kevesebb gépet szeretnénk telepíteni, mint kezdetben terveztünk:



14 PowerShell 3.0

A Windows Server 2012-ben a PowerShell használatával szerepköröket és szolgáltatásokat telepíthetünk, konfigurálhatunk, és egyéb kiszolgáló szoftvereket – Exchange, Sharepoint, System Center 2012 – üzemeltethetünk. A grafikus felület alkalmas a napi munkák elvégzésére, a PowerShell használatával pedig speciális feladatokat, vagy automatizálásokat hajthatunk végre. Bizonyos funkciókat pedig kizárólag PowerShellből tudunk elérni. A Windows Server 2012 üzemeltetéséhez hasznos, sőt, szinte elengedhetetlen a PowerShell ismerete.

14.1 Mi az a PowerShell?

A PowerShell sokkal több, mint egy egyszerű parancssori eszköz: Objektum-orientált üzemeltetési környezet, ahol a rendszergazdák scripteket hozhatnak létre, kötegelt módosításokat végezhetnek, és a grafikus felületen nem elérhető funkciókat használhatnak. Bizonyos programoknál (pl. Exchange) a grafikus felület (GUI) is a háttérben PowerShell cmdlet-eket futtat, sőt, ezeket a parancsokat le is menthetjük, ha az adott feladatot automatizálni szeretnénk. A PowerShellel hozzáférhetünk rengeteg objektumhoz, komponenshez, legyen az fájlrendszer, Active Directory, registry, tanusítványtár, stb.

A PowerShell szintaxisa az „ige-főnév”, pl. get-command vagy new-user. Az ige lehet get-, set-, new-, enable-, disable-, stb, a főnév pedig lehet bármilyen objektum, amit kezelni szeretnénk. Ezt a szerkezetet hívjuk cmdlet-nek. A cmdlet után következnek a paraméterek, amelyek parancsonként változnak, de a következő kategóriákba sorolhatók:

- Named: nevesített érték, pl egy könyvtár, vagy egy felhasználó neve
- Switch: kapcsoló, paramétert állít, pl. $true vagy $false
- Positional: a paraméter helyétől függően értelmezhető, pl. get-user –identity Gipszj helyett elég annyit írnunk, hogy get-user Gipszj. Mivel az első paraméter az identity, így nem kell külön kiírnunk.

14.1.1 Újdonságok a PowerShell 3.0-ban

A Windows Server 2012-ben megjelent 3-as verziójú PowerShell a következő újdonságokat tartalmazza:

- Több mint 260 alap cmdlet
- Az összes szerepkör és szolgáltatás kezelhető PowerShellből
- A Windows PowerShell Web Access-en keresztül biztonságosan, weboldalon keresztül futtathatunk scripteket távolról
- Időzített scriptek futtatása
- Online súgó
- Intelligens újracsatlakozás megszakadt távoli kiszolgálóhoz: újracsatlakozáskor a betöltött változók és az eddig használt parancsok megmaradnak

14.1.2 Alias-ok

Az aliasok egy már jól ismert parancs PowerShelles megfelelője, így az eddigi scriptjeinek, vagy megszokott parancsainkat továbbra is használhatjuk. A DIR parancs megfelelője a get-

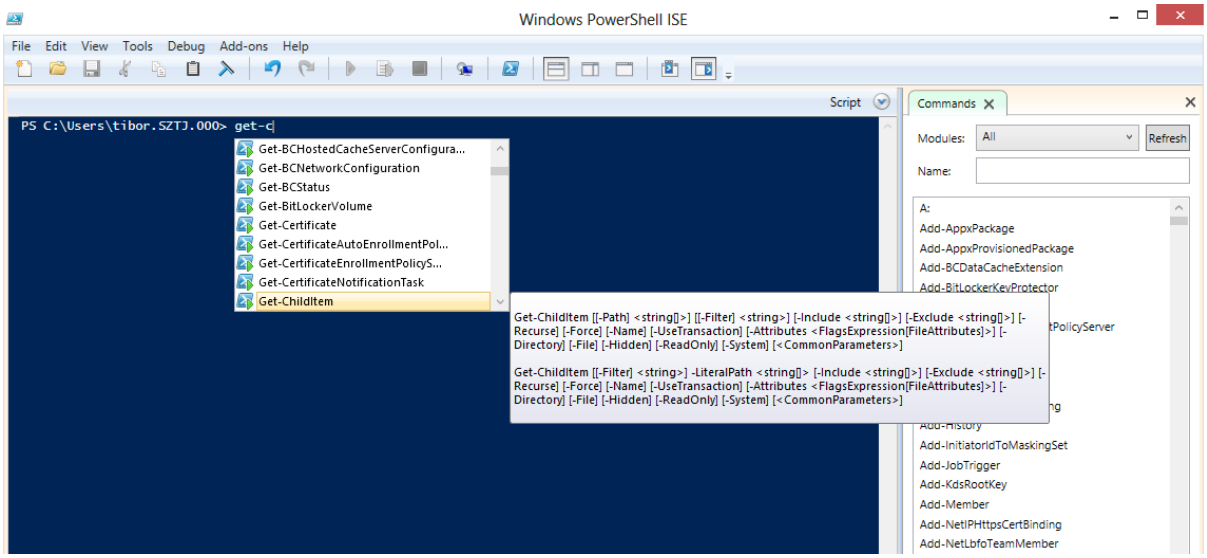
childitem, vagy a copy parancs cmdlete a copy-item. Teljes listát a get-alias parancs segítségével kérhetünk. Néhány példa:

- `kill -> Stop-Process`
- `move -> Move-Item`
- `rm -> Remove-Item`
- `type -> Get-Content`
- `help -> Get-Help`

14.1.3 PowerShell Integrated Scripting Environment (ISE)

A PowerShell ISE egy grafikus alkalmazás, beépített Intellisense-el PowerShell scriptek írásához, futtatásához, teszteléséhez. Funkciói:

- Szintaxis-színezés
- Tabulátoros kiegészítés
- Legördülő lista a parancsokhoz, paraméterekhez és értékekhez
- Intelligens parancs-keresés: ha csak nagyjából emlékszünk a PS cmdlet-re, az ISE felajánlja a hasonló parancsokat
- Elérési út megadásánál kiválaszthatjuk a megfelelő mappát.
- Változók betöltése: a $ jel után kilistázza a beépített, vagy általunk létrehozott változókat
- Parancsfüggő súgó
- Hibakeresés



A PowerShell ISE indításához nyissunk egy PS ablakot, és gépeljük be: ISE. A program megtalálható a Windows Server 2012 grafikus és ún. Minimal User Interface verziójában is, és a Windows 8-ban is.

Részletesebb leírás: http://blogs.msdn.com/b/powershell/archive/2012/06/13/intellisense-in-windows-powershell-ise-3-0.aspx

14.1.4 Súgó

A súgó eléréséhez írjuk be a get-help-et, utána a használni kívánt parancsot:

```
get-help Get-Certificate
```

Ha nem ismerjük a pontos cmdlet-et, használjunk helyettesítő karaktereket:

```
get-help *Certificate
```

A súgó részletességét is tudjuk szabályozni a következő paraméterekkel:

- -detailed: részletesebb súgó
- -examples: példákkal illusztrálva
- -full: teljes súgó, példákkal
- -online: böngészőben megnyitja a Microsoft Online Help oldalát a `cmdlet` szintaxisával

A számítógépünkön lévő súgót frissíthetjük az Internetről az `update-help` utasítással.

14.1.5 Modulok

A különböző szolgáltatások és szerepkörök telepítésével a PowerShell újabb modulokkal bővülnek. Ezek a modulok újabb cmdlet-eket tartalmaznak, az adott funkció felügyeletéhez. A Hyper-V telepítésével például feltelepül a Hyper-V nevű modul. Ezeket a modulokat betölthetjük az Import-module-al, illetve a betöltött modulokat kilistázhatjuk a get-module cmdlet-tel:

```
import-module activedirectory
get-module
```

Ha valamilyen cmdlet nem elérhető, akkor vagy nem töltődött be a modul, vagy nincs jogosultságunk az adott utasításhoz: A PowerShell csak azokat a parancsokat engedi használni, amihez jogosulstágunk van. Bizonyos alkalmazások telepítéséveé (pl. Exchange) a szükséges modulok automatikusan betöltődnek, így használhatjuk is a megfelelő cmdlet-eket.

14.1.6 Távoli PowerShell

A Remote PowerShell használatával távoli kiszolgálókra jelentkezhetünk be a PowerShell konzulunkkal, parancsokat futtathatunk, és az eredményt visszakapjuk a saját gépünkre. Ezzel egyszerűsítjük az üzemeltetést, nem kell távoli asztallal csatlakozunk a menedzselni kívánt kiszolgálóhoz, illetve egyszerre több kiszolgálót is üzemeltethetünk a saját gépünkről. Használatához szükségünk lesz Windows Remote Management-re (WinRM)

A WinRM egy web-alapú protokoll, egy fix portot használ, így akár tűzfalakon is képes átjutni. A forgalom HTTP protokollon utazik, titkosítatlanul az 5985-ös, titkosítva pedig az 5986-os TCP porton. A PowerShell saját maga is titkosítja az átküldött utasításokat és a válaszokat. A hitelesítéshez Active Directory-t és Kerberos protokollt használ, tartományi környezetben. Ha a távoli gépen engedélyeztük a WinRM-et (a Windows Server 2012-ben alapértelmezésként engedélyezett), akkor csatlakozni a következő cmdlet-tel tudunk:

```
Enter-PSSession –ComputerName távoli_számítógép
```

A PowerShell ISE konzolból a file menü/New Remote Powershell-el indítható a csatlakozás

14.1.7 Változók

A változók használatával adatokat tölthetünk be a memóriába, illetve lekérdezhetjük azokat egy adott PowerShell session-ben. Hasznos lehet, ha például össze szeretnénk hasonlítani értékeket, vagy az egyik script kimenetét szeretnénk betölteni változóba, és egy másik scriptben felhasználni. A változó mindig $ jellel kezdődik, utána pedig tetszőlegesen elnevezhetjük, pl. `$jelszo`. A változó tárolhat szöveget, számot, objektumot, tömböt, stb.

A feltöltés történhet a Set-Variable utasítással:

```
Set-Variable –Name ADDS –Value (Get-ADDomain)
```

vagy egy változó és egy érték definiálásával:

```
$ADDS = Get-ADDomain
```

A változókat használhatjuk számoláshoz is, pl:

```
> $A = 1
> $B = 2
> $A + $B
3
```

14.1.8 Pipeline

A PowerShell objektum-alapú környezet, így az egyik cmdlet eredményét, mint értéket betölthetjük egy másik cmdlet bemeneteként, pl. ha a tartomány összes fiókját szeretnénk engedélyezni:

```
get-aduser –filter * | enable-account
```

Mivel a betöltött érték nem szöveg, hanem objektum, arra is lehetőségünk van, hogy az objektum bármely attribútumát kezeljük. A pipe-ban lévő adatra a $_-al tudunk hivatkozni, és csak a parancs futásának idején érvényes változó. Például, ha le szeretnénk kérdezni a tiltott fiókokokat, és azokat engedélyezni, használhatjuk a Where-Object cmdlet-et:

```
Get-ADUser | Where-Object {$_.Enabled –eq $false} |  Enable-ADAccount
```

14.1.9 Kimenet formázása

A PowerShell kimenetét többféleképpen formázhatjuk:

- Format-list: A kimenetet lista formátumban írja ki. Kiválaszthatjuk, hogy melyik tulajdonságot szeretnénk megjeleníteni a –property kapcsoló megadásával, illetve használhatjuk az FL aliast is a Format-List helyett. Pl:

```
[dell]: PS C:\Users\tibor\Documents>  get-aduser tibor |fl


DistinguishedName : CN=Szentgyörgyi Tibor,CN=Users,DC=sztj,DC=local
Enabled           : True
GivenName         : Szentgyörgyi
Name              : Szentgyörgyi Tibor
ObjectClass       : user
ObjectGUID        : a9e53b2e-d2af-4ab1-a817-9b4d55d912b9
SamAccountName    : tibor
```

```
SID               : S-1-5-21-2421604837-3390990232-3674951276-1109
Surname           : Tibor
UserPrincipalName : tibor@sztj.local
```

- Format-table: Az eredményt táblázatos formában jeleníti meg, minden érték külön oszlop. Itt is használhatjuk a –property értéket,. és az FT rövidítést:

```
get-aduser tibor |ft -Property Name,userprincipalname
Name                                               userprincipalname
Szentgyörgyi Tibor                                 tibor@sztj.locall
```

- Format-wide: minden objektum egy tulajdonságát kérdezi le, amit a –property értékkel definiálunk:

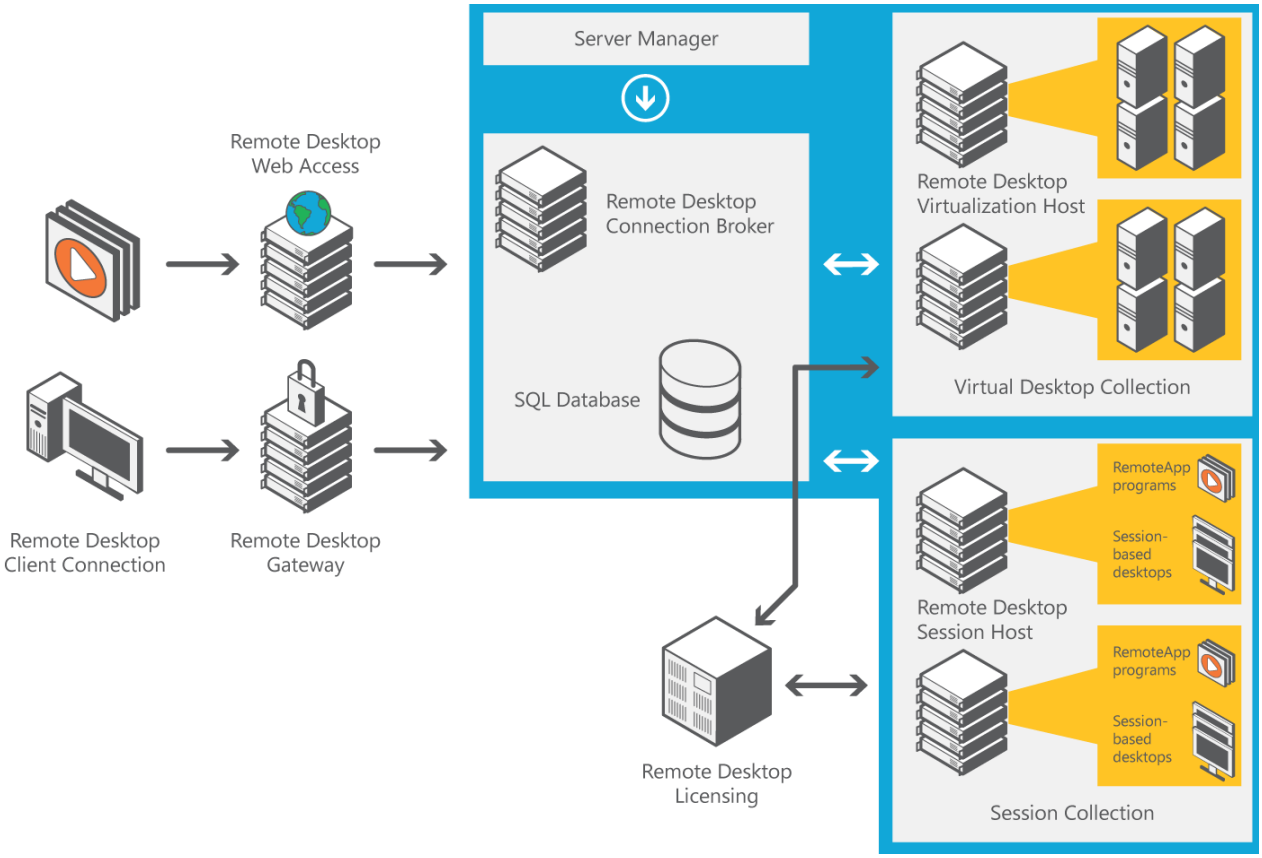
```
get-aduser  -Filter * |fw -Property Name


Guest                                               krbtgt
Administrator                                       Szentgyörgyi Tibor
Filkor Csaba
```

15 Távoli asztal szolgáltatások

A Windows Server 2012 távoli asztal szolgáltatások (RDS) segítségével távoli felhasználók csatlakozhatnak a kiszolgáló asztalához, kliens gépeikhez, vagy virtuális gépekhez, futtathatnak alkalmazásokat, anélkül, hogy a saját gépükre telepíteni kellene bármit. A RDS előnye, hogy az infrastruktúránkat központilag tudjuk felügyelni, az adatok a kiszolgálóinkon biztonságos helyen tárolódnak, a felhasználók pedig bárhonnan, bármilyen eszközről bejelentkezve ugyanazt a felhasználói élményt kapják. Ebben a részben végignézzük az RDS kiszolgáló komponenseit lépésről-lépésre, illetve kiépítünk egy komplett RDS és VDI környezetet.

15.1.1 Komponensek



A Remote Desktop Services komponensei

A Távoli asztal segítségével a felhasználók alkalmazásokat futtathatnak, vagy távoli számítógépeket érhetnek el RDP protokoll használatával. Az alkalmazások futhatnak Remote Desktop Session Host-on (RDSH), ebben az esetben egy kiszolgálót több felhasználó ér el egyidejűleg. A közösen használt RDSH kiszolgálón a felhasználók nem kaphatnak rendszergazdai jogot, illetve néhány program nem biztos, hogy fut Windows Server 2012 alatt. A másik lehetőség, hogy a felhasználók virtuális gépeken a már megszokott Windows 7/ Windows 8 felülettel találkoznak, és akár rendszergazda jogot is kaphatnak. Ezt a környezetet Remote Desktop Virtualization Host-nak (RDVH) nevezzük.

Arra is lehetőségünk van, hogy az alkalmazásainkat weboldalon keresztül kiajánljuk a felhasználóknak (Remote Desktop Web Access), vagy a helyi gép start menüjében a programok között elhelyezzük a távoli kiszolgáló alkalmazásait (RemoteApp), ilyenkor a felhasználó

számára még egységesebb felületete hozhatunk létre, hiszen az alkalmazottak nem is tudják, hogy az adott alkalmazás a helyi gépükön, vagy a központi kiszolgálón fut.

Ha több RDSH és RDVH kiszolgálót használunk, a felhasználók csatlakozási pontjánál érdemes telepítenünk egy Remote Desktop Connection Broker-t, ami a bejövő kéréseket továbbítja a megfelelő kiszolgálónak, kezeli a kapcsolatok újraépítését, és terheléselosztást valósít meg.

A Remote Desktop Gateway biztonságos hozzáférést biztosít a belső kiszolgálóinkhoz az Internetről: szabályozhatjuk, kik és hogyan férjenek hozzá a serverekhez, és HTTPS csatornába csomagolja az RDP forgalmat.

A Remote Desktop Licensing kiszolgálóval pedig egy helyről kezelhetjük az összes Remote Desktop licencünket.

15.1.2 Egyszerűbb üzembe helyezés

A Windows Server 2008-cal szemben a Windows Server 2012-ben egyszerűbbé vált a fent felsorolt szolgáltatások telepítése és beállítása. Amíg az előző verzióban a szerepköröket külön telepítettük és állítottuk be, a 2012-ben csak ki kell választanunk a megfelelő forgatókönyvet, és a szükséges szerepköröket a varázsló feltelepíti:

- Virtual desktop deployment: a VDI egyszerű telepítésénél a varázsló egy gépes környezetben összeállítja a komplett VDI infrastruktúránkat (Quick Config), nekünk már csak a virtuális gépeket kell előkészítenünk, illetve az egyéni alkalmazásainkat telepíteni. VDI telepítésekor két tipusú virtuális gép gyűjtemény közül választhatunk:

Pooled Collection	**Personal Collection**
Egy megosztott virtuális gép, több példányban fut különbözeti lemezeken.	Minden felhasználónak külön virtuális gépe van
a módosítások nem tárolódnak kilépéskor, de a felhasználói beállításokat külön VHD-ban tárolhatjuk (User Profile Disk)	Kilépéskor a módosítások megmaradnak
csak egy virtuális gépet kell kezelnünk, pl frissítéseket telepíteni, alkalmazásokat frissíteni, stb.	Központilag kell frissítenünk és kezelnünk a gépeket, akár WSUS-ból, akár System Center 2012-ből
Kevesebb helyet foglalhat	A felhasználók rendszergazda joggal rendelkezhezhetnek, programokat telepíthetnek, beállításokat módosíthatnak

A közös virtuális gépeknél tehát ugyanazt a virtuális gépet különböző időben különböző felhasználók használhatják, és a gépen végzett beállítások kilépéskor törlődnek. Így 100 virtuális gépek 3 műszakban akár 300-an is használhatnak. A felhasználók beállításait - a c:\users\felhasználónév mappát – pedig tárolhatjuk külön VHD állományban, így bármelyik viruális gépre bejelentkezve a felhasználó ugyanazt a profilt kapja meg.

A személyes virtuális gép akkor hasznos, ha a felhasználók a beállításaikat, programjaikat és adataikat saját gépen szeretnék tárolni. Ebben az esetben, az Active Directoryban mindegyik felhasználóhoz saját VDI gépet rendelhetünk. Ezek a virtuális gépek nem futnak folyamatosan

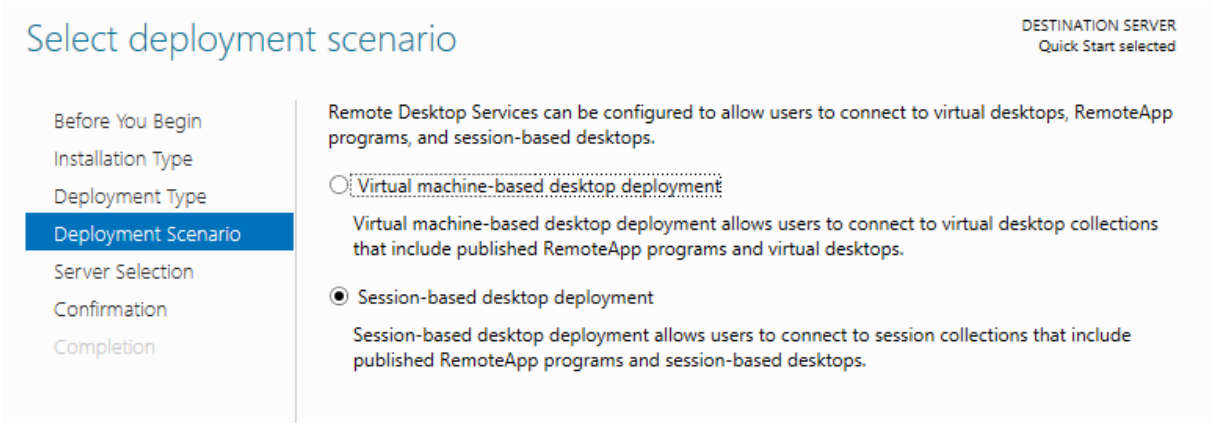
a Hyper-V hosztokon, a felhasználó kijelentkezése után mentésre kerülnek, és lekapcsolódnak. Adattárolás szempontjából sokkal több helyet foglalhatnak, de ha használjuk a Windows Server 2012 data deduplication szolgáltatását, ezt a helyet erősen leredukálhatjuk, hiszen a különböző VHD-k tartalma nagyrészben megegyezik.

- Session Virtualization Deployment: ebben a forgatókönyvben telepítésre kerül a Remote Desktop Session Host, a Licensing Server, Connection Broker, RD Gateway, és az RD Web Access, tehát minden szükséges komponens. Beállításukat egy egységes felületen tudjuk kezelni a Server Managerben. RDS telepítésénél is választhatunk standard vagy Quick telepítést, az első esetben több kiszolgálóból álló farmot, a második esetben egy kiszolgálók környezetet hozunk létre.

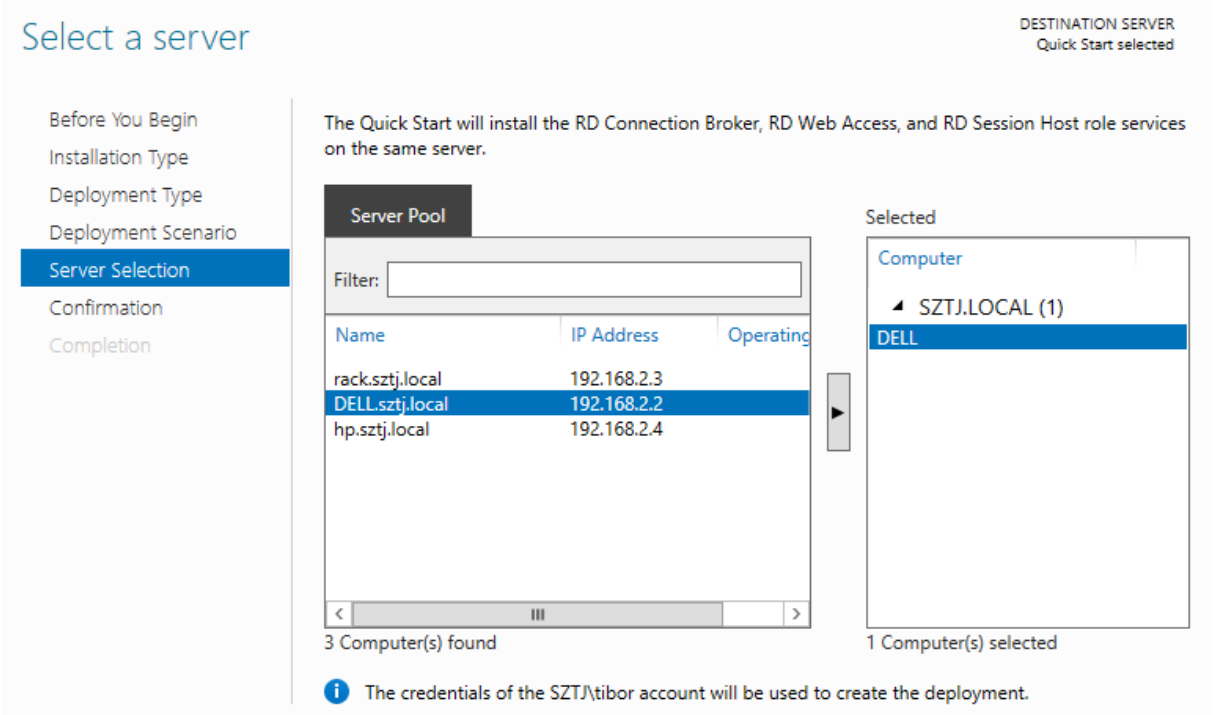
15.2 Telepítés

Egy tartományba, de külön fizikai gépekre telepíthetünk VDI és RDS rendszert is.

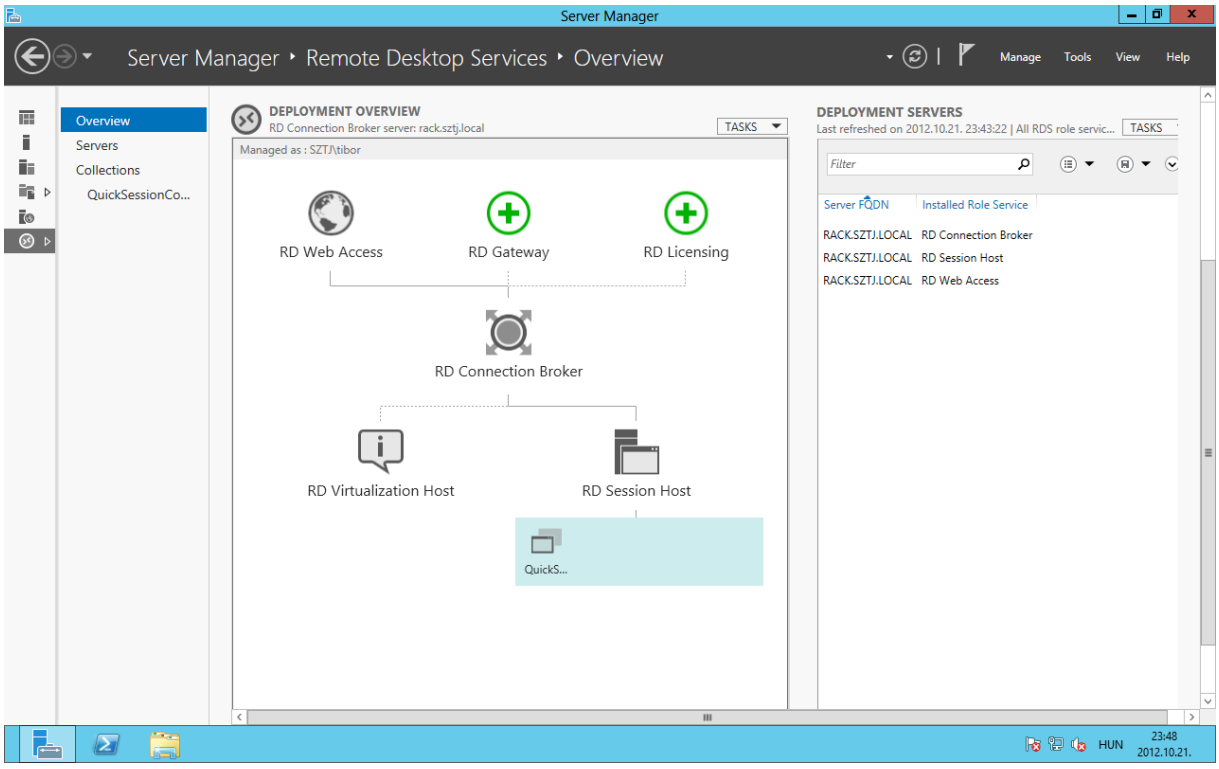
Az első részben a Session Virtualization-t nézzük végig: A Server Manager/Add Roles varázslójából először válasszuk a Remote Desktop Services installation menüpontot, majd a Quick Startot, ha szeretnénk minden szolgáltatást egy gépre telepíteni, vagy a Standard deployment-et, ha a különböző szolgáltatásainkat szét szeretnénk osztani különböző szerverekre. Mi most a Quick startot mutatjuk be. Az RDS telepítéséhez, a következő képernyőn válaszzuk a session-based dektop-deployment lehetőséget:



A Quick start tehát feltelepíti az RD Connection Brokert, az RD Web Access-t a hozzá kapcsolódó IIS szolgáltatásokkal, és az RDSH szerepköröket.



Sikeres telepítés után az RDS kiszolgálót a Server Manager/Remote Desktop Services részében konfigurálhatjuk:

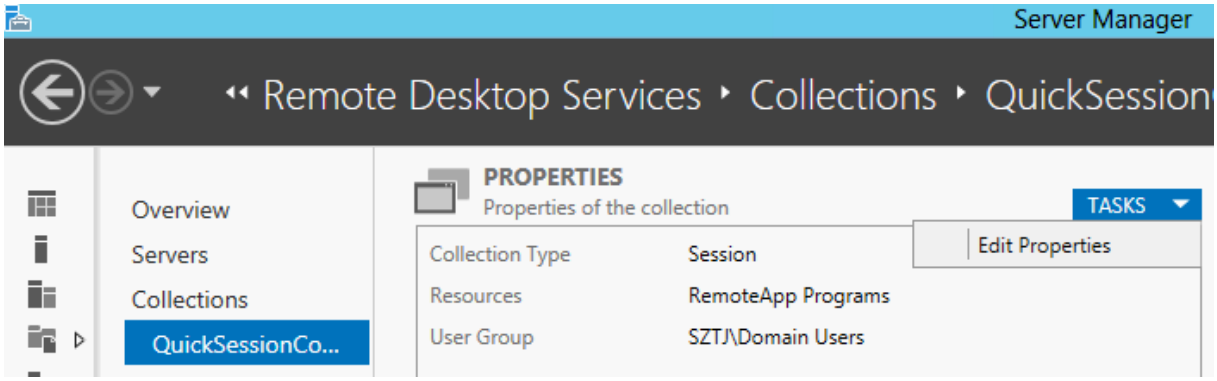


Az összefoglaló képernyőn láthatunk egy összefogó képet az infrastruktúránkról. Mint láthatjuk, az RD licensing és az RD Gateway további beállítást igényel. Létrejött azonban egy ún. QuickSessionCollection, ahol a következőket módosíthatjuk:

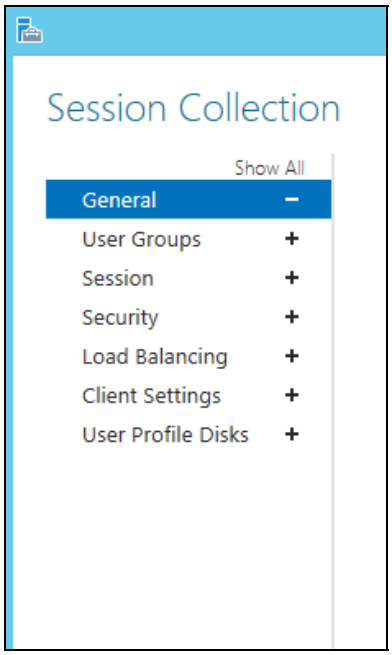
- Properties: az RDS kiszolgáló alapbeállításait, csoportjogosultságokat, kliens-beállításokat, User Profile Disk, stb.

- RemoteApp Programs: alkalmazásokat publikálhatunk a Remote Web Access felületre, illetve a kliens gépekre
- Host Servers: további RDSH gépeket adhatunk hozzá a collection-höz.

Nézzük a collection tulajdonságait: a QuickCollectionSet Properties részében indítsuk el az Edit properties taszkot:

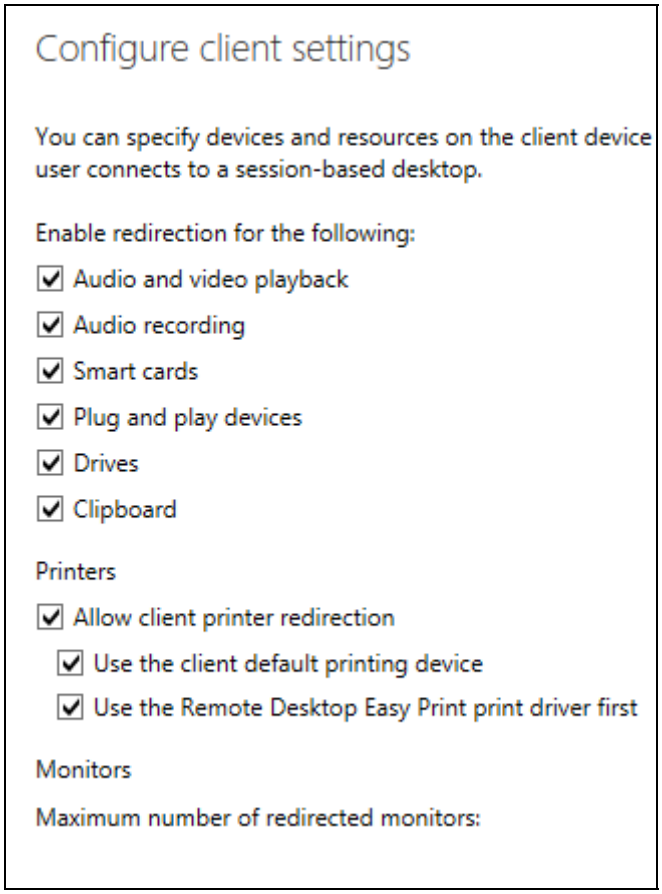


A collection tulajdonságainál a következő beállításokat találjuk:

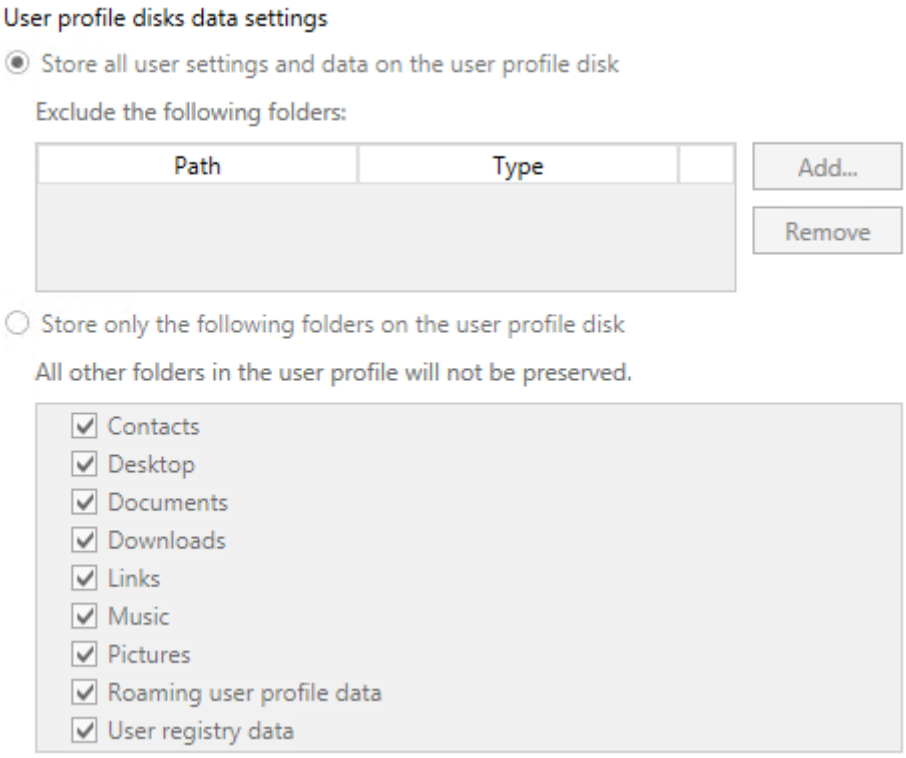


- General: a Collection neve
- User Groups: milyen csoportok csatlakozhatnak a távoli asztali kiszolgálóhoz, és futtathatnak RemoteApp programokat. Érdemes létrehozni egy külön RDS users csoportot, és ezen a csoporton keresztül kezelni a jogosultságokat.
- Session: aktív és üresjárati időkorlátot adhatunk a távoli felhasználóknak, megadhatjuk, hogy a lecsatlakozott munkameneteket a rendszer bizonyos idő után fejezze be (jelentkeztesse ki a felhasználót, illetve az átmeneti fájlokat szabályozhatjuk
- Security: hitelesítési és vonal-titkosítási szinteket állíthatunk, és a hálózati szintű hitelesítést (NLA) engedélyezhetjük vagy tilthatjuk. NLA használatához legalább 7.0-ás remote desktop client-et kell használnunk

- Load Balancing: ha több RDSH kiszolgálónk van, megadhatjuk, hogy melyik hoszton mennyi kapcsolatot engedélyezünk, illetve mi legyen a kiszolgáló relatív terhelése a többi kiszolgálóhoz képest.
- Client Settings: megadhatjuk, hogy a felhasználók milyen eszközöket használhatnak, pl nyomtató, PnP eszközök, hang, stb.



User Profile Disks: itt engedélyezhetjük a felhasználói profil lemezeket, megadhatjuk a hálózati elérést, ahol a VHD fájlt szeretnénk tárolni, ami tartalmazza a profilokat (pl. a felhasználó kezdőkönyvtára, vagy profilmappája), illetve maximális méretet adhatunk a VHD fájlnak. Megadhatjuk, hogy minden, a profilban tárolt tartalom költözzön a VHD-ba, vagy csak megadott mappák, vagy minden mappa, kivéve, amit kizárunk:

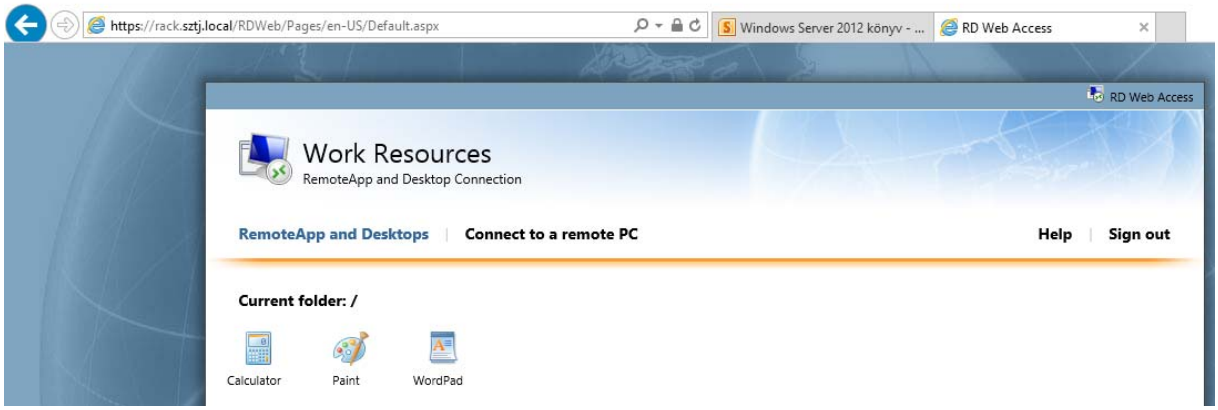


Miután a Collection beállításait megadtuk, már csak fel kell telepítenünk az egyéni alkalmazásainkat az RDSH hosztokra, amit szeretnénk, hogy a felhasználók elérjenek, és már használhatjuk is az RDS infrastruktúránkat

15.2.1 RemoteApp Programok

A RemoteApp alkalmazások a felhasználó számára helyileg futó programnak tűnnek, tehát nem kell bejelentezniük egy másik, távoli asztalra, hanem a helyi programok közül kiválasztja a távoli alkalmazást, ami képes együtt működni a helyi asztallal, nyomtatóval, stb.

A publikált RemoteApp programokat a felhasználók elérhetik akár az RD WebAccess felületről:

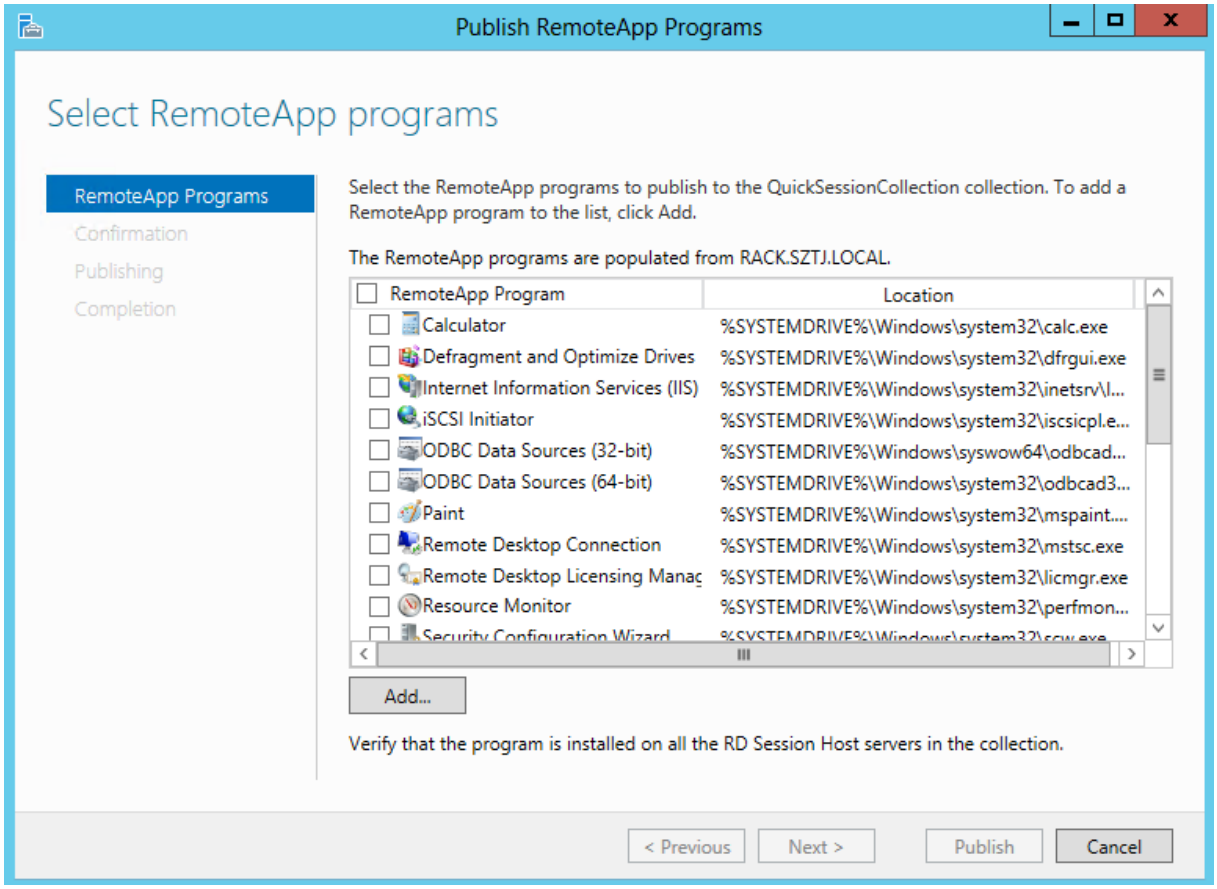


vagy Windows 7 és Windows 8-nál a vezérlőpult/RemoteApp alkalmazásoknál, illetve, ha csoportházirenből kiküldtük, akkor akár a helyi gép start menüjéből is. Amikor a felhasználó elindít egy RemoteApp programot, a háttérben megtörténik az RDP bejelentkezés, majd a

távoli alkalmazás megjelenik a helyi asztalon, ahol szabadon átméretezhetjük, tálcára tehetjük, stb. A második RemoteApp program futtatásakor már nem történik újabb bejelentkezés, ezért ez a program már sokkal gyorsabban indul.

15.2.2 Alkalmazások publikálása RemoteApp-on keresztül

A Server Managerben, a QuickSessionCollection résznél a RemoteApp programs résznél van lehetőségünk további alkalmazásokat publikálni, illetve a publikált programokat eltávolítani:



Választhatunk a felajánlott listából, vagy egyéni alkalmazásokat is tallózhatunk, illetve egyszerre több alkalmazást is publikálhatunk. Publikálás után az alkalmazás megjelenik mind az RD Web Acces oldalunkon, illetve a kliens gépeken is, ha feliratkoztunk az adott kiszolgáló RemoteApp programjaira.

15.2.3 RemoteApp program tulajdonságai

Ha megnyitjuk egy RemoteApp program tulajdonságait, a következő beállításokkal találkozunk:

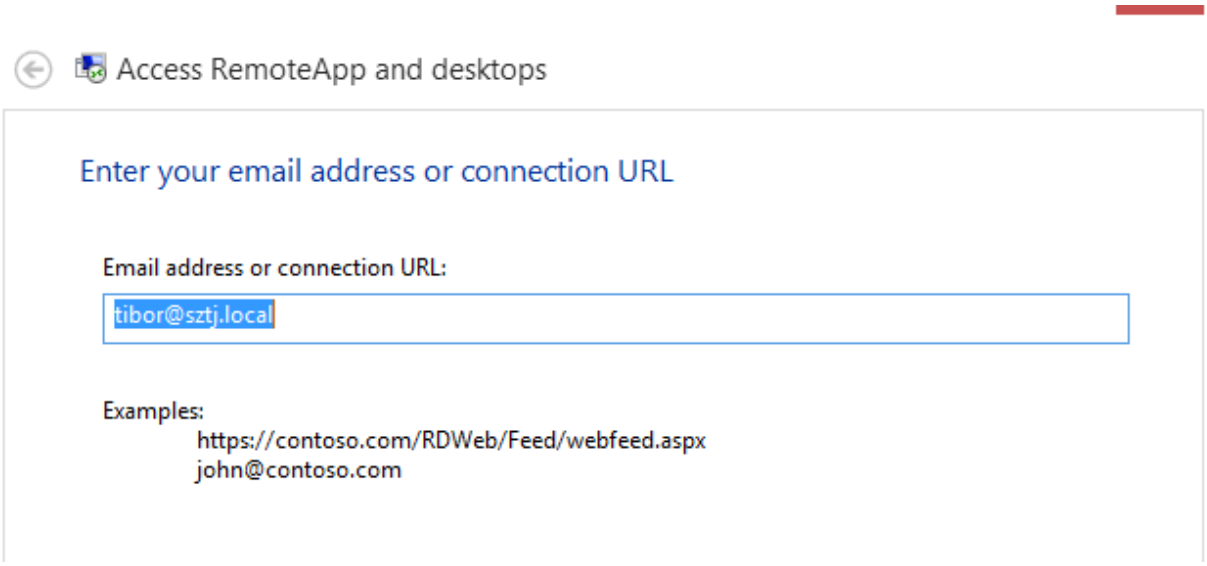
- General: a program nevét és ikonját módosíthatjuk, illetve engedélyezhetjük, hogy megjelenjen-e az RDWeb-en.
- Parameters: parancssori kapcsolókat adhatunk a programnak, és engedélyezhetjük, hogy a felhasználók adhassanak-e meg egyéni kapcsolókat
- User Assigment: felhasználói és csoportszinten engedélyezhetjük a programot. Egy Server Managert például érdemes korlátozni, hogy csak a rendszergazdák lássák, és

futtathassák, egy számlázó, könyvelő programnál pedig pl. a pénzügy csoportnak adhatunk engedélyt a program futtatására.

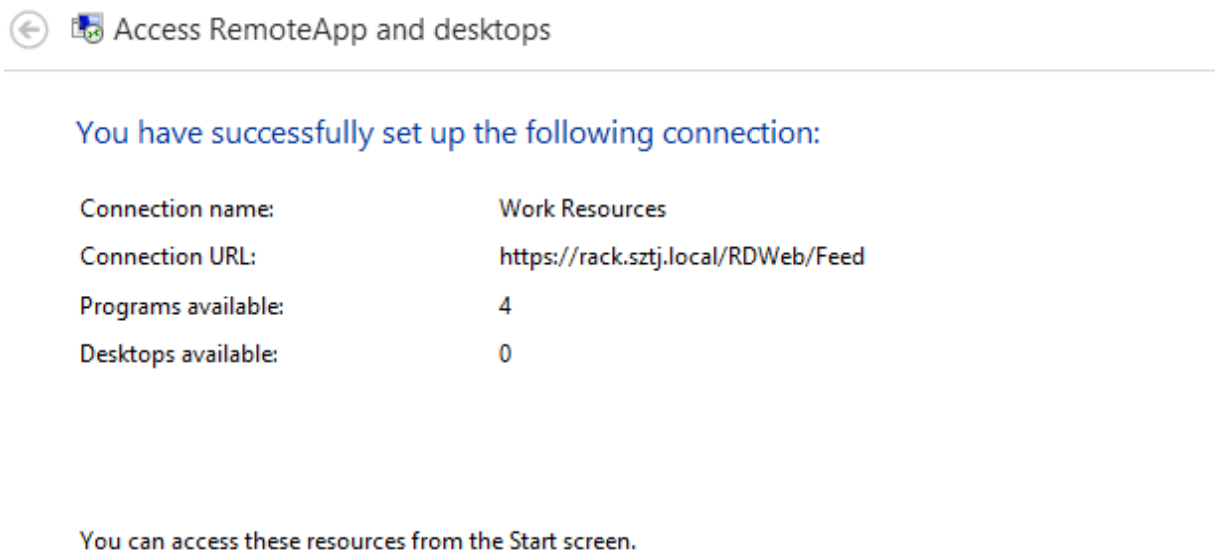
- File type Association: fájlkiterjesztésekhez rendelhetünk különböző RemoteApp programokat. Ez a funkció az RDWeb-nél nem érhető el, csak azokról a kliens gépekről, ahová csoportházirendből publikáltuk. Ehhez egy új csoportházirend-objektumot kell létrehoznunk a tartományban, és a to **User Configuration** -> **Policies** ->**Administrative Templates** -> **Windows Components** -> **Remote Desktop Services** -> **RemoteApp and Desktop Connections** résznél a **Specify Default Connection URL** értékékét kell beállítánunk valami ilyesmire: **https://RDWA1.corp.contoso.com/RDWeb**

15.2.4 RemoteApp programok elérése Windows 8-ból

Ha az alkalmazásainkat publikáltuk az RDS kiszolgálón, akkor a Windows 8-as gépeken lehetőségünk van feliratkozni ezekre a programokra, a vezérlőpult/RemoteApp programs résznél, ha az Access RemoteApp and desktops részt választjuk:

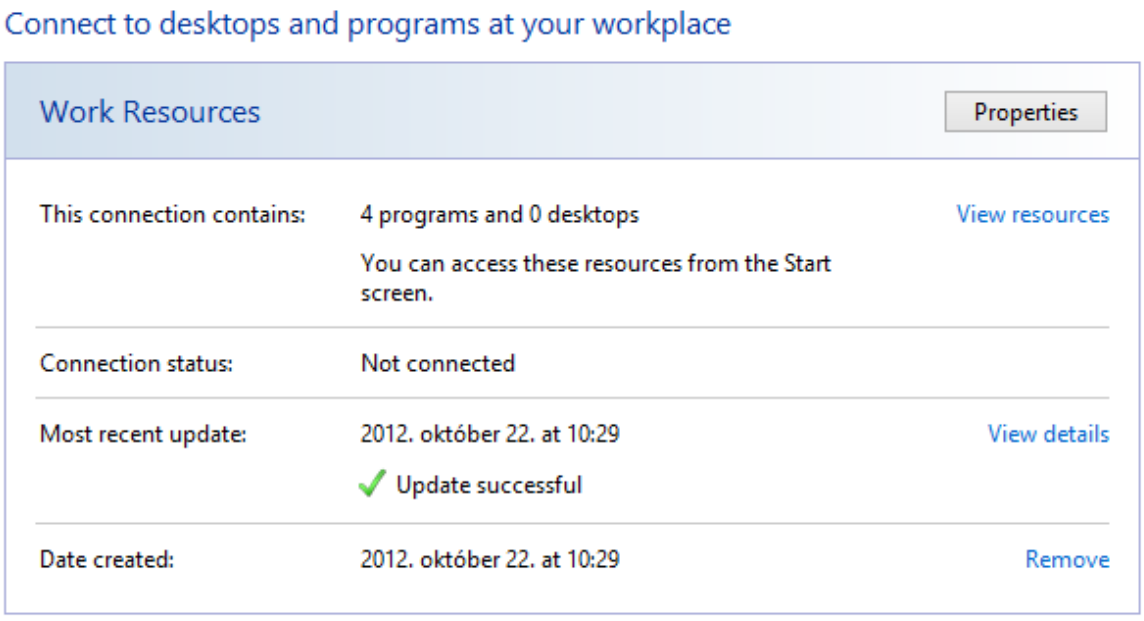


Miután megadtuk az e-mail címünket, a rendszer megtalálja a tartományban a RemoteApp feed-et, amire feliratkozva elérhetjük a publikált alkalmazásokat. Ha a kiszolgáló megtalálta a Connection URL-t, sikeresen csatlakoztunk a RemoteApp-hoz:



Ahhoz, hogy a felhasználók fel tudjanak iratkozni a RemoteApp csatornára, a DNS-ben létre kell hoznunk egy TXT rekordot, amely tartalmazza a RemoteApp kiszolgáló feed elérési útját: A DNS-ben, a tartományunk kiválasztása után hozzunk létre egy új TXT tipusú rekordot. A Rekord neve legyen **_msradc**. A szöveg részbe adjuk meg a kiszolgálónk RDWeb elérési útját, pl.: https://RDWA1.corp.contoso.com/RDWeb/Feed

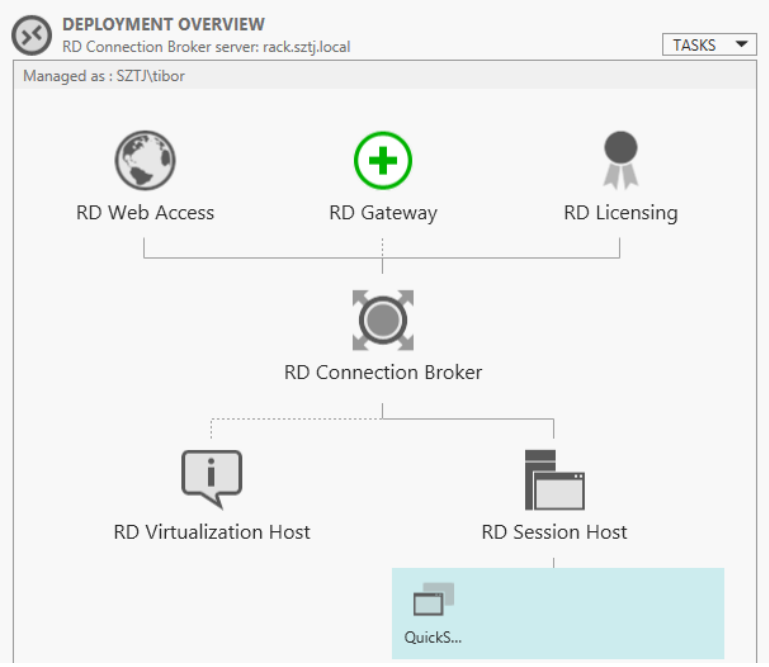
Ha mindent sikeresen beállítottunk, a vezérlőpult RemoteApp részénél láthajtuk a publikált alkalmazásainkat, illetve működni fog a fájlkiterjesztés alapú program-választás is:



15.3 RD Gateway

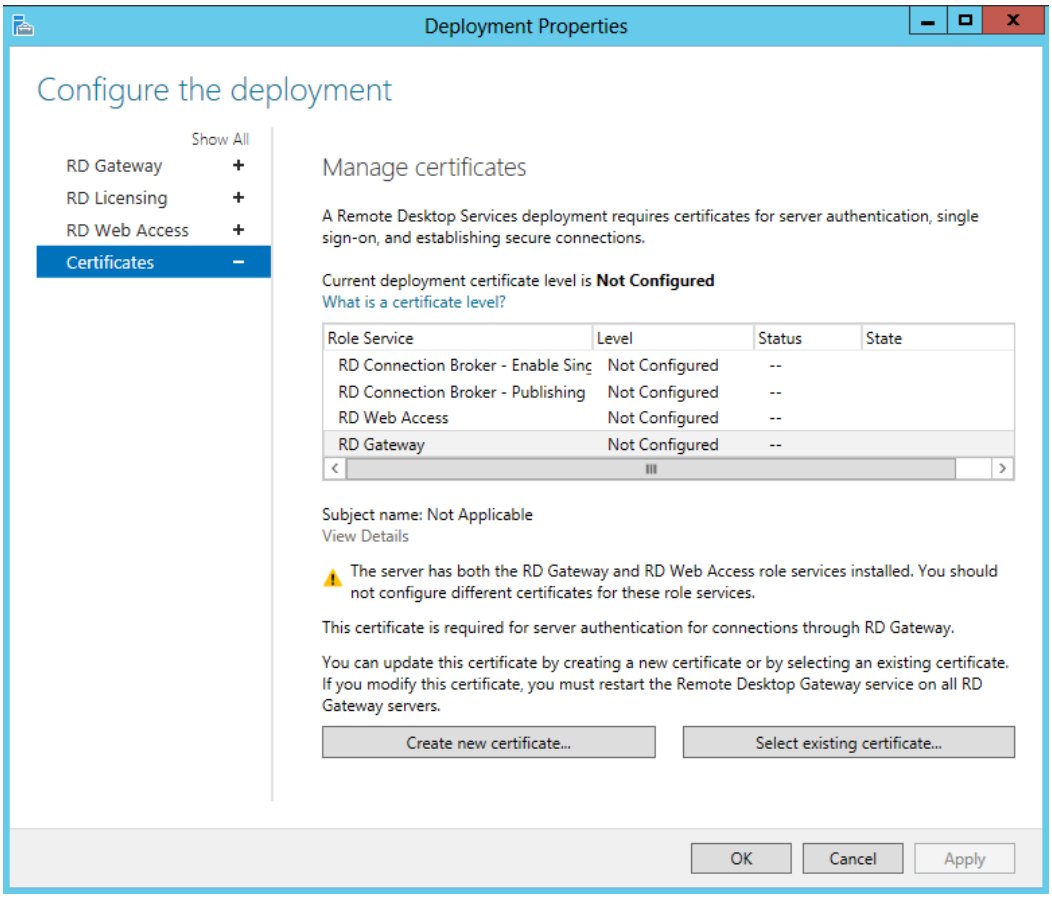
A Remote Desktop Gateway biztonságos hozzáférést biztosít a belső hálózatunk RDP kiszolgálóihoz, szabályozhatjuk a felhasználókat, a használt szolgáltatásokat, illetve titkosíthatjuk a

távelérési forgalmat. Telepítését a Server Manager/Remote Desktop Services részénél tudjuk indítani, az RD Gateway-ra klikkelve:



Miután kiválasztottuk a kiszolgálónkat, ahová RD Gatewayt szeretnénk telepíteni, meg kell adnunk a kiszolgáló külső nevét. Ehhez a névhez megfelelő tanúsítvánnyal kell rendelkeznünk, ha külső felhasználók csatlakoznak, akkor publikus tanúsítványt érdemes vásárolnunk.

Telepítés végén kiválaszthatjuk a megfelő tanúsítványt, illetve később is, ha a Collection tulajdonságain az Edit Deployment taszkot választjuk:

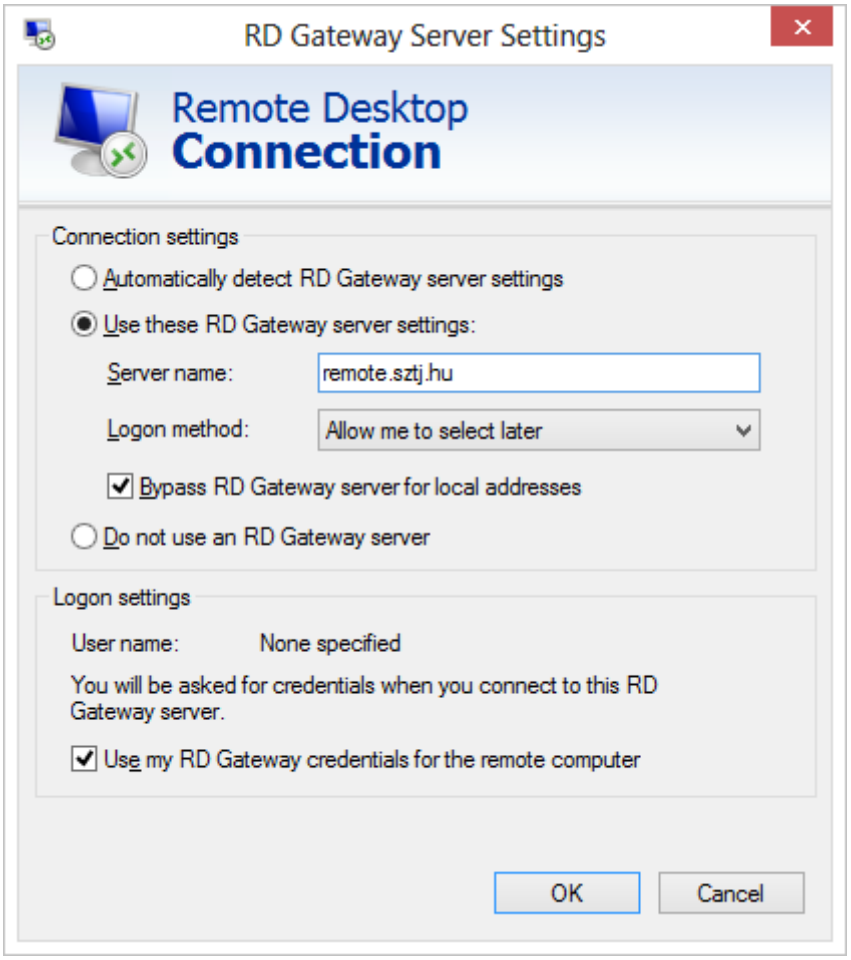


Ezen a konzolon (az Exchange 2010-hez hasonlóan) egy egységes felületen állíthatjuk be az összes tanúsítványt:

- létrehozhatunk önkiállított tanúsítványt
- importálhatjuk a megvásárolt tanúsítványainkat
- láthatjuk a tanúsítványaink állapotát,

Ha feltelepítettük és beállítottuk az RD Gateway szolgáltatásunkat, akkor a kliens oldalon, a csatlakozáskor is meg kell adnunk mind a belső kiszolgáló nevét, mind az átjáró külső DNS nevét. A külső néven megfelelő, elfogadott tanúsítványnak kell lennie.

A remote desktop kliens advanced fülén a Connect from anywhere résznél adhatjuk meg az átjáró nevét:


RD Gateway Server Settings
Remote Desktop
Connection
Connection settings
Automatically detect RD Gateway server settings
Use these RD Gateway server settings:
Server name:
remote.sztj.hu
Logon method:
Allow me to select later
Bypass RD Gateway server for local addresses
Do not use an RD Gateway server
Logon settings
User name:
None specified
You will be asked for credentials when you connect to this RD Gateway server.
Use my RD Gateway credentials for the remote computer
OK
Cancel

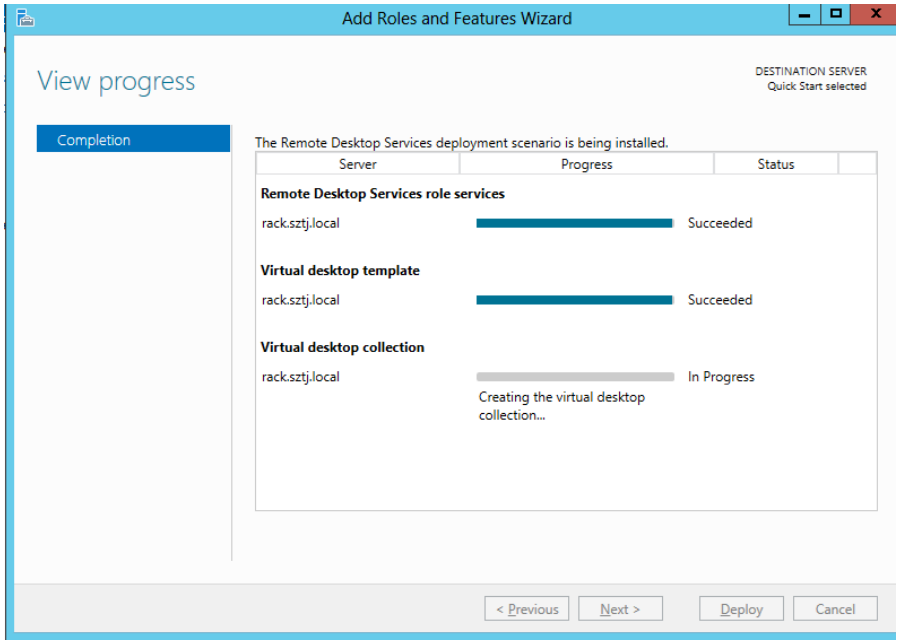
16 VDI

A Session Virtualization szolgáltatás mellett a távoli asztal másik alapköve a Virtual Desktop Infrastructure. Ebben a forgatókönyvben a virtuális gépen futú személyes vagy közösen használt kliens gépekhez csatlakoznak a felhasználók távoli asztalon (RDP), vagy akár a virtuális klienseken futó alkalmazásokat érik el RemoteApp segítségével. A telepítés megkezdése előtt elő kell készítenünk egy virtuális kliens gépet, ún. gold image-t. A gépre fel kell telepítenünk az összes alkalmazást, amit a felhasználók használni fognak, majd a sysprep segítségével le kell zárnunk. A VDI telepítője kérni fogja ezt a gold image-et, és ebből fogja létrehozni a szükséges számú virtuális kliens gépet.

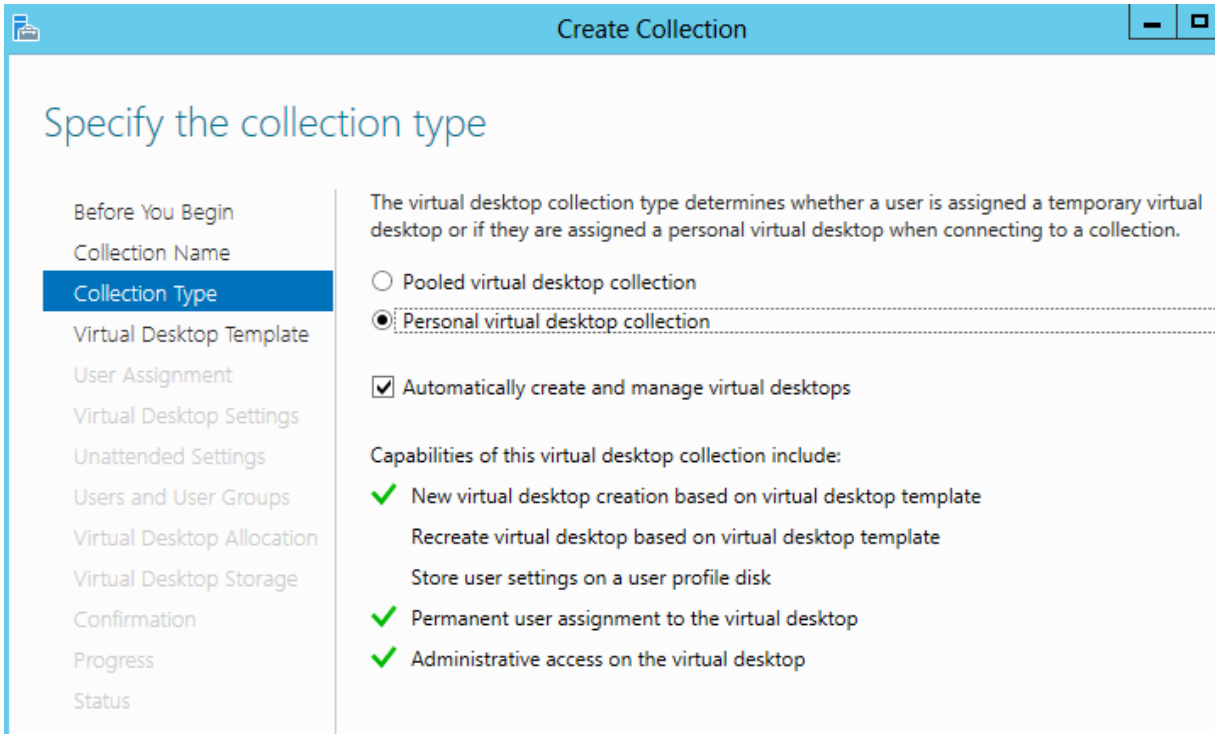
A telepítés megkezdéséhez indítsuk el a Server Manager / Add Roles varázslóját, majd a remote desktop services installation lehetőséget, azon belül a Quick Start-ot. A virtual machine-based deployment után megadhajtuk a kiszolgálóinkat, amelyeket szeretnénk bevonni a VDI infrastruktúrába, majd ki kell választanunk a virtuális gépek sablonaként használandó VHD állományt. Ha ezzel megvagyunk, már kész is a VDI környezetünk.

Nézzük, a varázsló milyen konfigurációkat hoz létre:

- Ha nem talált a hálózaton, akkor feltelepíti az RD Connection Broker-t
- Telepíti az RD Web Access-t és az RD Virtualization Host-ot.
- létrehozza a virtuális gép sablont
- Létrehoz egy collection-t QuickVMCollection néven.



Ebben a gyűjteményben közös virtuális gépek jöttek létre.
Hozzunk létre egy új Collection-t:
A collections menüben a Task fülön hozzunk létre egy új collection-t:
Miután megadtuk a gyűjtemény nevét, ki kell választanunk, hogy milyen típusú gépeket szeretnénk használni, közös, vagy személyes:



A varázsló felsorolja mindkét választás előnyeit, illetve automatikusan létrehozza a virtuális gépeket. A hyper-V managerben sem a telepítés alatt, sem később nem kell semmilyen konfigurációt módosítanunk, minden beállítást a VDI felületről végezhetünk el.

Ki kell választanunk a virtuális gép sablonunkat (QuickMasterVM), amiből az új virtuális gépek származnak (különbözeti VHD jön létre minden új virtuális géphez), majd megadhatjuk, hogy a felhasználó-gép összerendelés automatikus legyen-e (javasolt), és hogy a felhasználók rendszergazdai joggal bírjanak a személyes virtuális gépeiken.

A következő lépésben betölthetjük az előre elkészített telepítési válaszfájlunkat, vagy ha nincs ilyen, a varázslóval létrehozhatunk egyet. Ez a válaszfájl tartalmazza az időzóna beállítását, illetve a számítógépek helyét az Active Directoryban.

A válaszfájl után meg kell adnunk, hogy kik használhatják a VDI gépeket, itt érdemes létrehozni egy külön VDI users csoportot, definiálhatjuk a virtuális gépek számát, illetve elnevezését.

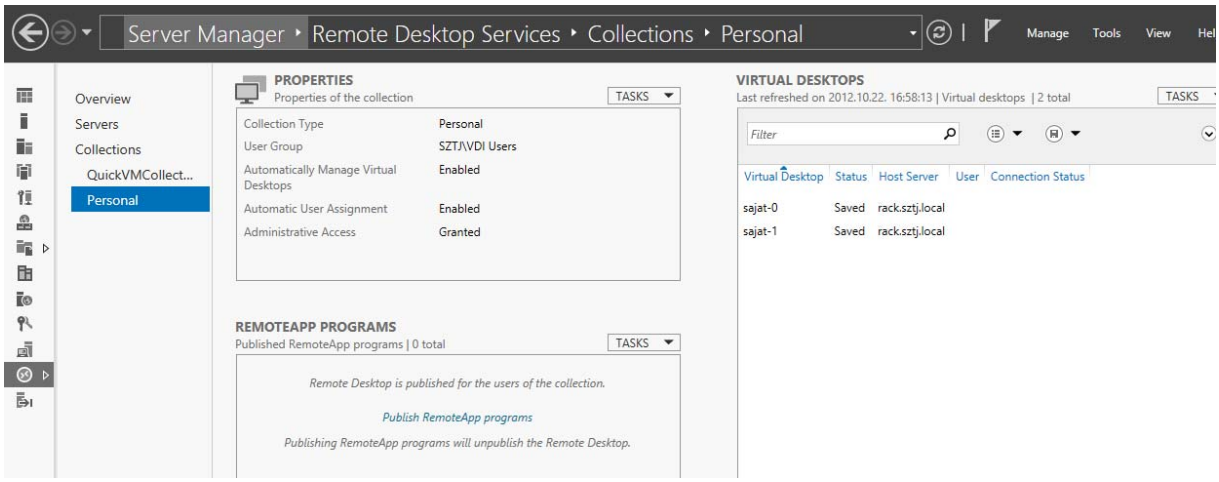
A Virtual Desktop Allocation-nál elhelyezhetjük a virtuális gépeinket a különböző RD Virtualization Host-okon, ha van ilyenünk,

A Virtual Desktop Storage-nál megadhatjuk, hogy a különbözeti VHD-kat helyi gépen, megosztott mappán vagy fürtözött adattárolón szeretnénk tárolni. Az SMB megosztásokon tárolt VHD újdonság a Windows Server 2012-ben, használatához SMB3.0-ás, vagyis Windows Server 2012-es fájlkiszolgáló vagy fájlkiszolgáló-fürt szükséges.

Az összefoglaló képernyő után pedig már készül is a személyes virtuális gép alapú VDI collection-ünk: a varázsló exportálja a virtuális gép sablonunkat, majd importálja annyi példányban, amennyi VDI gépet kértünk a gyűjteménybe.

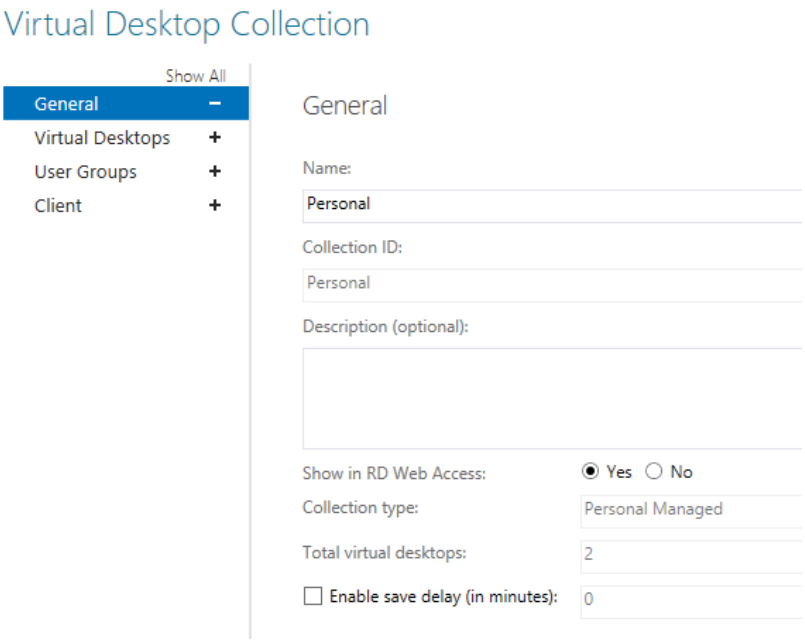
16.1.1 VDI Kezelése

Ha létrejött a személyes virtuális gép gyűjteményünk, nézzük a beállításait:

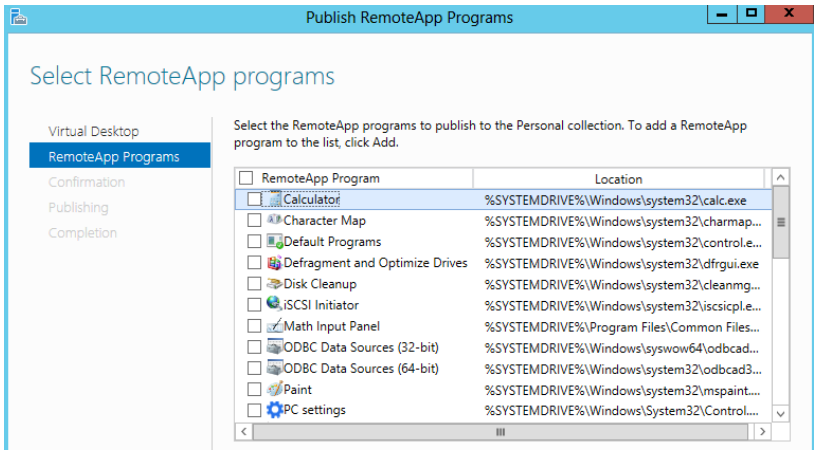


A középső properties résznél állíthatjuk a Personal Collection alapbeállításait, ami nagyjából megegyezik a shared Collection tulajdonságaival:

- General: megadhatjuk a Collection nevét, hogy megjelenjen-e az RD Web Access-en, a gépek számát, illetve engedélyezhetjük a Save Delayt, ami a felhasználó kijelentkezése után adott idővel mentett állapotba helyezi a virtuális gépet.
- Virtual Desktops: virtuális gépek elhelyezkedése az Active Directoryban és a fájlrendszerben
- User Groups: kik férhetnek hozzá a virtuális gépekhez
- Client: milyen erőforrásokat érhetnek el a felhasználók: hang, vágólap, PnP, stb.

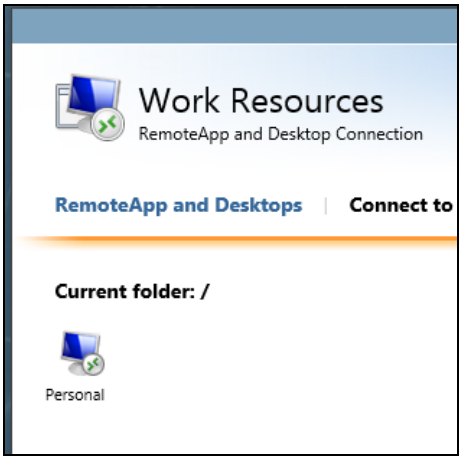


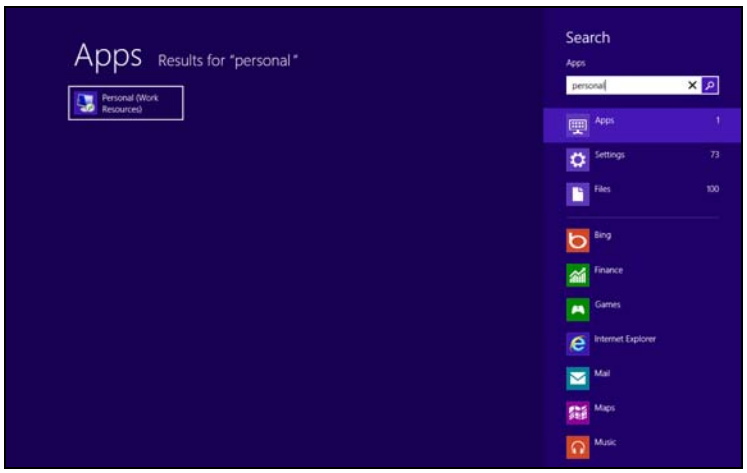
A collection tulajdonságai alatt a RemoteApp programokat tudjuk publikálni: ki kell választanunk egy virtuális gépet, és az azon a gépen telepített programokat tudjuk kiajánlani a RemoteApp programok közé, akár az RD Web oldalra, akár a felhasználók gépeire, a fent megismert módszerrel, feliratkozással:



A jobb oldali Virtual Desktops résznél hozhatunk létre további virtuális gépeket, illetve a meglévőket rendelhetjük felhasználókhoz.

Ha mindent jól csináltunk, a virtuális gépeink megjelennek az RD Web Access felületen, illetve a Windows 8-as kliensek Start menüjében is:





17 Server Core használata

A Windows 2012 Server Core változata az operációs rendszernek egy minimális installációja. A Windows Server telepítés kezdetén eldönthetjük, hogy használjuk a teljes értékű telepítési módot vagy helyette egy csökkentett funkcionalitású Server Core változatot. Első ránézésre szembetünik, hogy a Server Core változatnál csupán egy Command Prompt ablak nyílik meg, de helyileg vagy távoli eléréssel elérhetjük a teljes felügyeleti lehetőséget. Felügyelhetjük a belépés után Command Promptból, de akár a Windows 8 operációs rendszerű munkaállomásunk segítségével a Remote Server Administrator Tools telepítésével elérhetjük a távoli rendszerünk összes konzol-ját illetve lehetőségünk van távoli Powershell parancsokkal befolyásolni a rendszer működését.

Felvetődik a kérdés, hogy tulajdonképpen miért érdemes egy csökkentett funkciókkal rendelkező operációs rendszert telepíteni?

Egyrészt kevesebb erőforrást igényel a kiszolgáló, a GUI és az ahhoz kötődő rengeteg alkalmazás hiánya, kedvezőbb a processzoridőt, memóriamennyiséget és kb. 4 GB tárterületet igényel, ezáltal használatba vehetünk egy régebbi szervert, vagy virtuális gépként kevesebb erőforrással is megelégszik az operációs rendszerünk. Ebből következően a csökken a biztonsági frissítések száma és az ebből származó leállási idő. Tapasztalatok szerint kb. 60 %-al kevesebb frissítést kell havonta telepítenünk. Másodrészt biztonsági szempontból is előnyös, hiszen ami a rendszerünkből hiányzik, azt nem lehet támadni.

A Server Core-t már a Windows Server 2008-ban is használhattunk, viszont ha már egyszer telepítettük a GUI-s változatot, nem tudunk áttérni Server Core-ra, azaz csak egy clean install lehetőségünk maradt. A Windows 2012-ben ez már nem akadály. További újdonság, hogy megjelent egy új Minimal Server installation (vagy MinShell) is, amelyben a Server Manager, az MMC illetve néhány Control Panel elem is elérhető a Core változattal ellentétben. A Minimal Server Installation kb. 300 MB-al helyet is megtakaírthatunk a GUI-s változathoz képest. Találhatunk egy Desktop Experience lehetőséget is, amely eredetileg nem települ a Windows Server 2012 GUI-s telepítőjével sem. Amennyiben ezt a Feature-t telepítjük a következő komponensek települnek: Windows Media Player, Desktop themes, Video for Windows (AVI support), Windows SideShow, Windows Defender, Disk Cleanup, Sync Center, Sound Recorder, Character Map, Snipping Tool, Windows Store. Ezeken kívül megkapjuk a Windows 8 metro kezdőképernyőjét is.

További újdonság, hogy az ASP.NET-es alkalmazásokat már támogatja a Server Core verzió, az előző Windows 2008 Core verzió ezt nem tette lehetővé. Ez azt is jelenti, hogy immár a website-okat már nem csak „nagy" Windows Server alá tudjuk telepíteni.

Az új SQL Server 2012 adatbáziskezelő is támogatja a Windows 2012 Server Core-t, így egy biztonságos, kevesebb erőforrást használó adatbáziskiszolgálót kapunk.

A Server Core telepítése előtt át kell gondolnunk, hogy tulajdonképpen milyen szerepet szánunk a szervernek, milyen szerepköröket kell telepítenünk a kiszolgálóra? A lenti szerepkörök állnak rendelkezésre egy Server Core telepítésnél:

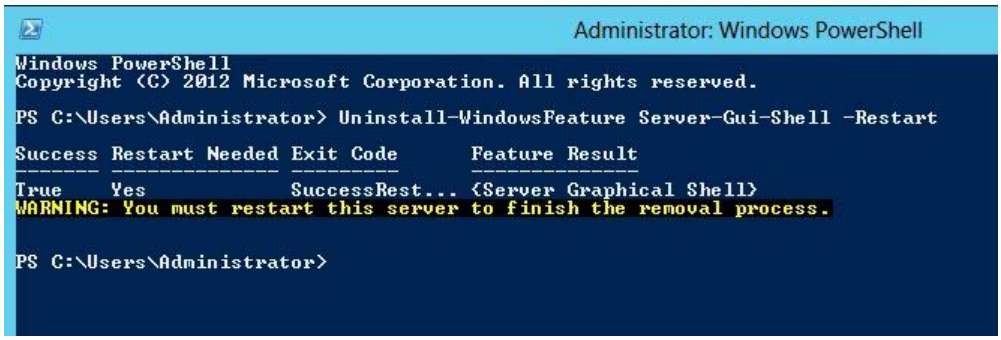
- Active Directory (AD)
- Active Directory Certificate Services (AD CS)
- Active Directory Domain Services (AD DS)

- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Server (AD RMS)
- DHCP Server
- DNS Server
- File and Storage Services
- Hyper-V
- Print and Document Services
- Remote Desktop Services (RDS)
    - Remote Desktop Connection Broker
    - Remote Desktop Licensing
    - Remote Desktop Virtualization Host
- Routing and Remote Access Server (RRAS)
- Web Server
- Windows Server Update Server (WSUS)

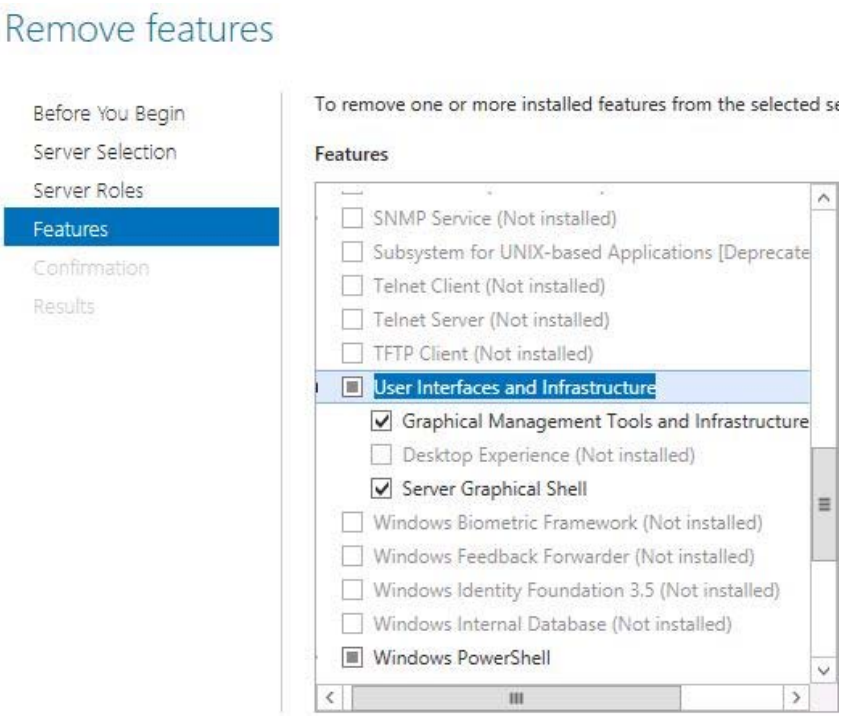
17.1 Telepítés

Ha a számunkra szükséges szerepkörök a listában szerepelnek, akkor kezdhetjük kiszolgálónkat telepíteni egy friss installációval, amely egy teljesen új, DVD-ről történő Windows Server 2012 telepítés, vagy már meglévő teljes értékű Windows Server 2012-t is „lecsupaszíthatunk” Server Core szintre. Mindezt a következő powershell paranccsal:

```
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra, Server-Gui-Shell -Restart
```



De ugyanezt megtehetjük kényelmesen a kiszolgálókezelőn keresztül is:



Ha a fenti ábra alapján, mindkét pipát kivesszük akkor végeredmény egy Windows 2012 Server Core lesz, ha csak a Server-Gui-Shell-t, akkor egy Minimum Server telepítéshez jutunk.

Amennyiben későbbiek folyamán szeretnénk mégis visszatérni a grafikus felületre (pl. olyan szerepköröket szeretnénk telepíteni, amit csökkentett funkcionalitással rendelkező változatokban nem elérhető), akkor azt Minimal Server Installation esetén Powershellből, de akár a Kiszolgálókezelőn keresztül is könnyen megtehetjük. Server Core esetében, mivel itt eltávolításra kerül a Powershell, megtehetjük távolról az említett két eszköz segítségével, vagy lokálisan a Command Promptból.

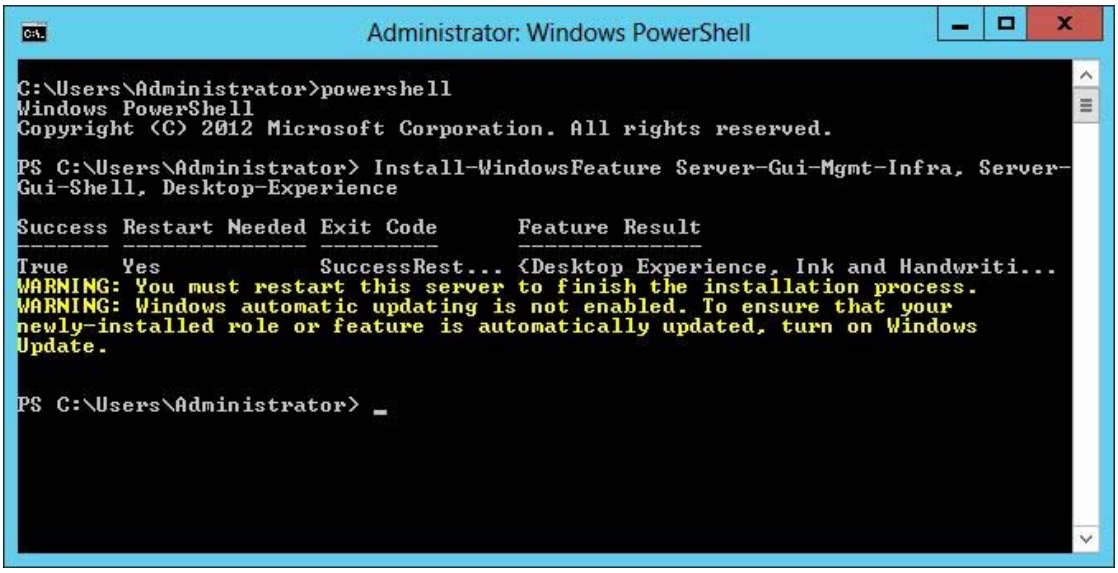
Ha közvetlenül a Server Core Command Promptjából szeretnénk megtenni akkor ezt a dism paranccsal végezhetjük el:

```
dism /online /enable-feature /featurename:ServerCore-FullServer
```

Az újraindítás után még nincs vége a telepítésnek. A szokásos Command Prompt jelenik meg a belépés után, de már elérhető a powershell.

Telepítsük Powershell-el, úgy, hogy a Desktop Experince-t is szeretnénk telepíteni:

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell,Desktop-Experience –
          Restart
```



17.2 Konfiguráció

A konfiguráció elvégezésére az egyik lehetőség, hogy használjuk a Server Configuration Utility-t (sconfig), de azt is megtehetjük, hogy command prompt segítségével állítjuk be a szervert.

Az sconfig egy text alapú menü, amely jelentősen megkönnyíti szerverünk konfigurálását. A következő lehetőségek vannak arra, hogy testreszabjuk a kiszolgálónkat:

- Tartományba léptetés: A kiszolgálónk beléptetése a tartományba vagy egy munkacsoportba.
- Kiszolgáló nevének változtatása.
- Helyi rendszergazda fiók beállítása: Ha tartományi felhasználó akkor használjuk a domain\username formációt, amennyiben nem akkor csak a felhasználói nevet adjuk meg.
- Hálózati beállítások: Beállíthatjuk, hogy a kiszolgálónk DHCP szervertől kapjon automatikusan a IP címet illetve manuálisan is adhatunk egy IP címet. A DNS kiszolgáló IP címét szintén itt adhatjuk meg.
- Windows Update beállítások: Automatikus és manuális frissítés beállítása. Alapértelmezés szerint a szerver 3:00-kor ellenőrzi a frissítéseket, amennyiben manuális frissítést állítjuk be, ez esetben nem teszi meg. A frissítés letöltését és telepítését a Download and Install Updates menüpont alatt érhetjük el.
- Remote Desktop beállítások: Alapértelmezés szerint kikapcsolva. Beállíthatjuk, hogy hálózati szintű azonosítást végezzen vagy régebbi típusú rdp klienssel is együttműködjön.
- Date and Time settings: Dátum és idő beállítása.
- Enable Remote Management: Itt megtaláljuk a Powershell-t, a Server Managert és a Microsoft Management Console-t. Ezeket az eszközöket csak legalább Minimal Server installation esetén tudjuk elindítani.
- To Logoff, Shutdown and Restart the server: Kijelentkezés, a szerver kikapcsolása és a szerver újraindítása
- To Exit to the command line: kilépés az sconfig-ból.

Az sconfig alatti beállításokat megtehetjük parancssorból is.

A Server Core telepítése után általában kapunk egy véletlenszerű nevet a kiszolgálónknak, ezt a következő parancssor segítségével könnyedén megváltoztathatjuk:

```
Rename-Computer ServerCore
```

A gépnév változtatása után érdemes újraindítani a kiszolgálót, a következő paranccsal:

```
Restart-Computer
```

A fenti parancs mellett továbbra is használható az előző változatokból is ismert “shutdown”.

Az újraindítás után adjunk meg egy statikus IP címet a szervernek:

```
New-NetIPAddress -IPAddress 192.168.1.10 -InterfaceAlias "Ethernet" -
         DefaultGateway 192.168.1.1 -AddressFamily IPv4 -PrefixLength 24
```

Majd állítsuk be a DNS szerver IP címét is:

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
         192.168.1.2
```

Amennyiben tartományba szeretnénk léptetni a gépünket, adjuk ki a következő parancsot:

```
Add-Computer -DomainName domain2012.local
```

A Windows Server 2012 használata 30 napig lehetséges a licencinformációk nélkül, mindezt érdemes mielőbb megtennünk:

```
slmgr –ipk <Product key>
```

18 Magas rendelkezésre állás

Néhány évvel ezelőtt a kiszolgálók és az infrastruktúra magas rendelkezésre állása csak nagyvállalati környezetben volt elérhető. Az elmúlt 1-2 évben azonban ez az igény megjelent a kis- és középvállalkozásoknál is, illetve az új technológiákkal lassan elérhetővé is váltak azok az eszközök és szolgáltatások, amelyekkel könnyebben építhetünk magas rendelkezésre állású rendszereket. A Windows Server 2012 egyik nagy újdonsága, hogy a failover cluster és egyéb HA (highly available) szolgáltatásokat már a Standard verzióban is elérhetjük, vagy akár az ingyenes Hyper-V Server 2012-ben is. Az operációs rendszer, és kiszolgáló szolgáltatások magas rendelkezésre állásának megvalósítása előtt azonban fontos, hogy az alap infrastruktúrát (áramellátás, hálózat, elosztók, tárolók) is folyamatos rendelkezésre állásra tervezzük, tehát bármelyik eszköz meghibásodása, vagy tervezett karbantartás esetén a rendszer képes legyen tovább működni.

18.1 Infrastruktúra magas rendelkezésre állása

A Windows Server 2012 szerepköreinek egy része – Active Directory, DNS, DHCP – önmagában képes magas rendelkezésre állást nyújtani: a címtárszolgáltatás (AD DS) több kiszolgálón, különböző telephelyeken elosztva működik, a törölt elemeket pedig az Active Directory lomtárból állíthatjuk vissza. A DNS kiszolgáló szintén beépítve tartalmazza a magas rendelkezésre állás képességeit, az elsődleges és másodlagos zónák létrehozásával. Azoknál a szolgáltatásoknál, amelyek önmagukban nem képesek magas rendelkezésre állást biztosítani, a Windows Server 2012 beépített szolgáltatásai közül a következőket választhatjuk:

- Network Load Balancing: (NLB) szoftverkomponens, amely a hálózati forgalmat képes különböző állomások között szétosztani, terhelés-elosztást és magas rendelkezésre állást nyújtva ezzel. A kiszolgálókon azonos adatoknak kell lenniük, például webkiszolgálóknak passzív tartalommal.
- Failover Cluster: számítógépek magas rendelkezésre állású fürtje, amelyek figyelik egymást, és vagy szinkronizálják az adatokat, vagy egy központi adattárat érnek el közösen. A szolgáltatások vagy virtuális gépek képesek költözni a fürttagok (NODE) között, akár hiba esetén automatikusan, akár tervezett karbantartás esetén manuálisan. Néhány szolgáltatásnál a Failover Cluster az ajánlott megoldás a magas rendelkezésre állás megvalósításához, ilyen a Hyper-v, az iSCSI target, Exchange, SQL, stb.

18.1.1 Guest Cluster és Host Cluster

A failover cluster szolgáltatást virtuális környezetben többféleképpen használhatjuk: Biztosíthatunk magas rendelkezésre állást a virtuális gazdagépeknek, így a virtuális gépek képesek költözni több fizikai gép között, ezt hívjuk host clusternek, vagy a gazdagépekre telepíthetünk külön virtuális gépeket, és azokon, az adott termék magas rendelkezésre állási képességeit használva hozhatunk létre fürtöt (guest cluster). A második megoldás sokkal szofisztikáltabb, mert a guest cluster nem csak a fizikai gép meghibásodásakor, hanem az adott szolgáltatás hibája esetén is képes költözni. Ha például egy host cluster alapú Exchange kiszolgálón leáll az adatbázis, azt hiába költöztetjük egyik fizikai gépről a másikra, az adatbázis off-line állapotban marad. Ezzel szemben, ha az Exchange-re bízzuk a szolgáltatás felügyeletét, akkor az egyik kiszolgálón történt adatbázis-hiba esetén a másik gépen lévő külön Exchange Server elindítja az ottani adatbázist.

A két szolgáltatást akár egyszerre is használhatjuk, tehát a fenti példából kiindulva, az egyik virtuális Exchange kiszolgálót futtathatjuk az egyik Hyper-V clusteren, a másik példányt egy másikon, így minden hibára felkészültünk.

18.1.2 Újdonságok a Windows Server 2012-ben

Habár a Windows Server 2008R2 óta nagyon nagy változások nem történtek a magas rendelkezésre állásban, van néhány dolog, amit érdemes kiemelni:

- A fürtbe rendezhető gépek maximális száma 16-ról 64-re nőtt
- Továbfejlesztett Cluster Shared Volume (CSV) a virtuális gépeink lehetnek SMB 3.0 alapú magas rendelkezésre állású megosztásokon is, és kihasználhatjuk az SMB multichannelt is.
- Cluster-képes frissítés: egy automatizált folyamat, ami egyenként telepíti a Windows frissítéseket a fürttagokra, miközben átmozgatja az erőforrásokat a frissítendő gépről egy másik tagra, majd továbblép a fürt következő tagjára, és így tovább.

18.1.3 Összetevők

A feladatátvevő fürt különálló gépek csoportja, amelyek közösen magas rendelkezésre állást nyújtanak. Ezeket a gépeket fürttagnak, vagy Node-nak hívjuk. Ha az egyik fürttag meghibásodik, a rajta lévő szolgáltatások (workload) átköltöznek egy másik fürttagra. Ezt a folyamatot hívjuk failover-nek

A feladatátvevő fürt a következő komponensekből áll:

- Fürttagok
- Hálózat: a fürt kiépítéséhez több hálózati kapcsolatra lesz szükségünk, külön hálózaton csatlakoznak a kliensek, külön kommikálnak a fürttagok egymással, egy másik hálózaton történik a tárolók elérése, stb.
- Erőforrás: a fürttagokon lévő komponens, amelyet a fürt futtat, indít/leállít, és képes költöztetni a fürttagok között. Pl. IP cím, hálózati név, stb.
- Fürt tároló: megosztott tároló, amit az összes fürttag elér. Nem minden környezetben kötelező, az Exchange például az adatbázis log-fájlokat másolja a különálló tárolókra, és így tartja szinkronban az adatbázist.
- Kliensek: számítógépek, akik a fürthöz csatlakoznak
- Szolgáltatás vagy alkalmazás: szoftver-komponens, amit a kliensek elérnek
- Quorum: szavazati többség. Ha páros számú fürttagunk van, akkor a tagok meghibásodás esetén nem képesek eldönteni, ki legyen az aktív: Ha a passzív tag nem éri el az aktív tagot, akkor két dolog történhet: Vagy az aktív tag leállt, ilyenkor a passzív tagnap aktivvá kell vállni, vagy a passzív tag szakadt le a hálózatról, ilyenkor viszont nem szabad elindulni, mert két aktív lesz a hálózaton (split brain) Ilyenkor egy külső döntőre (witness) van szükség, hogy a passzív tag eldöntse, ő állt-e le, vagy az aktív tag. Ez lehet egy lemez (disk witness) vagy megosztás egy fürtön kívüli gépen (file share witness). Ha a passzív tag nem látja az aktív tagot, de a witness-t igen, akkor aktiválja magát, ha nem látja sem az aktív tagot, sem a witness-t, akkor nem indul el.

18.1.4 Fürt tárolók

Ha a fürt közös adattárat igényel, akkor olyan lemez alrendszert kell választanunk, amihez egyszerre több fürttag is hozzáférhet. Ebben az esetben a következő lemez-típusokból választhatunk:

- SAS (Serial Attached SCSI) Ez a legolcsóbb megoldás, viszont a fürttagoknak fizikailag közel kell lenniük egymáshoz, a SAS kábel maximum 10 méter hosszú lehet. http://en.wikipedia.org/wiki/Serial_attached_SCSI
- iSCSI tároló: IP hálózaton szállít SCSI parancsokat, 1GB vagy 10GB-es hálózati közegen. A Windows Server 2012-ben beépítve található iSCSI server, amit akár magas rendelkezésre állásúvá is tehetünk. Erről részletesebben az adattárolás fejezetben írtunk.
- Fibre Channel: drágább megoldás, mint az iSCSi vagy a SAN adattárak, de nagyobb sebességet, és jobb teljesítményt képesek nyújtani.
-
- Amikor lemeztípust választunk, illetve clustert építünk, a következő feltételekre érdemes odafigyelni:
- A tárolón minden fürtnek érdemes külön logikai egységeket (LUN) létrehozni, hiszen a fürtöt költöztetünk, a LUN is költözik az új fürttagra. Ha ugyanazon a LUN-on például több virtuális gép van, és az egyiket költöztetjük, akkor előfordulhat, hogy a többi virtuális gép alól kirántjuk a lemezeket, ami nem szerencsés.
- Az adattár eléréséhez érdemes MPIO technológiát használnunk.
- A lemezeknél a partíció típusa lehet MBR vagy 2TB-nál nagyobb lemezeknél GPT, a fájlrendszer NTFS kell, hogy legyen, a lemezeket pedig alaplepezként kell importálni, nem dinamikus lemezként.

18.1.5 Fürt megosztott kötetei

A klasszikus fürtben egy időben csak egy fürttag birtokolhat egy LUN-t. Ez a fent említett problémát okozhatja, vagy a Hyper-V hoszton futtatott összes virtuális gépnek külön LUN-t kellene létrehoznunk a tárolón. Ezt a problémát hivatott megoldani a Windows Server 2008R2-ben bemutatott Cluster Shared Volume, vagy fürt megosztott kötet. CSV esetén ugyanazt a LUN-t több host is eléri, és nem LUN szinten, hanem fájlszinten zárolnak, mindegyik host az általa éppen futtatott virtuális gép konfigurációját és VHD-it. A CSV tehát lehetővé teszi, hogy egy időben több gép érje el ugyanazt az NTF partíciót.

A Windows Server 2008R2-ben kizárólag Hyper-V fürtözésnél használhattunk CSV-t, a 2012-es verzióban viszont egyéb adatokat is tárolhatunk rajta, akár magas rendelkezésre állású fájlkiszolgálót is. Ezeken a megosztásokon pedig lehetnek SQL vagy Exchange adatbázisok is akár.

CSV használatához először egy Failover Cluster-t kell építenünk, majd a szabad lemezek közül tetszőleges számú lemezt konfigurálhatunk CSV-be. A lemeznek előrhetőnek kell lennie, és bármelyik gépről el kell tudnunk érni. Ha egy lemezt felveszünk CSV-ként, akkor a cluster eltávolítja a betűjelét, és becsatolja a c:\clustersharedvolume mappa egy almappájába. Ez azért fontos, mert a rajta lévő adatok elérési útjának azonosnak kell lenniük, pl. a virtuális gépek konzisztens konfigurációja miatt: ha a virtuális lemez az egyik gépen d:\VHDs\ mappában van, a másikon pedig e:\VHD mappában, akkor a virtuális gépet nem tudjuk majd költöztenit, mert nem találja meg a lemezeit.

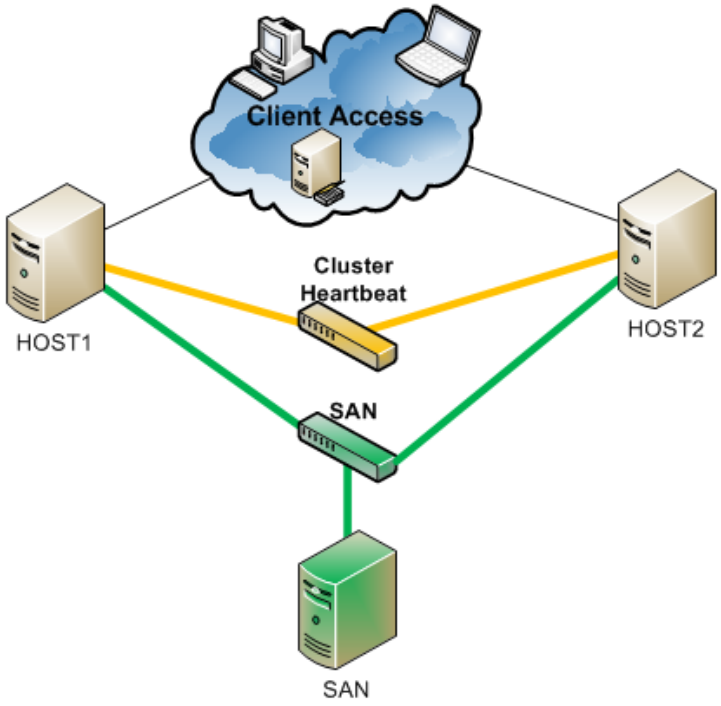
18.1.6 Fürthálózatok

Egy fürt építéséhez legalább 3 hálózatra van szükségünk:

- Belső hálózat, ahol a fürt tagjai kommunikálnak egymással, ellenőrzik a többi fürttagot. Érdemes ezt a hálózatot fizikailag különválasztani a többi hálózattól
- Külső hálózat: ezen keresztül csatlakoznak a kliensek a fürt erőforrásaihoz
- iSCSI hálózat: a tároló blokk-szintű elérésére. Ezt a hálózatot szinten szeparálnunk kell a többitől. Ha nem iSCSI-ra építjük a clustert, vagy nincs szükségünk közös adattárra, akkor erre a hálózatra nem lesz szükségünk.

Létrehozhatunk vegyes hálózatot is, ahol a cluster belső kommunikációja és a kliens-hozzáférés történik, de ha lehetőségünk van, akkor a vegyes hálózatot csak tartalékként használjuk, ha a belső hálózati kapcsolatunk megszakad.

Mindegyik hálózatot lehet és érdemes NIC teaming-re építeni, így nagyobb sebesség mellett nagyobb rendelkezésre állást is elérhetünk.



Fürthálózat

18.2 Építsünk fürtöt!

Ebben a részben lépésről-lépésre végighaladunk egy fürt építésén, megismerkedünk a Validate a Configuration Wizard-al, létrehozzuk a fürtöt, CSV-t, majd különböző szolgáltatásokat helyezünk el a fürtünkön.

A feladatátvevő fürt alapvető feladata, hogy magas rendelkezésre állást biztosítson, így a fürttagok hardverét is ez alapján kell választanunk, az általános kiszolgálónak szánt server nem

biztos, hogy megfelel magas rendelkezésű kiszolgálónak. Érdemes egyébként azonos gyártó azonos típusú kiszolgálóiból építenünk a fürtöt. A hálózati, és adattároló infrastruktúrát is magas rendelkezésre állásúvá kell tennünk.

18.2.1 Előkészületek: tervezés

Mint minden rendszer életciklusában, a fürtözésnél is a legfontosabb lépés a megfelő tervezés. Egy rosszul megtervezett fürtöt nagyon nehezen tudunk módosítani, újratervezni. Meg kell egyeznünk a rendelkezésre állás mértékében, mekkor kiesés elfogadható, a 99,9% például éves szinten 8 óra leállást enged meg. A kiesésbe nem számít bele a tervezett leállás, a firmware-k, frissítések telepítése, de minden más igen, pl. áramszünet, stb.

Szintén meg kell terveznünk az elfogadható lemezelérést. Egy 1GB-es iSCSI hálózat elég lehet 2-3 virtuális gép futtatásához, de 8-10 gép ugyanazon az 1GB-es vonalon már használhatatlanul lassú lesz. Az is fontos szempont, hogy a fürtözött rendszerek aktív-passzív módon működnek, tehát egy időben csak egy gépen fut az adott alkalmazás. További fürttagok üzembe helyezésével a teljesítményünk nem nő, csak a rendelkezésre állás. Ha skálázni szeretnénk az alkalmazásainkat, akkor a fürttagokat kell bővítenünk memóriával, CPU-val, stb.

Vannak bizonyos szolgáltatások, amelyeket nem, vagy csak nagyon körülményesen tudunk fürtözni, vagy esetleg a szoftver gyártója nem támogatja a fürtözött működést. Például egy faxkiszolgálót, ami USB vagy belső fax kártyával működik, nehezen tudunk Hyper-V clusterbe építeni. Ha az adott szoftver hardveres kulcsot használ, szintén nem virtualizálható.

A Node-okat úgy érdemes terhelni, hogy ha az egyik tag kiesik, a feladatok átvételére a maradék tagnak legyen szabad kapacitása, különben a maradék kiszolgálót is túlterheljük, így egy rövid idő után ez a tag is leállhat, vagy képtelen lesz kiszolgálni a felgyülemlett terhelést. Ha például 2 tagú fürtöt építünk, érdemes a tagok egyéni terhelését 40-50% alatt tartani, de ha 3 tagú fürtöt építünk, és szeretnénk, hogy 2 tag kiesése esetén is működjenek a szolgáltatásaink, akkor a tagok egyéni terhelése nem lehet több, mint 30%.

Meg kell vizsgálnunk a rendszerünket, hogy nincs-e benne „Single Point of Failure”, vagyis olyan pont, amelynek kiesésénél az egész fürt összeomolhat. Ez lehet hálózati kártya, FC csatoló, RAID kötetek, redundáns tápegységek, stb.

18.2.2 Feltételek

A fürt építésekor a következő hardver, szoftver és hálózati feltételeket kell figyelembe vennünk:

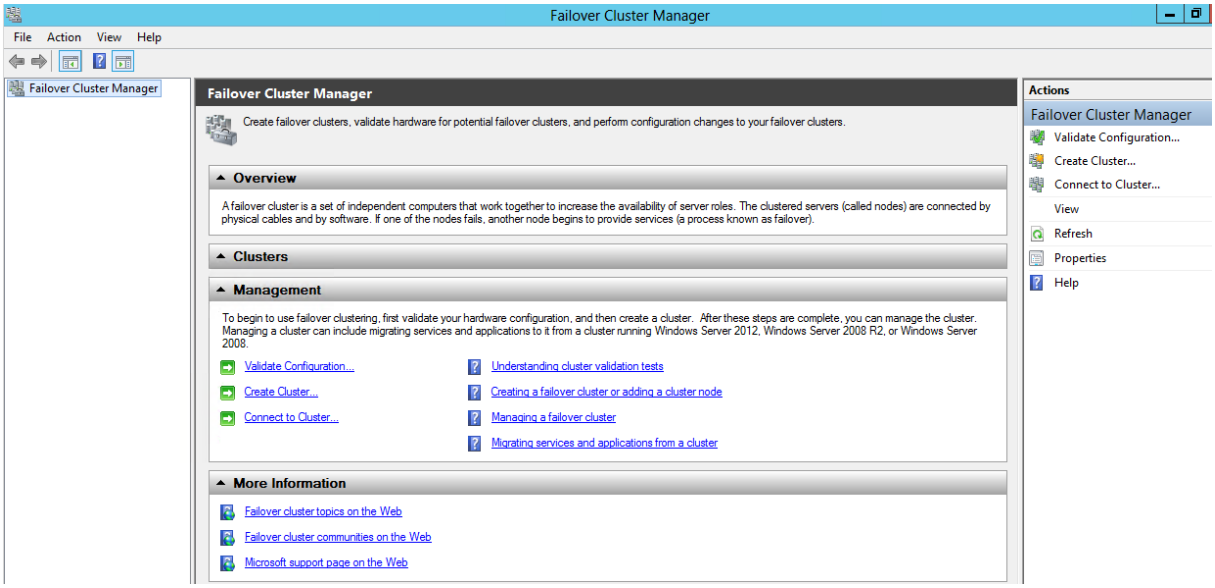
- A hardvereknek meg kell felelniük a „Certified for Windows Server 2012” feltételeknek. A Validate a Configuration Wizard leellenőrzi a tervezett hardvert, lemezelérést, lemezköltöztetést, stb. A cluster létrehozásahoz a tesztnek sikeresen le kell futnia.
- Hálózat: a node-ok hálózati vezerlőinek azonos sebességgel, duplexitással és funkciókkal kell rendelkezniük. Ha iSCSI hálózatot tervezünk, akkor az iSCSI hálózati kártyán egyéb beállításokat is el kell végeznünk: Jumbo framet és a TCP offloadot: https://technetklub.hu/blogs/virtualizacio/archive/2010/08/11/hyper-v-r2-f-252-rt-tervez-233-s.aspx. A hálózatnak természetesen redundásnak kell lennie.
- Szoftver: a fürtben ugyanolyan verziójú Windows Server 2012-t kell használnunk, vagy az összes tag Standard verzió (vagy a Standard Server alapjaira épített ingyenes

Hyper-V server 2012), vagy mindegyik Datacenter. A kiszolgálókon azonos verziójú szervízcsomagnak kell rendelkezniük, és azonos patchelési szinten kell lenniük.

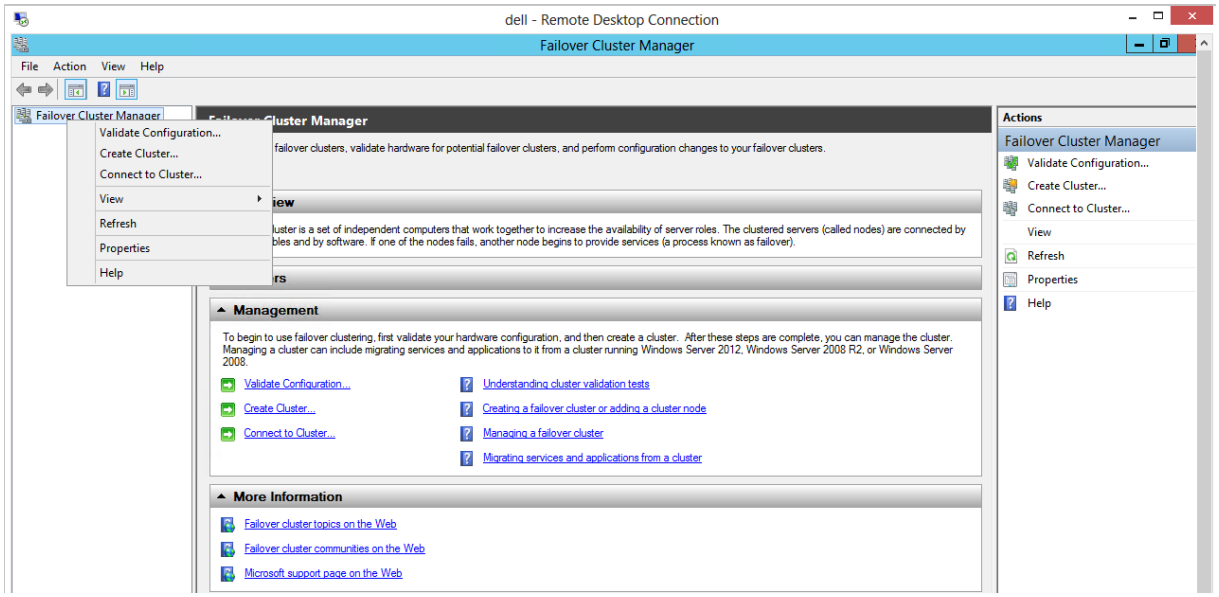
- A fürttagoknak ugyabban a tartományban kell lenniük. Javasolt, hogy a gépek tartománytagok legyenek, mert a tartományvezérlőkön már található magas rendelkezésre állási szolgáltatás, ami ütközhet a fürtözéssel.
- A fürtlemezt mindkét tervezett node-nak látnia kell, és NTFS partícióval kell, hogy rendelkezzen

18.2.3 Telepítés

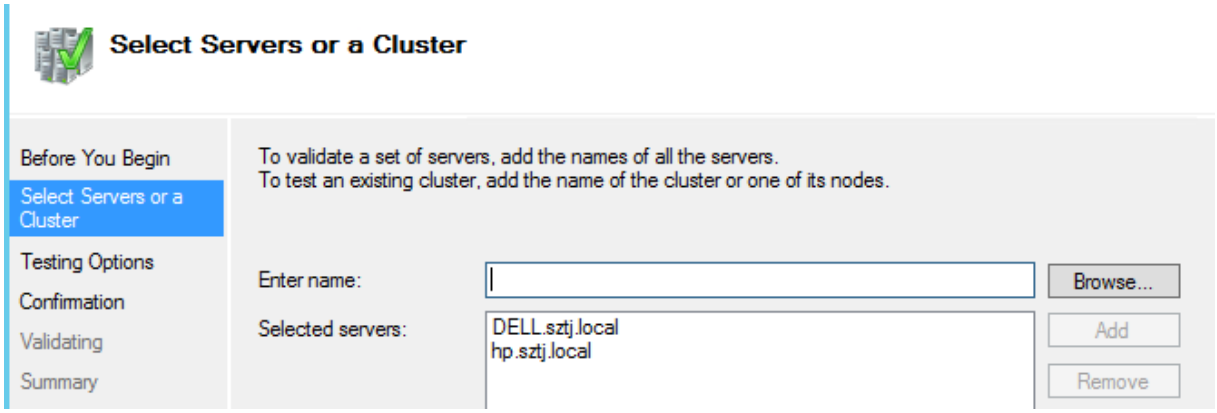
A Failover Cluster szerepkör telepítését a Server Manager/Add Roles and Features menüjéből indíthatjuk. Telepítés után a Tools menüben megjelenik a Failover Cluster Manager:



Ha mindkét kiszolgálónkra feltelepítettük a szolgáltatást, és a megosztott lemezeket is elérjük, akkor elindíthatjuk a Validate Configuration varázslót:

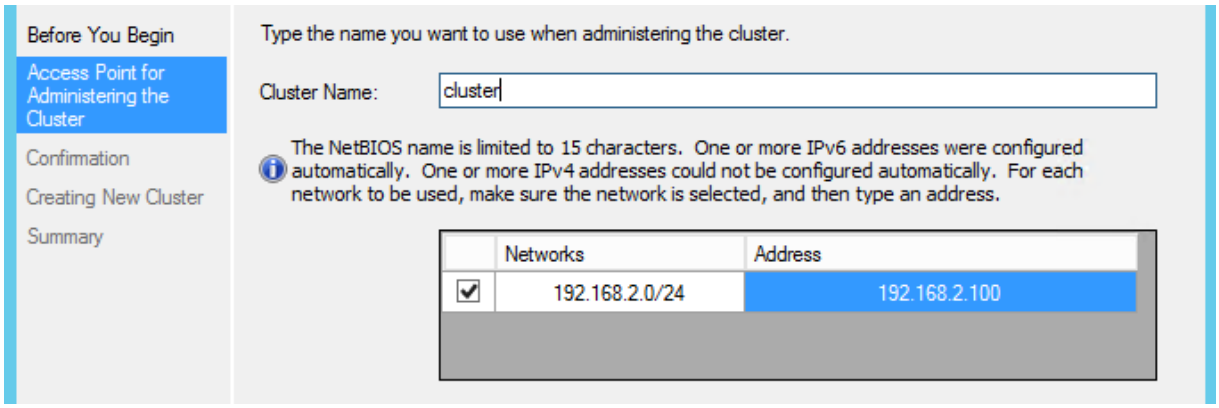


Első lépésben hozzá kell adnunk az összes kiszolgálót, akik tagjai lesznek a fürtnek, majd le kell futtatnunk az összes tesztet.

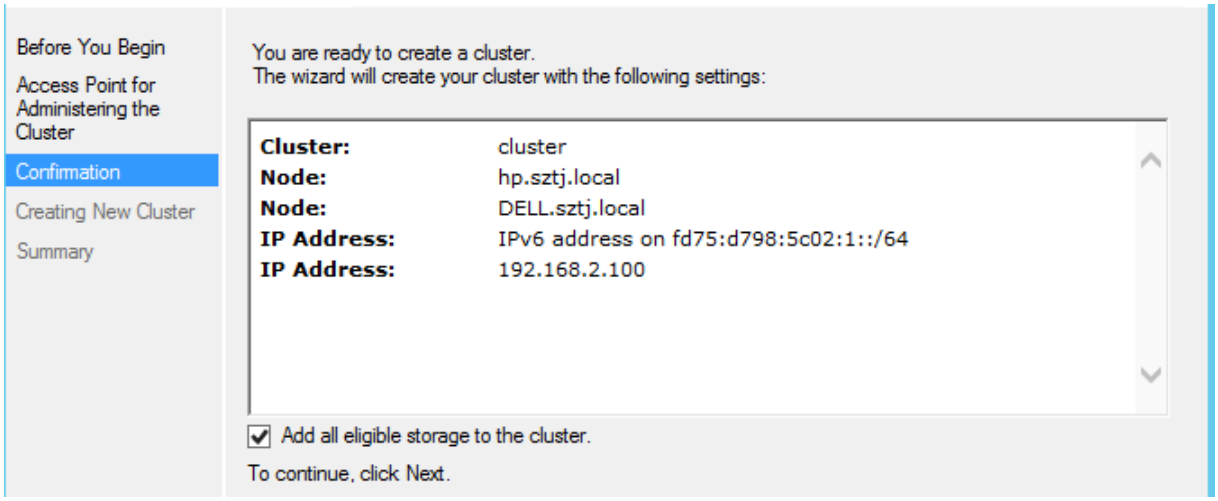


A teszt megkeresi a Quorum használatra alkalmas lemezeket, teszteli az iSCSI lemez mozgatását, a lemezírási sebességet, a hálózati infrastruktúrát, szerepköröket, stb.

Ha a teszt sikeresen lefutott, akkor nekiállhatunk a fürt létrehozásának a Create Cluster varázslóval:

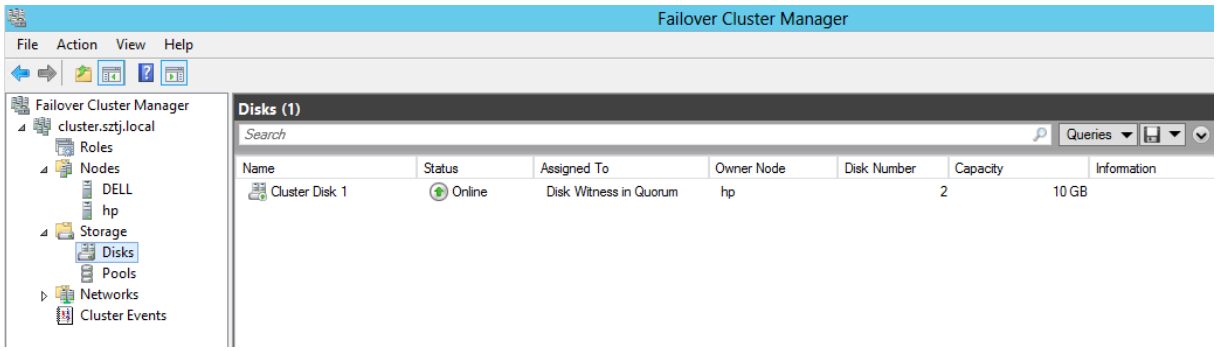


Meg kell adnunk az új fürt nevét, és egy IP címet. Ez két alap-erőforrás, ami nélkül a fürt többi erőforrása nem fog elindulni, illetve ezek az erőforrásokat mindig az aktív tag birtokolja. Ha sem a név, sem az IP cím nincs használatban, akkor létrehozhatjuk a fürtöt az alábbi beállításokkal:



18.2.4 Failover Cluster Manager

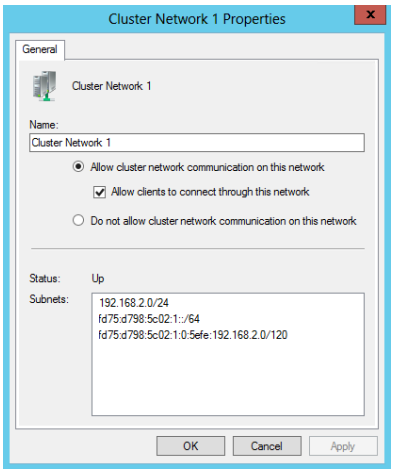
Miután létrehoztuk a fürtünket, ismerkedjünk meg a felülettel:



- A Roles részben adhatunk hozzá szolgáltatásokat vagy virtuális gépeket a fürthöz.
- A Nodes-nál láthatjuk a fürt tagjait, az aktuális állapotukat, illetve karbantartási módba helyezhetjük bármelyik node-ot.
- A Storage résznél az összes szabad, vagy szolgáltatáshoz rendelt lemezeinket látjuk, köztük a Qourom lemezt, illetve itt adhatunk a fürthöz további lemezeket, ha az iSCSI

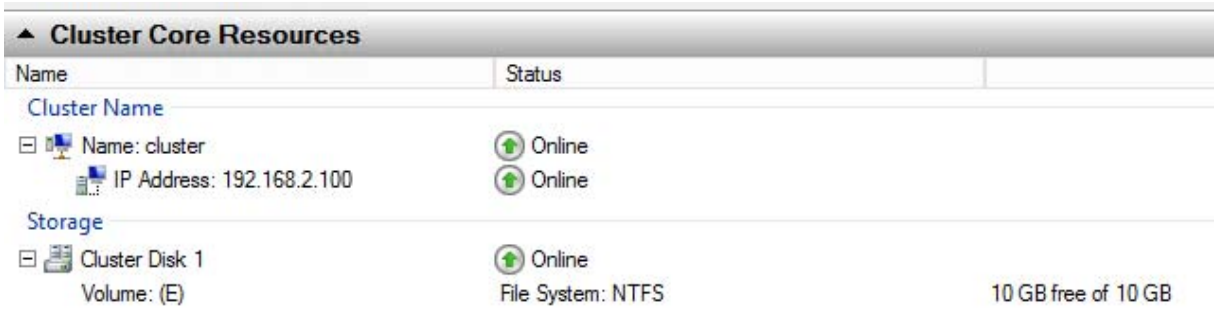
target-en létrehoztuk azt, és az összes node eléri. A 2008 R2-vel szemben a 2012 iSCSI kezeli a 2TB-nál nagyobb lemezeket is

- Pools: a Windows Storage Spaces-ben létrehozott, több fizikai lemezből álló virtuális tárolót adhatjuk hozzá a Clusterhez.
- Networks: a felismert hálózatok típusát adhatjuk meg, ez lehet külső, belső vagy vegyes hálózat.
- Cluster Events: a fürttagokról összegyűjtött eseménynaplókat tekinthetjük meg itt.



A szolgáltatások elhelyezése előtt be kell állítanunk mindegyik hálózatunkat, hogy engedélyezzük-e rajt a fürt forgalmat, illetve a külső elérést:

- Az iSCSI kártyákon le kell tiltani a Cluster forgalmat
- A hearthbeat kártyákon csak a fürttagok kommunikálhatnak
- A külső hálózaton a klienseket engedjük hozzá a fürthöz:

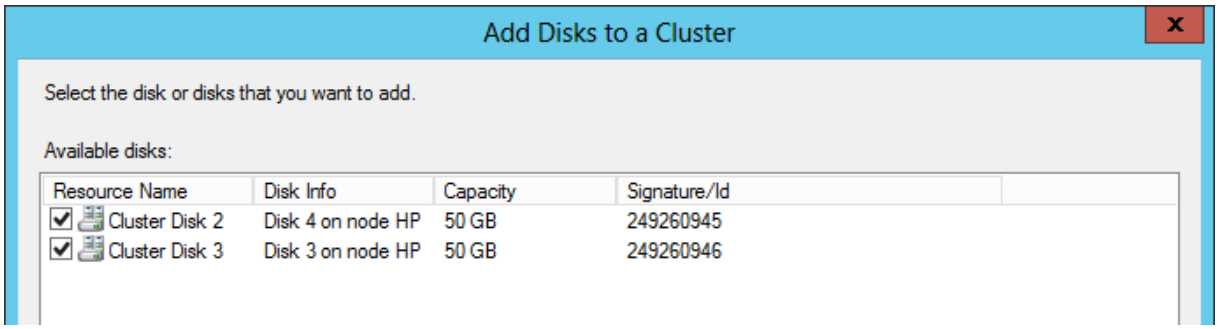


A konzol alsó-középső részén látjuk a fürt alap erőforrásait: IP, név, Quorum

18.2.5 Fürt erőforrások felvétele

Miután sikeresen létrehoztuk a fürtöt, különböző erőforrásokat kell hozzáadnunk. Ebben a részben létrehozunk egy magas rendelkezésre állású fájlkiszolgálót, illetve egy Hyper-V Cluster-t is, ahová virtuális gépeket fogunk elhelyezni. Mindkettőhöz szükségünk lesz egy-egy külön lemezre, amit az iSCSI konzolon kell létrehoznunk. Érdemes a két lemezt külön LUN-ra tenni, vagy használhatunk Cluster Shared Volume-ot is.

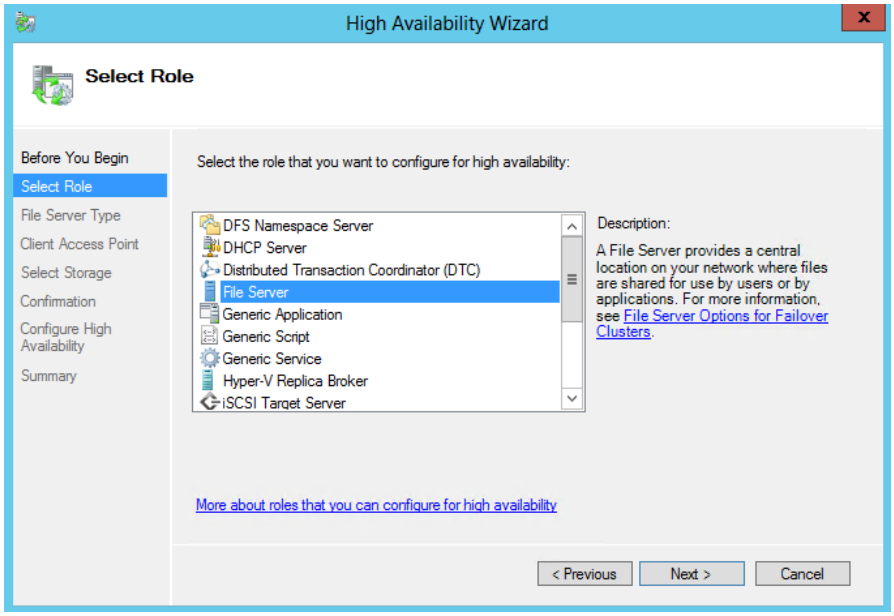
A magas rendelkezésreállású fájlkiszolgáló használatához iSCSI storage-on létrehozott lemezt hozzá kell adnunk a clusterhez a Storage résznél az Add Storage varázslóval:



Az egyik lemez a fájlkiszolgálóé, a másik a Hyper-V clusteré lesz

A lemezek importálás után bekerülnek a szabad tárolók közé, így a szolgáltatások létrehozásakor ki tudjuk választani ezeket.

A Roles menüben a Configure Roles menüponttal vehetünk fel új szolgáltatásokat. A konzol ellenőrzi, hogy a kiválasztott szolgáltatás –jelen esetben fájlkiszolgáló - telepítve van-e a fürttagokon:



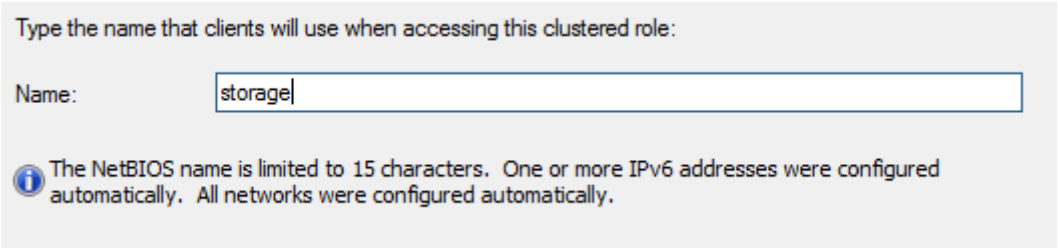
A File Server kiválasztása után két lehetőség közül választhatunk:

- **Clustered file server for general use**: Fájlkiszolgáló fürt általános használatra. Ez a verzió megtalálható a Windows Server 2008R2-ben is.
- **File server for scale-out application data**: az új Scale-Out fájlkiszolgáló, alkalmazások, fájlok és virtuális gépek magas rendelkezésre állásához.

A következő táblázatban összehasonlítjuk a két szolgáltatást:

Clustered file server for general use	**Scale-Out File Server**
Magas rendelkezésre állást nyújt az olyan alkalmazásoknál, ahol a fájlokat nem maradnak folyamatosan nyitva	Magas rendelkezésre állást biztosít a hosszú ideig, vagy folyamatosan nyitva lévő fájloknak
Egyszerre egy fürttagon fut	Egyszerre több node-on fut, az SMB kliensek kapcsolatai eloszlanak a fürttagok között, ezzel nagyobb sávszélességre képes. Ezt a funkciót a Distributed Network Name szolgáltatással éri el, ami lehetővé teszi, hogy külön IP címeken lévő fürttagok egyszerre válaszoljanak a kérésekre DNS round robin használatával
Nem használhat CSV-t	Kötelezően Clustered Shared Volume-ot használ
Aktív-passzív módon működik, automatikus failover-el	Nem támogatja az NFS-t, a BranchCache-t, a Data Deduplication-t, és egyéb fájlkiszolgálói képességeket

Válasszuk a Scale-Out fájlkiszolgálót, majd adjunk meg egy hozzáférési nevet, amit a kliensek elérnek majd:

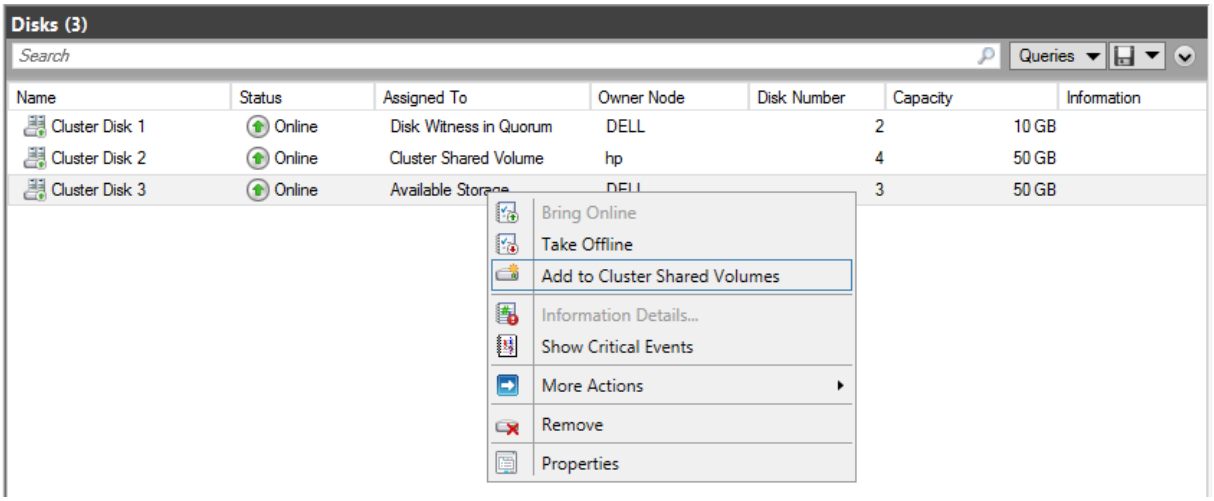


Ha az erőforrás sikeresen létrejött, akkor már csak hozzá kell adnunk megosztásokat, az erőforrás tulajdonságain Add File Share varázslóval.

18.3 Hyper-V Cluster

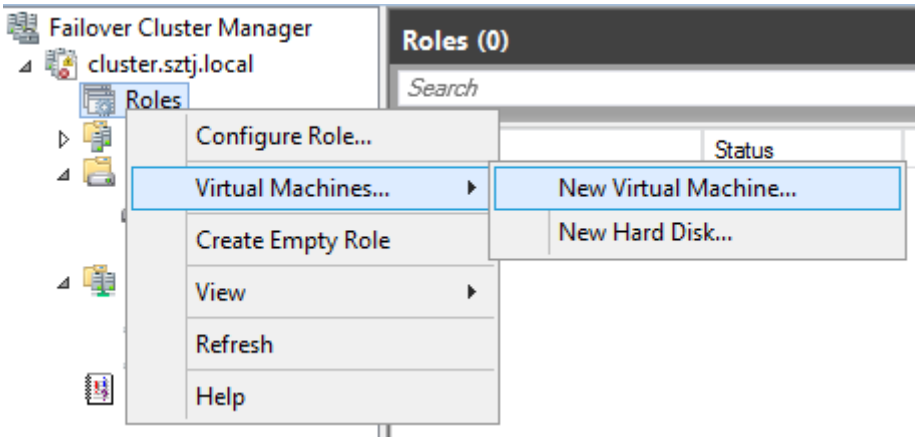
Ha sikeresen létrehoztuk a fürtünket, akkor akár Hyper-V alapú virtuális gépeket is elhelyezhetünk rajta. Ennek feltétele a Cluster Shared Volume (CSV), a megfelelő hálózatok megléte (külső, belső), és a Hyper-V szerepkör a fürttagokon.

Első lépésként a szabad lemezeink egyikét CSV-be kell tennünk:



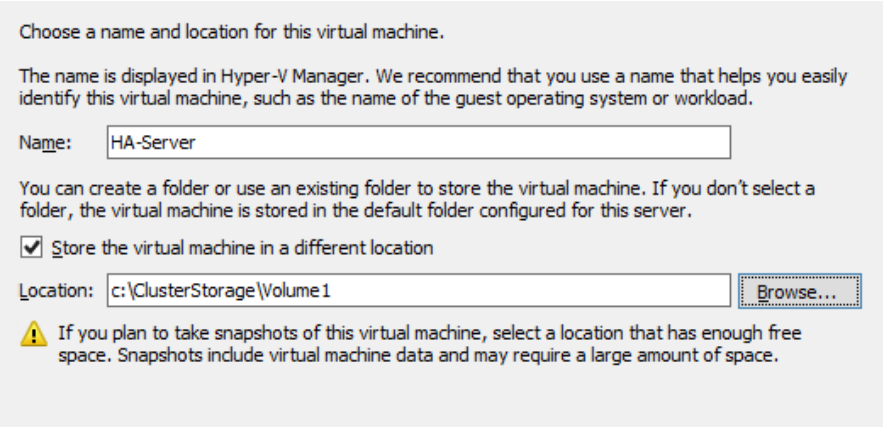
Ezután a lemezünket a C:\ClusterStorage\Volume1 könyvtárában érjük el, ide kell majd elhelyeznünk az új magas rendelkezésre állású virtuális gépünket.

A következő lépésben létre is hozhatjuk a VM-et. A Roles menüben válasszuk az új Virtual Machine menüt:



A virtuális gép létrehozásakor meg kell adnunk azt a Node-ot, ahol létrehozzuk a virtuális gépet. A Hyper-V kezelőt sem a gép létrehozásakor, sem kezelésekor nem kell használunk, minden feladatot a Failover Cluster Managerből tudunk elvégezni.

Ha kiválasztottuk a fürttagot, meg kell adnunk az új Virtuális gép nevét, és a konfigurációs állományok és pillanatfelvételek helyét. Fontos, hogy ez már a CSV-n legyen:



Ezután a szokásos módon meg kell adnunk a kezdeti memóriát, és engedélyezhetjük a dinamikus memóriakezelést. Fontos, hogy az összes node-on kell, hogy legyen ennyi szabad memóriánk, különben a VM nem tud költözni.

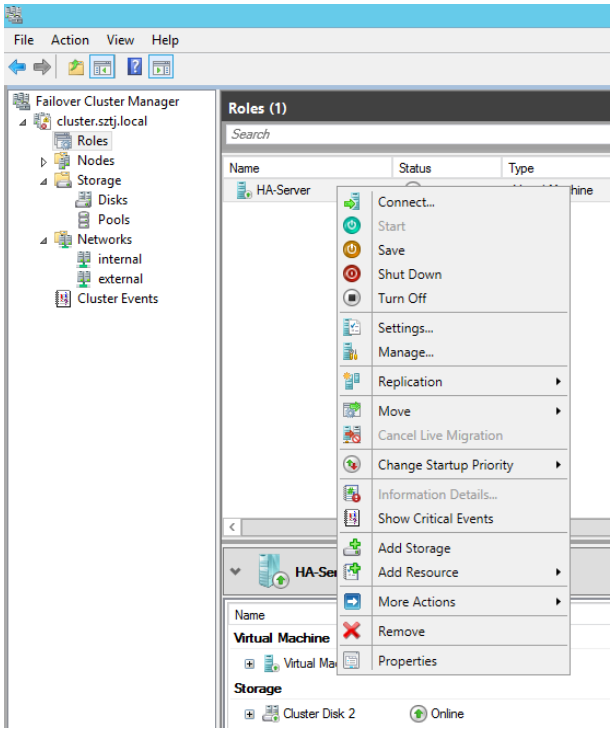
A hálózat kiválasztásánál adjuk meg a külső hálózatot. Mindkét Hyper-V hoszton ugyanazt a hálózati elnevezést kell használnunk, hogy zökkenőmentes legyen a költözés

A VHD állományunkat ismét a CSV mappában kell elhelyeznünk. Mivel ebben a mappában tárolódnak a konfigurációs állományok és a pillanatfelvételek, úgy tervezzük az iSCSI lemezünket, hogy ezek mind elférjenek. Ha a pl a VHD-t 2TB-ra méretezzük, a CSV alapú lemeznek legalább 3TB-ot érdemes adni.

Az utolsó lépésben a telepítési forrást kell kiválasztanunk. Ha van a hálózatunkon WDS, akkor érdemes hálózatról telepíteni, de a telepítés végén az örökölt hálózati kártyát ki kell majd cserélnünk szintetikus kártyára.

A varázsló végén létrejön a virtuális gépünk, amit a Cluster managerből kezelhetünk, hasonlóan a Hyper-V managerhez:

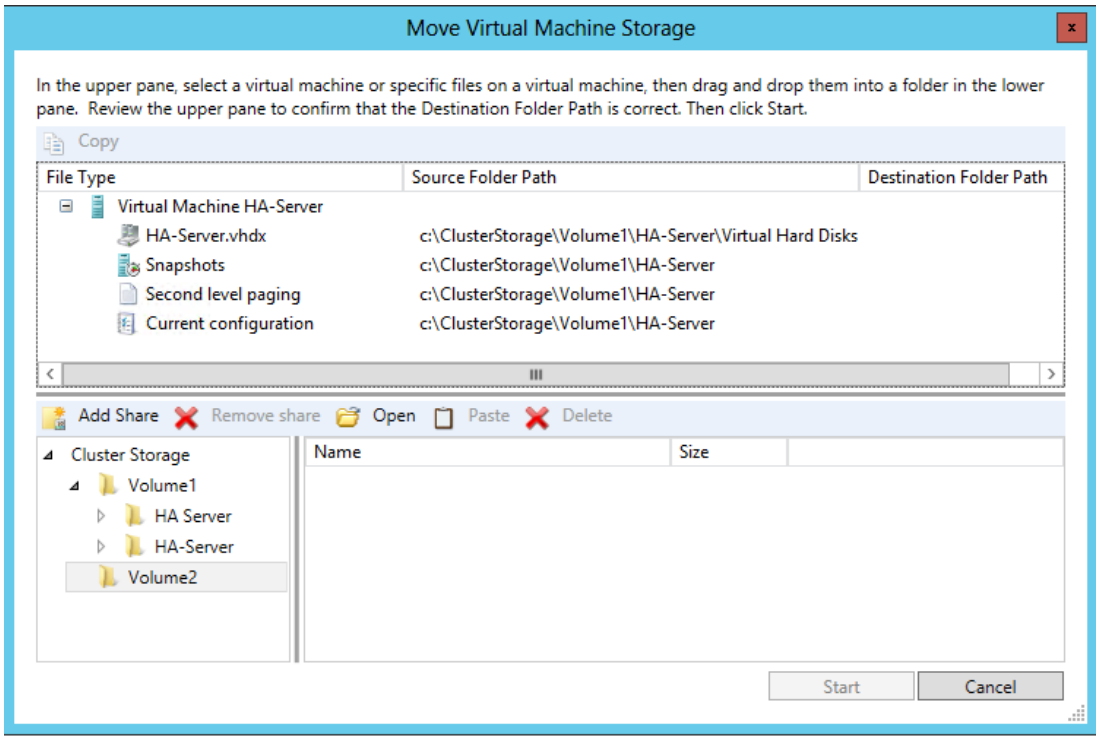
- A settings részben a konfigurációt módosíthatjuk
- A manage menüből a Hyper-V managert indíthatjuk
- Lemezt hozzáadni a lenti Add Storage varázslóval tudunk
- A gép kezelését (start/stop/save) is itt érjük el.
- Engedélyezhetjük a replikációt egy másik fürtre vagy különálló Hyper-V hosztra.
- A properties részben adhatjuk meg a preferált Hyper-V hosztot, illetve failover/failback tulajdonságait.



18.3.1 Virtuális gépek mozgatása

A failover Cluster-ben létrehozott virtuális gépek mozgatásakor a következő lehetőségek közül választhatunk:

- Live migration: a gép menet közbeni költöztetése, leállást nem igényel.
- Quick migration: a virtuális gépek mozgatás hosztok között. Ebben az esetben az új hoszton a virtuális gép újraindul. Tipikusan nem tervezett leállásnál használjuk, amikor az aktív fürttag már nem működik, így nincs lehetőség Live Migration-re. Ebben az esetben a memória tartalma elveszik.
- Virtuális gép vagy tároló migrálása: megegyezik a *Virtualizáció* fejezetben megismert technológiákkal: a bekapcsolt virtuális gépeket tudjuk mozgatni host-on belül másik könyvtárba, akár Offloaded Data Tranferrel (ODX)
- Virtuális gépek exportálása/importálása: gép leállással jár, akkor lehet érdemes, ha másik fizikailag más környezetbe mozgatjuk a virtuális gépeinket, vagy nincs hálózati kapcsolat a forrás és a célgépek között. A Windows Server 2012-ben akkor is importálhatunk virtuális gépeket, ha azok nem voltak megfelelően exportálva.



Storage Migration a Hyper-V konzolon. A virtuális gép alkatrészeit drag&drop-al mozgathatjuk a storage különböző mappáiba

19 Windows 8 bevezető

A Microsoft szerint a Windows 8 elmossa a határokat a platformok között, minden eddiginél tökéletesebb felhasználói élményt nyújt érintőképernyős, illetve hagyományos, billentyűzettel és egérrel vezérelt eszközökön egyaránt. Tulajdonképpen egy olyan rendszerbe akarja integrálni termékeit a cég, amely tökéletesen átjárható, és hasonló felülettel rendelkezik. Egy felhasználó, ha a Windows 8 munkaállomása után kezébe vesz egy Windows 8 RT-vel rendelkező tabletet, vagy előveszi a Windows Phone 8 alapú okostelefonját, kis túlzással szinte ugyanazt a felületet látja, azaz nem kell megtanulnia minden eszközének kezelését. Az adatokkal hasonló a helyzet, hiszen felhő segítségével bárhonnan és bármikor elérheti a Skydrive-on vagy éppen az Office 365-ön lévő adatait.

A fenti céloknak az elérésének érdekében a Microsoft teljesen az alapoktól kezdte el a Windows 8 fejlesztését. Egy olyan Windows kiadást kell elképzelnünk, amely olyan mérföldkőnek tekinthető, mint egykor a Windows 95 kiadása volt. A PC piac zsugorodik, egyre kevesebb eladást produkál, a felhasználók a nehéz, statikus PC és a szintén nehézkes notebookok helyett a könnyen hordozható eszközökre tértek át. Ez arra ösztökélte a informatikai ipar szereplőit, hogy tablet és okostelefon eszközökre fejlesszenek, akár hardver, akár szoftver termékekről van szó.

A Windows 8 Metro felülete megtalálható számos eszközön és kiválóan használható az érintőképernyős eszközökön. A felület csempékből épül fel, minden egyes csempe egy-egy alkalmazásnak felel meg. De ezen kívül különböző információk is elérhetőek, azaz nem kell feltétlenül megnyitnunk semmilyen programot, ha éppen az időjárásra, vagy éppen a beérkezett levelek számára vagyunk kíváncsiak.

A megváltozott felület a Start menü megszünését vonta maga után ezt felváltotta az ikonsor.

19.1 Újdonságok

A Windows 8-ban számos újdonságot találhatunk, amelyek a következők:

- Internet Explorer 10, Metro-stílusban, mely nem támogatja többé az ActiveX-vezérlőket, de kezeli az Adobe Flash-t.
- Microsoft-fiók és SkyDrive-integráció, amelynek eredményeképp az adatok szinkronizálhatóak egy másik számítógéppel.
- Jelszó helyett kép alapú védelem és PIN-kód is megadható.
- A Windows Intéző is megkapja a szalagos menüsort.
- Hibrid indítás, mely ötvözi a hagyományos kilépést a hibernálással, felgyorsítva a rendszer felállásának idejét.
- Windows To Go - pendrive-ról indítható operációs rendszer.
- Két új helyreállítási funkció: az egyik segítségével a rendszerfájlok visszaállíthatóak eredeti állapotukba, a másikkal pedig a teljes Windows rendszer visszaállítható a telepítéskori állapotba.
- USB 3.0 támogatás
- Újfajta képernyőlezárási metódus
- Vadonatúj Feladatkezelő
- Xbox Live integráció

- Valós merevlemezek virtuális meghajtóként kezelése, akár több valódi merevlemezből is létrehozható egyetlen virtuális.
- Továbbfejlesztett családbiztonsági funkciók
- Vírusirtóként is funkcionáló Windows Defender

19.2 Kiadások

A következő Windows 8 kiadásokkal találkozhatunk, ezek a következőek:

Windows 8: Alapvetően otthoni használatra tervezve, az vállalati funkciókat kiszedték belőle, mint pl. háttértár titkosítást, virtualizációt vagy éppen a group policy szikronizációt. Ezeken kívül viszont megtaláljuk a Windows Store-t, amely segítségével könnyedén tudunk telepíteni új alkalmazásokat, illetve ugyanezen a felületen frissíthetjük is. Az itt letöltött alkalmazásokat aztán 5 eszközön használhatjuk.

Windows 8 Professional: Gyakorlatilag a Windows 7 Professional verziójának utódja. Ezt már bátran használhatjuk üzleti környezetben is, megkapta a Windows 8 consumer verzióban lévő funckiókat és a Bitlocker és EFS titkosítást, a virtualizációs, tartományi csatlakozási lehetőséget.

Windows 8 Enterprise: Nagyvállalati verzió, ebben minden funkció megtalálható, de csak mennyiségi licensszel rendelkező vállalatoknál érhető el. A Windows 8 Professional verzión felül megtaláljuk a Applockert, a Windows to Go-t, DirectAccess-t, Branchcache-t, Hyper-V Remote FX támogatást. A Windows to Go egy olyan lehetőség, amely más operációs rendszereknél már egy ideje elérhető, tulajdonképpen egy élő USB eszközön tárolt Windows 8-ról beszélünk. Az előnye, hogy bármilyen USB eszköz indításra képes PC-n elindítható, ezáltal otthonunkon kívül is a megszokott felület fogad minket. Egy külső helyszinen lévő PC-re nem kell mentenünk semmit és a biztonsági beállítások a Windows-unkon már előre konfiguráltak (mint pl. Windows tűzfal, virusvédelem, publikus hálózati beállítások).

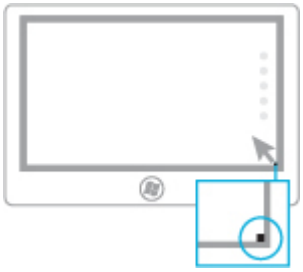
Windows 8 RT: Tabletekre optimalizált, érintőképernyővel rendelkező, Office 2013-mas termékekkel ellátott kiadás.

A Windows 7-ről történő frissítés esetén a következő lehetőségek állnak rendelkezésünkre:

<table>
<tr><th>Windows 7 kiadás</th><th>Windows RT frissítés</th><th>Windows 8 frissítés</th><th>Windows 8 Pro frissítés</th><th>Windows 8 Enterprise frissítés</th></tr>
<tr><td>Enterprise</td><td rowspan="6">Nem</td><td rowspan="3">Nem</td><td>Nem</td><td>Igen</td></tr>
<tr><td>Ultimate</td><td rowspan="5">Igen</td><td>Nem</td></tr>
<tr><td>Professional</td><td>Igen</td></tr>
<tr><td>Home Premium</td><td rowspan="3">Igen</td><td rowspan="3">Nem</td></tr>
<tr><td>Home Basic</td></tr>
<tr><td>Starter</td></tr>
</table>

19.3 Használat

Az egér és a billentyűzet Windows rendszerben történő használata – főként az asztal esetében – alapvetően nem változott. Ez a témakör útmutatást nyújt a Windows 8 új szolgáltatásainak egérrel és billentyűparancsokkal történő használatához, valamint néhány megszokott funkció megkereséséhez az új környezetben.

Művelet	Egérrel	Billentyűzettel
A gombok aktiválása (Keresés, Megosztás, Kezdőképernyő, Eszközök és Beállítások).	Mutasson a jobb felső vagy a jobb alsó sarokra a gombok megjelenítéséhez. (Vigye a mutatót a sarokba egészen addig, amíg el nem tűnik.) Amikor megjelennek a gombok, a kurzort a szélen fel-le mozgatva kattintson a kívánt gombra. 	Minden gomb: Windows billentyű +C Keresés gomb: Windows billentyű +Q Megosztás gomb: Windows billentyű +H Kezdőképernyő gomb: Windows billentyű Eszközök gomb: Windows billentyű +K Beállítások gomb: Windows billentyű +I
Keresés a számítógépen (alkalmazások, beállítások és fájlok), az interneten vagy egy alkalma-	Mutasson a jobb felső vagy a jobb alsó sarokra a gombok megjelenítéséhez. (Vigye a mutatót a sarokba egé-	Ha a kezdőképernyőn van, kezdje el beírni a keresőkifejezést. Ha látni szeretné a számí-

zásban.	szen addig, amíg el nem tűnik.) Amikor megjelennek a gombok, a kurzort a szélen fel-le mozgatva kattintson a **Keresés** gombra, majd adja meg a keresett kifejezést. Ha beállításokat, fájlokat vagy másik alkalmazást kíván keresni, kattintson a kívánt kategóriára.	tógépén lévő összes alkalmazást, kattintson a jobb gombbal a kezdőképernyőre, majd kattintson a **Minden alkalmazás** gombra. Keresés az alkalmazásokban vagy egy alkalmazás megkeresése: dows billentyű +Q Beállítások keresése: Windows billentyű +W Fájlok keresése: Windows billentyű +F
Jelenítse meg a kezdőképernyőt.	Mutasson a bal alsó sarokra. Amikor megjelenik a kezdőképernyő, kattintson a sarokra. Mutasson a jobb felső vagy a jobb alsó sarokra a gombok megjelenítéséhez. (Vigye a mutatót a sarokba egészen addig, amíg el nem tűnik.) Amikor megjelennek a gombok, a kurzort a szélen fel-le mozgatva kattintson a **Kezdőképernyő** gombra.	A billentyűzeten nyomja meg a Windows billentyűt .
Parancsok és helyi menük elérése.	A jobb gombbal kattintva megjelenítheti a parancsokat és a helyi menüket. A jobb gombbal az elemekre kattintva általában megjelennek az adott elem esetében elérhető lehetőségek. 	Windows billentyű +Z A Tab billentyűvel vagy a nyílbillentyűkkel jelölje ki az elemeket, majd nyomja meg a Szóköz vagy az Enter billentyűt.
Váltás az utoljára használt alkalmazások között.	A legutóbb használt alkalmazásra történő váltáshoz mutasson a bal felső sarokra. (Vigye a mutatót a sarokba egészen addig, amíg el nem tűnik.) Amikor megjelenik	Windows billentyű +Tab

	az előző alkalmazás, kattintson a sarokra. Egy másik alkalmazásra történő váltáshoz mutasson a bal felső sarokra, és finoman mozgassa lefelé a mutatót. Amikor megjelennek az alkalmazások, kattintson a kívánt alkalmazásra. 	
Két alkalmazás egymás melletti használata alkalmazás dokkolásával. Megjegyzések Alkalmazások dokkolásához legalább 1366×768 képpontos képernyőfelbontás szükséges. A beállítás ellenőrzése: A Képernyőfelbontás megnyitásához pöccintsen befelé a képernyő jobb széléről, koppintson a **Keresés** gombra (egér használata esetén mutasson a képernyő jobb felső sarkára, húzza a mutatót lefelé, és kattintson a **Keresés** gombra), a keresőmezőbe írja be a **Képernyő** kifejezést, koppintson vagy kattintson a **Beállítások** kategóriára, majd a **Képernyő** találatra. Az asztalt alkalmazásként kezeli a rendszer.	Vigye a mutatót a bal felső sarokba, amíg meg nem jelenik a második alkalmazás, majd húzza ezt az alkalmazást a képernyő jobb vagy bal oldalára, amíg meg nem jelenik mögötte egy üres terület. Ha a bal felső sarokra mutat, majd lefelé mozgatja a mutatót, megtekintheti a nemrég használt alkalmazásokat. A kívánt alkalmazást kattintással és húzással dokkolhatja. Megtarthatja az alkalmazás aktuális méretét, vagy átméretezheti úgy, hogy a teljes képernyő kétharmadát töltse ki.	Windows billentyű +pont
Az asztal megnyitása.	Jelenítse meg a kezdőképernyőt, és kattintson az Asztal csempére.	Windows billentyű +D

Nagyítás vagy kicsinyítés	A kezdőképernyőn használja a nagyítás ikonját a jobb alsó sarokban, vagy használja a Ctrl+görgetőkerék kombinációt.	Ctrl+pluszjel – nagyítás Ctrl+mínuszjel – kicsinyítés
Alkalmazás bezárása	Mutasson a képernyő felső szélére, majd kattintson az alkalmazásra, és húzza a képernyő aljára. A bal felső sarokra mutatva, majd a mutatót lefelé húzva is bezárhatja a nemrég használt alkalmazásokat. Kattintson a jobb gombbal a kívánt alkalmazásra, majd kattintson a **Bezárás** gombra.	Alt+F4
Leállítás	Mutasson a jobb felső vagy a jobb alsó sarokra a gombok megjelenítéséhez. (Vigye a mutatót a sarokba egészen addig, amíg el nem tűnik.) Amikor megjelennek a gombok, a kurzort a szélen fel-le mozgatva kattintson a **Beállítások** gombra. Kattintson a **Főkapcsoló** ikonra, és válassza ki a kívánt leállítási lehetőséget.	Nyomja le a **Ctrl+Alt+Del** billentyűkombinációt. A TAB billentyűvel lépjen a **Főkapcsoló** ikonra. Megjelenik a leállítási lehetőségek listája. A fel és le nyílbillentyűkkel válassza a kívánt lehetőséget. Nyomja meg az **Enter** billentyűt.

19.4 Keresés

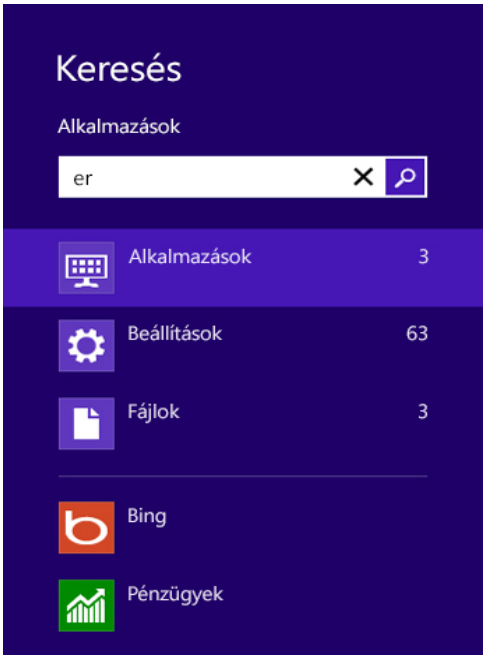
A számítógépen lévő alkalmazások, beállítások és fájlok a Keresés gombbal kereshetők. A Keresés gomb használható a megnyitott alkalmazásban vagy egy másik kijelölt alkalmazásban lévő elemek kereséséhez is. A Keresés gombbal kereshet például új alkalmazásokat az Áruházban vagy névjegyeket a Kapcsolatok alkalmazásban.

A Keresés gomb használata

Pöccintsen befelé a képernyő jobb széléről, és koppintson a **Keresés** elemre. (Egér használata esetén mutasson a képernyő jobb felső sarkára, húzza a mutatót lefelé, és kattintson a **Keresés** elemre.)

Adja meg a keresési kifejezést.

Ha alkalmazást, beállítást vagy fájlt keres a számítógépen, kattintson az **Alkalmazások**, a **Beállítások** vagy a **Fájlok** lehetőségre. Ha adott alkalmazáson belül keres, koppintson vagy kattintson a listában az alkalmazásra.



Ha billentyűzettel rendelkezik, és a kezdőképernyőn van, a Keresés megnyitásához egyszerűen csak kezdjen el beírni.

Ha a számítógépen keres egy alkalmazást, megnyomhatja a Windows billentyű +Q billentyűkombinációt Ha fájlt keres, megnyomhatja a Windows billentyű +F billentyűkombinációt.

20 Hordozható munkakörnyezet

Napjaink felhasználói különböző ugyan különböző eszközökről dolgoznak – céges PC, saját laptop, VDI, RDS környezet, de minden eszközön azonos felületet szeretnének elérni: asztal, levelezés beállítások, Internetes kedvencek, stb. Ha belegondolunk a saját munkavégzési szokásainkba, üzemeltetőként hasonló igényeink vannak: a tanúsítványok, távoli asztali beállítások, mentett jelszavak bármelyik kliensre vagy kiszolgálóra bejelentkezve velünk legyenek, és akár a számítógépünk cseréje is kevésbé legyen fájdalmas: ne kelljen az összes beállítást újra megadni. A Windows 8-ban a jól ismert technológiák mellett néhány újjal is találkozunk:

- felhasználói profilok
- mappaátirányítás
- File History
- Elsődleges számítógép
- Windows To Go
- UE-V

20.1.1 Felhasználói profilok

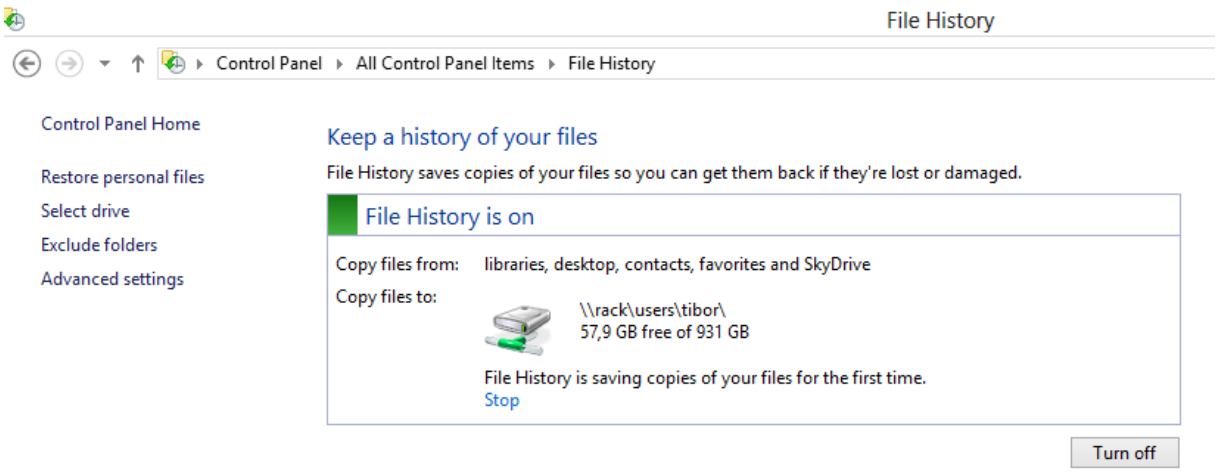
A felhasználó személyes beállításai, az asztaltól kezdve a nyomtatókon keresztül a tárolt jelszavakig mind a felhasználó profiljában tárolódik. Amikor a felhasználó először bejelentkezik, az alapértelmezett profilból kap egy másolatatot, és a későbbiekben ezt használja. Ez a profil lehet helyileg tárolt, de megadhatjuk azt is, hogy kilépéskor szinkronizáljuk a kiszolgálóra, és egy másik gépre bejelentkezéskor töltsük le onnan. Ez lehetővé teszi, hogy a felhasználó bármelyik gépről bejelentkezve ugyanazt a felületet használhassa, de vannak vele kihívások is: ha egy felhasználó egy időben két gépre jelentkezik be, ahonnan később jelentkezik ki, az a beállítás mentődik, így a másik gépen végzett módosítások elvesznek. A másik probléma, hogy ha a felhasználó az asztalán tárol dokumentumokat, a profil mérete több GB-os is lehet, ami minden bejelentkezéskor letöltődik, kilépéskor pedig visszatöltődik a kiszolgálóra, így mind a bejelentkezési, mind a kijelentkezési időt jelentősen megnövelheti. Megadhatunk kötelező profilt is, ha azt szeretnénk, hogy a felhasználók egységes felületet érjenek el, amin nem tudnak változtatni – például iskolai vagy megosztott gépes környezetben.

20.1.2 Mappaátirányítás

Csoportházirendből szabályozhatjuk, hogy a tartományi felhasználóink a fontos dokumentumaikat ne (ne csak) a helyi gépen tárolják, hanem a kiszolgálók megosztásain, vagy helyileg és a kiszolgálón, folyamatosan szinkronizálva. A dokumentumok mappa átirányítása mellett vihetjük a többi fontos mappát is, mint a fényképek, videók, letöltések, keresések, stb., így minden fontos adatot biztonságban tudhatunk. Ha a felhasználók hazaviszik a hordozható gépeiket, a kapcsolat nélküli fájlok segítségével otthonról ugyanúgy dolgozhatnak a fájljaikkal, és a céges hálózatra csatlakozáskor a változások szinkronizálódnak. A kapcsolat nélküli elérést a felhasználók bármelyik további mappára is engedélyezhetik, pl. közös mappák, dokumentációk, stb.

20.1.3 File History

Új szolgáltatás a Windows 8-ban, képes arra, hogy a helyi mappákat adott időközönként mentse hálózati meghajtóra, vagy külső adattárolóra. Szemben a Windows 7-ben használt előző verziókkal, itt lehetőségünk van a mentéseket a kiszolgálón tárolni. Beállítani a Windows 8-as vezérlőpoltban tudjuk, a File History menüben:

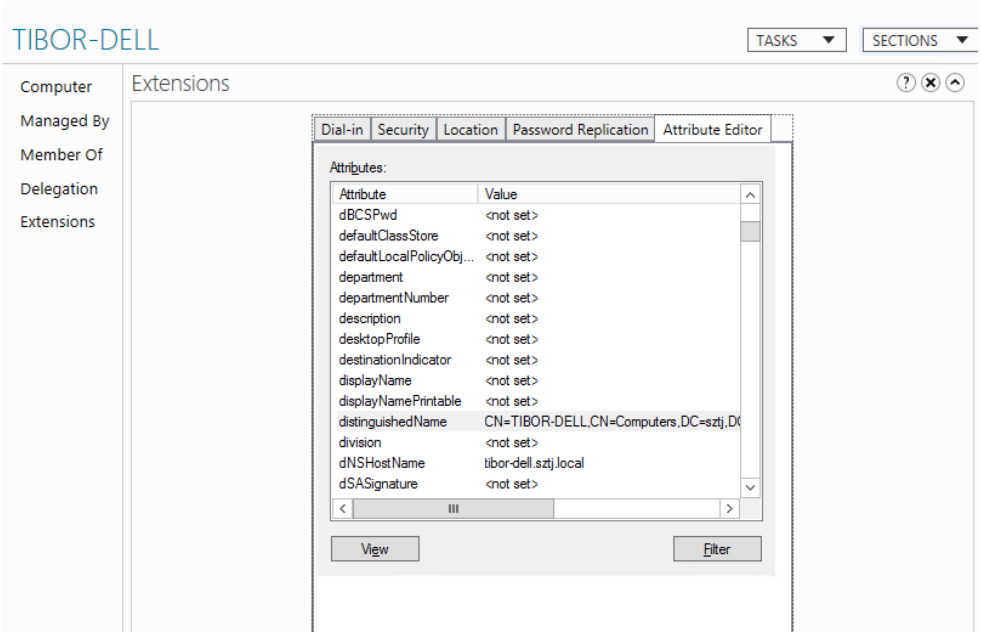


A File History alapesetben menti az összes mappánkat, amik a libraries-ben szerepelnek, az asztalt, a kapcsolatokat, kedvenceket és a SkyDrive-unk tartalmát. Ha további mappákat is szeretnénk menteni, akkor egyszerűen fel kell azokat venni bármelyik Library-be, illetve ki is zárhatunk mappákat a Library-n belül.

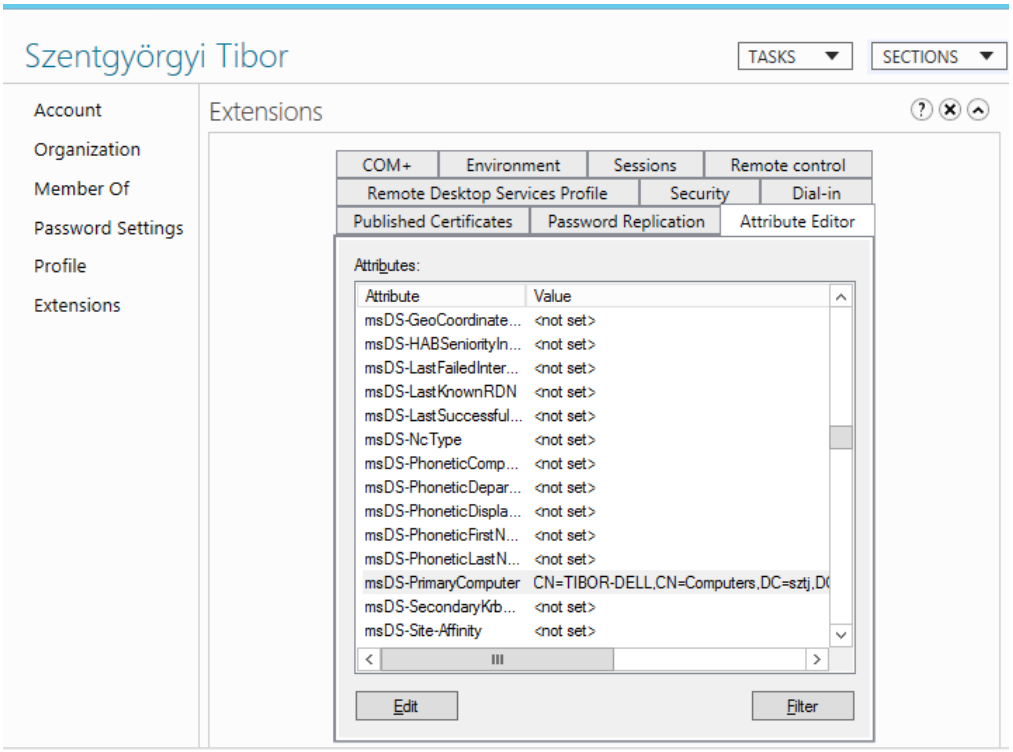
20.1.4 Elsődleges számítógék kijelölése

A vándorló profilok, mappaátirányítás és a kapcsolat nélküli fájlok hasznosak lehetnek a felhasználók többségének, de egy rendszergazda nem szeretné, hogy minden beállítása letöltődjön az összes gépre, ahová bejelentkezik, vagy egy cégvezető sem szeretné, hogy a profiljában lévő bizalmas anyagok lekerüljenek bármelyik kliens gép helyi lemezére, ahová bejelentkezik. A Windows Server 2012-ben kijelölhetünk a felhasználóknak elsődleges gépeket, ahová szeretnénk a beállításaikat vándoroltatni, a többi gépen pedig ideiglenes helyi profil jön létre. A beállításokat az új Active Directory Administrative Center-ből tudjuk elérni: első lépésben a számítógép Distinguished Name értékét kell megkeresnünk, valami ilyesmit: CN=TIBOR-DELL,CN=Computers,DC=sztj,DC=local

Ezt az ADAC-ben a számítógép objektum Extensions / Attribute Editor részében fogjuk megtalálni:

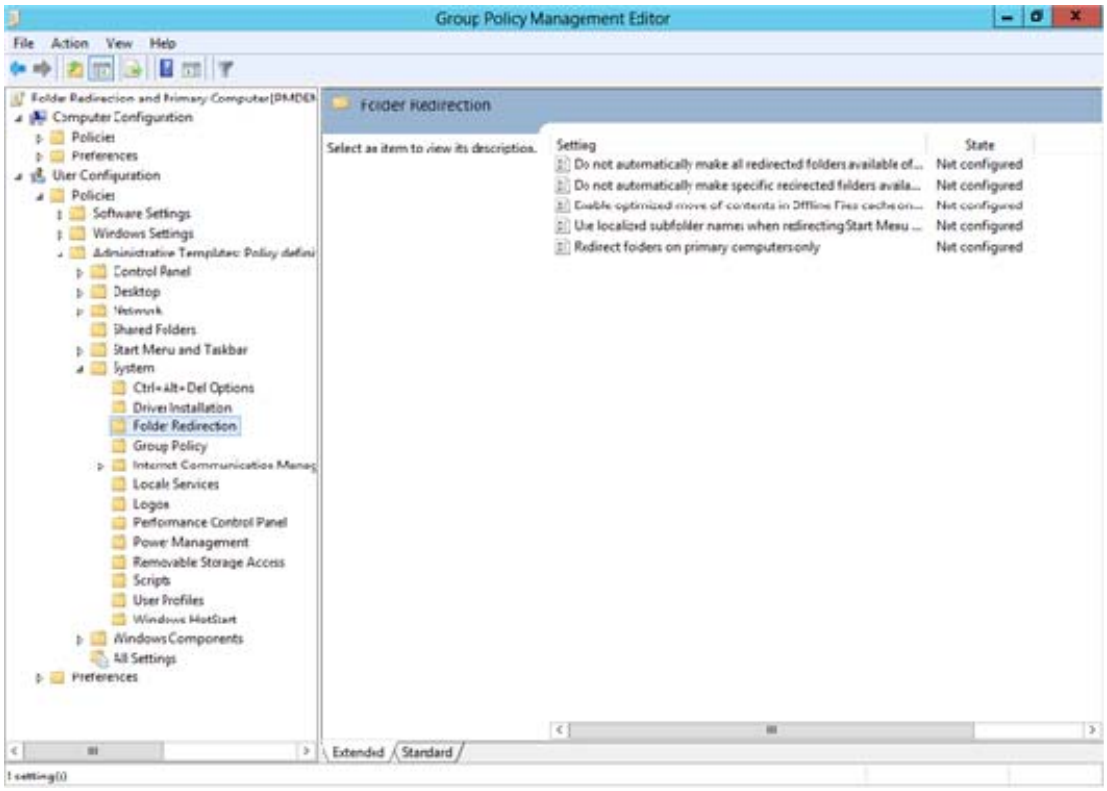


Ezt az értéket kell megadnunk a felhasználónak, szintén az ADAC-ban, szintén az Extensions / Attribute Editorban, az msDS-PrimaryComputer-nél. Természetes több elsődleges gépet is megadhatunk:



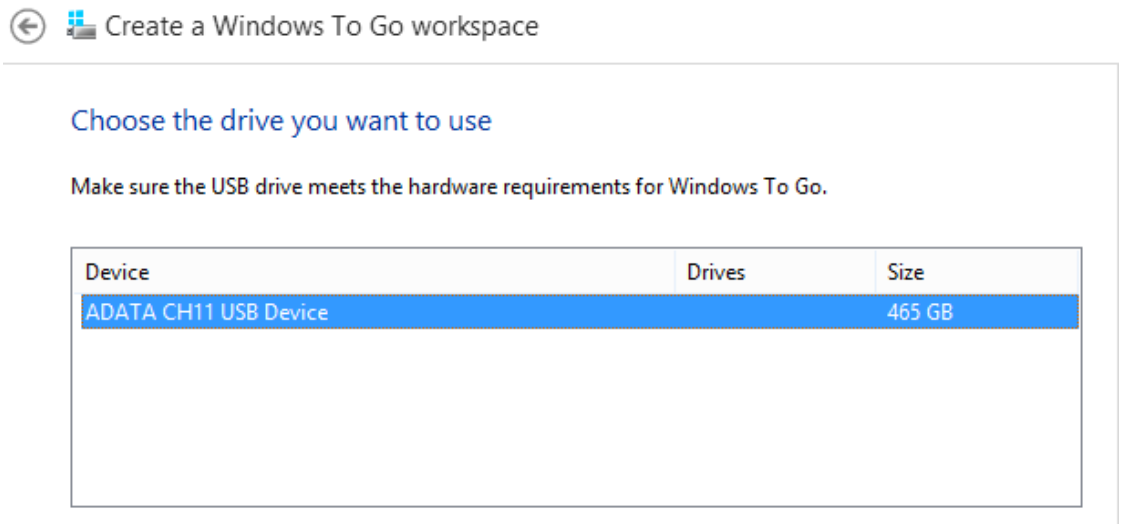
Ha ezzel készen vagyunk, már csak egy olyan házirendet kell létrehoznunk, ahol megadjuk, hogy a mappa átirányítás csak az elsődleges gépeken érvényesüljön.

Ezt a mappaátirányítási házirendben, a *User Configuration/Policies/Administrative Templates/System/Folder redirection* útvonalon találjuk, a „Redirect Folders on primary computers only” opciót kell engedélyeznünk:

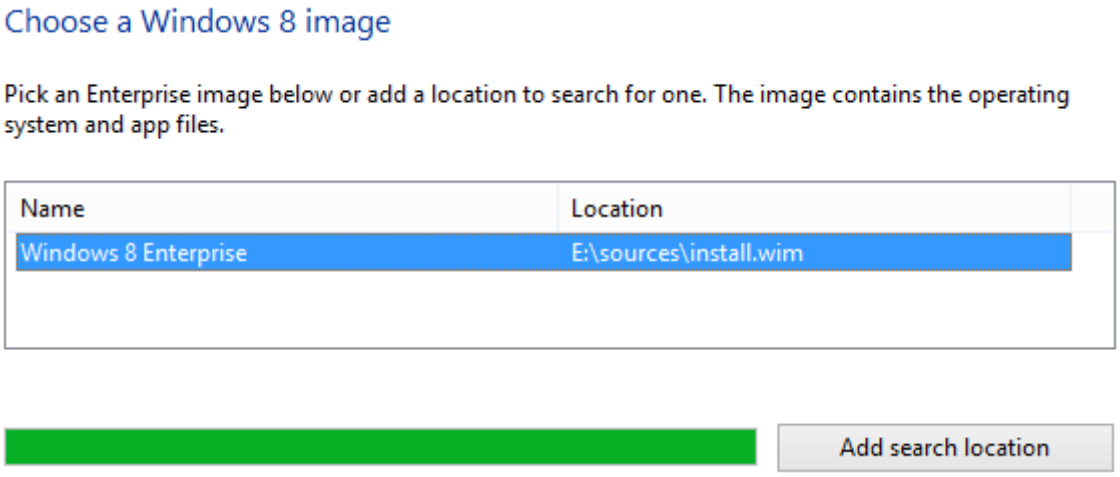


20.1.5 Windows To Go

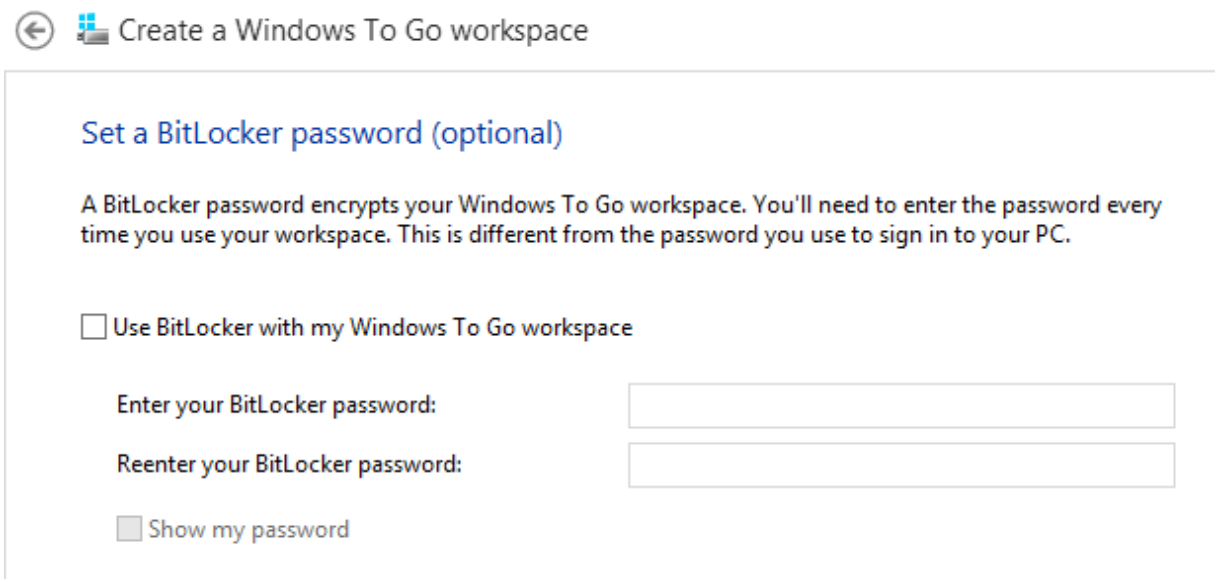
A Windows 8-ban új szolgáltatás (és az USB 3-as szabvány) lehetővé teszi, hogy olyan USB pendrive-okat hozzunk létre a felhasználóknak, ahonnan el tudják indítani a Windows 8-at, és a céges felhasználói felületüket tudják használni bármelyik számítógépen. A külsős felhasználóknak tehát nem kell mindenképpen saját számítógépet adni, elég egy Windows To Go USB eszköz, előtelepítve a céges hálózati feltételeknek megfelelően – pl beállított DirectAccess vagy VPN – a felhasználónak szükséges alkalmazásokkal, stb. A Windows To Go-n futó Windows 8-at biztonsággal használhatjuk bármelyik számítógépen, mert USB-ről induláskor a helyi gép merevlemezei nem lesznek elérhetők. A Windows To Go a Windows 8 Enteprise verziójában található meg, a készítését is egy már feltelepített Windows 8 Enterprise-ból tudjuk elindítani:



A létrehozásához szükségünk lesz egy USB 3-as pendrive-ra, vagy jelen esetben egy USB 3-as külső merevlemezre, illetve a telepítő kérni fogja a Windows 8 telepítőlemezét is:



Az USB eszközünket erősen javasolt Bitlocker-el titkosítani, hiszen a felhasználók sokkal könyebben elhagyhatják, mint egy notebookot:



A megadott jelszót a Windows To Go minden indításkor kérni fogja.

Ha minden információt megadtunk, a varázsló formázza az USB eszközt, majd feltelepít rá egy teljesen új Windows 8 Enterprise-t.

21 Office 365

Az Office 365 a Microsoft felhőalapú szolgáltatáscsomagja, iskolai környezetben Microsoft Digitális Alapcsomag néven is ismerős lehet. Ez váltja ki a Tiszta Szoftver program szerver termékeinek egy részét, és ez az utóda a nagy sikerrel futó Live@edu rendszernek, amely világszerte iskolák ezreinek a levelezését biztosítja.

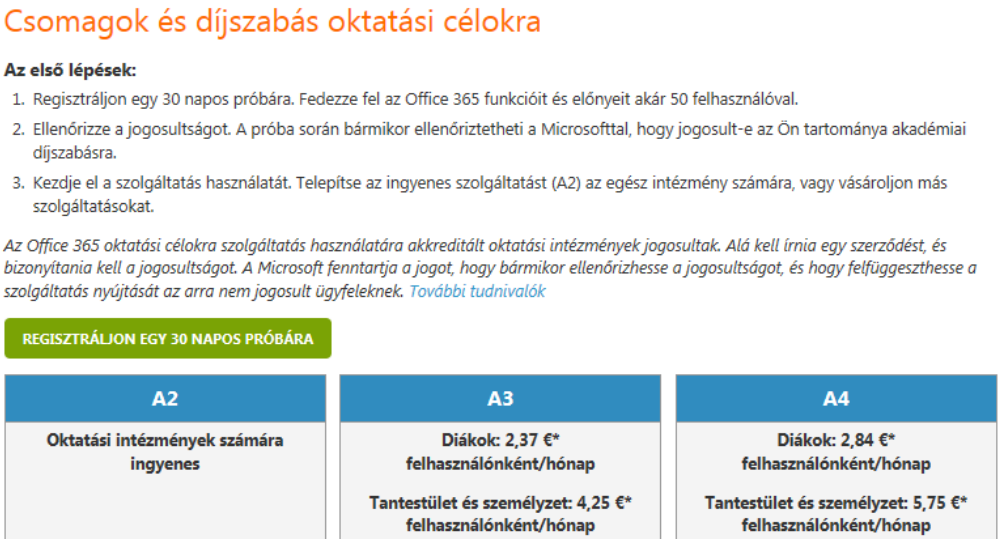
Három fő részből áll: az Exchange Online segítségével egységes intézményi levelezőrendszert hozhatunk létre saját domain név használatával. A SharePoint Online egy fejlett, és az Office alkalmazásokba integrált intranet rendszert kínál, és lehetőséget ad egy egyszerűen kezelhető publikus weboldal létrehozására is. A Lync Online pedig egy azonnali üzenetküldő, konferencia és együttműködés-támogató rendszer, amely más szolgáltatásokkal is összekapcsolható, és képes kiváltani akár a belső hagyományos telefonhálózatot is.

A könyvnek ebben a fejezetében a rendszert rendszergazdai szempontból mutatjuk be, a regisztrációtól kezdődően, a már helyileg telepített szolgáltatások felhőbe költöztetésén át egészen azok kezeléséig.

21.1 Regisztráció

A szolgáltatásra a http://office365.hu oldalon tudunk regisztrálni, ahol a *Csomagok és díjszabás* menüben válasszuk az *Oktatás* menüpontot. Itt kattintsunk a *Csomagok összehasonlítása* gombra. Ezen az oldalon összehasonlíthatjuk az oktatási csomagokat, melyekből az A2 csomag ingyenesen jár, a további csomagokat pedig az oldalon jelzett előfizetési díj ellenében vehetjük igénybe.

A regisztrációhoz kattintsunk a *Regisztráljon egy 30 napos próbára* feliratú gombra.



A közoktatás számára a nagyobb csomagok is kedvezményes áron érhetőek el

21.1.1 Adatok megadása

A gombra kattintás után egy űrlapot fogunk látni. Ebben az alapvető intézményi adatok megadása után találunk egy *Új tartománynév* mezőt. Ez a név a „.onmicrosoft.com” utótaggal a szervezetünk egyedi azonosítója lesz az Office 365 rendszerben. Ameddig nem rendeljük

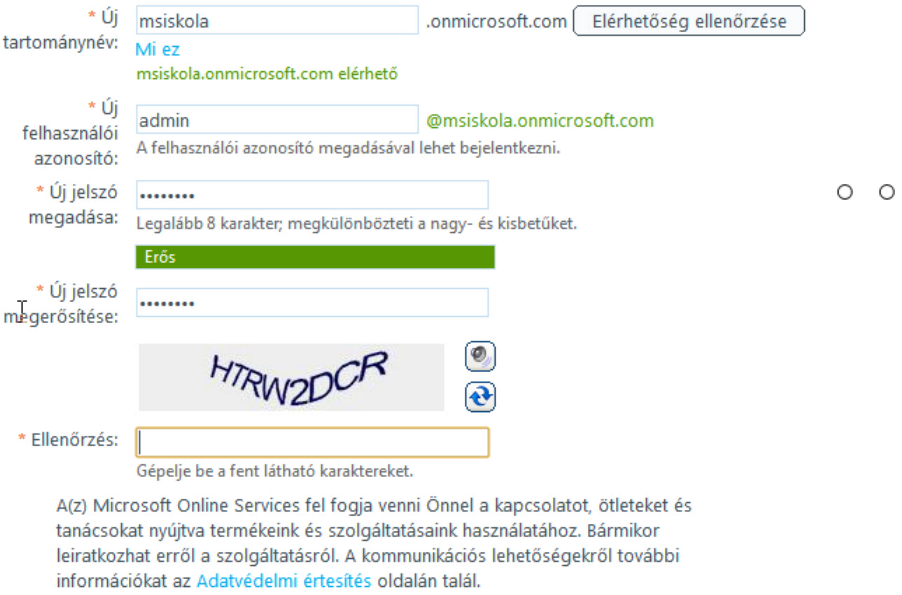
hozzá a saját domain nevünket a szervezethez, addig a felhasználók e-mail címének ez lesz az utótagja, tehát a kukac utáni része.

Az elérhetőség ellenőrzése gombra kattintva kiderül, hogy szabad-e még a választott tartománynév, és ha igen, akkor további mezők jelennek meg az űrlapon.

Meg kell adnunk egy új felhasználói azonosítót. Ez lesz az első, rendszergazdai jogkörökkel bíró felhasználó azonosítója. Fontos, hogy ha a későbbiekben Active Directory szinkronizációt szeretnénk használni, akkor az itt megadott azonosító lehetőleg ne létezzen az AD tartományban. Használjuk például az *admin, admin365, felhoadmin*, vagy ezekhez hasonló azonosítót.

A példákban a tartománynév *msiskola.onmicrosoft.com* lesz, a felhasználói azonosító pedig *admin@msiskola.onmicrosoft.com*.

Az ellenőrző kód beírása után kattintsunk az *Elfogadás és folytatás* gombra.



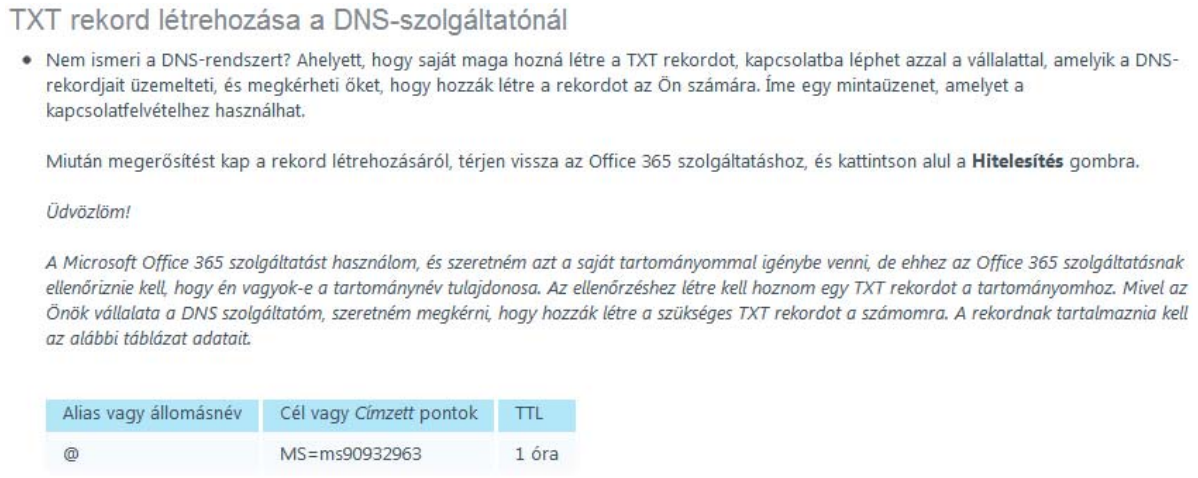
Az admin felhasználónak korlátlan a hozzáférése – fontos az erős jelszó

21.1.2 Saját domain név hozzáadása és ellenőrzése

A következő oldalon egy varázsló fogad bennünket, amely egy új domain név hozzáadásában és a tulajdonjog ellenőrzésében segít. A varázsló első, üdvözlőoldalán eldönthetjük, hogy most azonnal szeretnénk-e hozzáadni és ellenőrizni a domaint, vagy inkább később térünk vissza erre. Amennyiben már van domain nevünk, kattintsunk a *Tovább* gombra. Ha még nincs, akkor addig is kipróbálhatjuk az Office 365-öt, de bizonyos szolgáltatások nem fognak működni saját domain név nélkül.

Ha továbbléptünk, meg kell adnunk a domain nevet, pl.: msiskola.hu, majd kattintsunk ismét a *Tovább* gombra. A következő lapon a rendszer ellenőrzi, hogy a megadott domain név felett valóban mi rendelkezünk-e. Ezt kétféleképpen tehetjük meg: TXT rekord létrehozásával (ajánlott), vagy MX rekord létrehozásával. Mindkét módszerhez részletes instrukciókat találunk az oldalon, illetve egy mintalevelet is, amit a szolgáltatónak küldhetünk el, ha magunk nem vagyunk jártasak a DNS rendszerben.

Ha magunk hoztuk létre a kért bejegyzést, akkor a *Hitelesítés* gombra kattintva rögtön ellenőriztethetjük is a rendszerrel a domaint. Ha levelet küldtünk a szolgáltatónak, vagy a módosítások még nem léptek érvénybe, akkor kattinthatunk a *Később ellenőrzöm* linkre. Ebben az esetben, ha megérkezett a szolgáltatónk visszaigazolása, az adminisztrációs felület *Tartományok* menüpontja alatt hajthatjuk végre a hitelesítést.


TXT rekord létrehozása a DNS-szolgáltatónál

- Nem ismeri a DNS-rendszert? Ahelyett, hogy saját maga hozná létre a TXT rekordot, kapcsolatba léphet azzal a vállalattal, amelyik a DNS-rekordjait üzemelteti, és megkérheti őket, hogy hozzák létre a rekordot az Ön számára. Íme egy mintaüzenet, amelyet a kapcsolatfelvételhez használhat.

Miután megerősítést kap a rekord létrehozásáról, térjen vissza az Office 365 szolgáltatáshoz, és kattintson alul a **Hitelesítés** gombra.

Üdvözlöm!

A Microsoft Office 365 szolgáltatást használom, és szeretném azt a saját tartományommal igénybe venni, de ehhez az Office 365 szolgáltatásnak ellenőriznie kell, hogy én vagyok-e a tartománynév tulajdonosa. Az ellenőrzéshez létre kell hoznom egy TXT rekordot a tartományomhoz. Mivel az Önök vállalata a DNS szolgáltatóm, szeretném megkérni, hogy hozzák létre a szükséges TXT rekordot a számomra. A rekordnak tartalmaznia kell az alábbi táblázat adatait.

Alias vagy állomásnév	Cél vagy *Címzett* pontok	TTL
@	MS=ms90932963	1 óra

Nem kell DNS szakértőnek lenni a beállításhoz – segít az előre megírt levél

21.2 Licencek igénylése

Az Office 365 rendszerben a számlázás felhasználókhoz rendelt licencek alapján történik. A licencek kaphatóak csoportokban, amiket egy betű és egy szám kombinációjával jelölnek, pl. A1, A2, A3; és kaphatóak külön-külön is, pl. csak Exchange Online. Licencet vásárolhatunk rögtön a regisztráció végén, de bármikor később is, az adminisztrációs felület *Előfizetések* menü, *Vásárlás* linkjén keresztül.

A közoktatás számára három különböző licenckonstrukció érhető el ingyen: a tantestület és a diákok az A2-es szintű Office 365 csomagot használhatják, az elballagó diákok pedig a levelezésüket tarthatják meg az *Exchange Online volt diákoknak* licenccel. Ezeknek a csomagoknak az ára 0 Euro az oldalon.

Licenc vásárlásához a *Vásárlás* oldalon kattintsunk a kiválasztott licenc melletti *Hozzáadás* linkre. A megjelenő ablakban adjuk meg, hány darab licencet szeretnénk igényelni, majd kattintsunk a *Bevásárlókocsiba* gombra. Miután a bevásárlókocsiban van az összes vásárolni kívánt licenc, kattintsunk a *Megrendelés* gombra.

Ezek után meg kell adnunk a szolgáltatás felhasználási helyét, a számlázási adatokat, a fizetés módját és ütemezését, majd el kell fogadnunk a szerződési feltételeket. A megrendelés véglegesítése után a megrendelt licencek rögtön megjelennek a *Kezelés* oldalon, és innentől kezdve felhasználókhoz is rendelhetőek.

21.3 Telepítési terv

21.3.1 Az e-mail áttelepítés tervezése

A regisztrációs folyamat végeztével elkezdhetjük megtervezni az áttérési folyamatot. Az Office 365 számos áttelepítési forgatókönyvet támogat. Hogy számunkra melyik az ideális, azt egyrészt adottságok határozzák meg, például, hogy milyen a jelenlegi levelezőrendszerünk, vagy, hogy hány postafiókkal rendelkezünk, másrészt pedig döntések, amiket meg kell hoznunk. El kell döntenünk például, hogy meg szeretnénk-e tartani néhány postafiókot a helyi Exchange telepítésünkön. Egyszerre az összes felhasználót áttelepítjük, vagy először csak néhányat? Szeretnénk, hogy a felhasználók az Active Directory-beli jelszavukkal léphessenek be a felhő-alapú levelezésükbe is, vagy ott külön jelszavuk lesz?

Meglévő rendszer	Áttelepítendő postaládák száma	Maradnak helyi postaládák?	Támogatott áttelepítési eljárások
Exchange 2010, 2007, 2003	< 1000	Nem	Átállásos Exchange áttelepítés
Exchange 2007 vagy 2003	Nincs korlát	Igen	Szakaszolt vagy hibrid
Exchange 2010	> 1000	Mindegy	Hibrid telepítés
Exchange 2000 és alatta	Nincs korlát	Igen	IMAP alapú
Nem Exchange	Nincs korlát	Igen	IMAP alapú

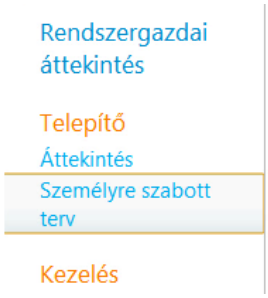
Lehetséges áttelepítési eljárások a meglévő levelezőrendszer típusa alapján

21.3.2 E-mail migráció típusai

- Átállásos (cutover): egyszerre az összes postafiókot felmásolja a felhőbe (a hozzájuk tartozó felhasználókat létrehozza), majd 24 óránként szinkronizálja az új leveleket a helyi szerverrel egészen addig, míg az MX rekordok átállítása meg nem történik, így már az új levelek is a felhőbe érkeznek.
- Szakaszolt (staged): a felhasználók egy részét telepíti át a már AD-szinkronizált felhőbe. Az áttelepítendő felhasználókat a felhőben postaládákká konvertálja, majd a meglévő helyi postaládát szinkronizálja a felhőalapúval. A felhasználónak e-mailtovábbítást állít be a felhőalapú postaládára címezve, további szinkronizáció nem történik.
- Hibrid telepítés: a helyi Exchange kiszolgáló is megmarad és működik. A postaládák egy része helyben maradhat, miközben a másik része a felhőben van. A globális címlista, az elérhetőségi információk, a keresés a postaláda helyétől függetlenül működik, a felhasználó számára teljesen transzparens módon.
- IMAP áttelepítés: bármilyen, IMAP kompatibilis levelezőrendszerből áttelepíthetők a postafiókok. Az első szinkronizáció után 24 óránként minden postafiók ismét szinkronizálva lesz, egészen az MX rekordok átállításáig.

21.3.3 Személyre szabott telepítési terv

Hogy a fenti telepítési módok közül melyik a legcélravezetőbb a konkrét helyzetben, illetve, hogy az egyes lépéseket milyen sorrendben kell végrehajtanunk, ebben segít a *Személyre szabott terv* varázsló.



A személyre szabott tervet a menüből érhetjük el

A varázslót az adminisztrációs felület *Személyre szabott terv* menüpontjából érhetjük el. Első lépésben ki kell választanunk, hogy *Próba* vagy *Központi telepítés* típusú tervet készítünk. A kettő között a legfőbb különbség az, hogy míg a *Próba terv* olyan megoldást ajánl, amihez a meglévő, helyi rendszereinket a lehető legkisebb mértékben kell módosítani (ahogy a neve is jelzi, előbb kipróbálhatjuk a rendszert), addig a *Központi telepítés* típusú terv célja, hogy miután a kipróbálás már megtörtént, tényleges átállást hajtsunk végre.

Válasszuk ki tehát a céljainknak megfelelő típusú tervet, és kattintsunk a *Tovább* gombra. A következő lapon válasszuk ki, mely szolgáltatásokat szeretnénk beállítani, majd kattintsunk ismét a *Tovább* gombra. Ha bejelöltük, hogy szeretnénk használni a levelező szolgáltatást, akkor a következő lapon meg kell adnunk, hogy milyen a jelenlegi levelezőrendszerünk.

Ezután varázsló felajánlja az előzőekben megadott konfiguráció támogatott áttelepítési lehetőségeit. Itt kell majd eldöntenünk, hogy szeretnénk-e meghagyni helyi postafiókokat is, hogy szinkronizáljuk-e az Active Directoryt, és hogy a jelszavakat hol tároljuk.

Egy utolsó összefoglaló lap után, a *Befejezés* gombra kattintva megnézhetjük a végleges tervet.

A telepítési folyamat ettől a ponttól kezdve jelentősen függ a tervben meghatározott céloktól, és a meglévő levelezőrendszer adottságaitól. A fejezet hátralévő részében bemutatjuk az egyes telepítési lépéseket, de ezek közül telepítési környezettől függően nem mindegyiket szükséges végrehajtani, és a sorrend is változó lehet.

A pontos lépéseket és sorrendet az előbbiekben létrehozott Személyre Szabott Terv határozza meg.

21.4 Az egyszeri bejelentkezés beállítása

Az egyszeri bejelentkezési szolgáltatás beállításával elérhető, hogy a felhőbeli felhasználók a helyi Active Directory-beli jelszavukkal tudjanak bejelentkezni az Office 365 szolgáltatásaiba. Megfelelő konfigurációval az is elérhető, hogy a tartományi felhasználóknak (a szolgáltatás nevével összhangban) valóban csak egyszer, a Windowsba való belépés alkalmával kelljen megadni a jelszavukat, a továbbiakban a bejelentkeztetés automatikus legyen.

(https://portal.microsoftonline.com/IdentityFederation/IdentityFederation.aspx)

21.4.1 A szolgáltatás felépítése, előkövetelményei

A szolgáltatás két fő részből áll: telepítenünk kell egyrészt az Active Directory Federation Services 2.0 szervert (továbbiakban: ADFS) és az ADFS 2.0 proxy-t. Az előbbihez fognak kapcsolódni a tartományi kliensek, amelyek NTLM hitelesítéssel jelentkeznek be a szolgáltatásba, ami nem igényel felhasználói beavatkozást – teljesen automatikus. Az utóbbihoz pedig az interneten keresztül kapcsolódnak majd a távoli kliensek, ezért itt űrlap alapú hitelesítés lesz beállítva.

Ahhoz, hogy a fenti működés megvalósuljon, ugyanannak az összevonási szolgáltatás URL címnek tartományon belülről az ADFS szerverre, tartományon kívülről pedig az ADFS proxy szerverre kell majd mutatnia.

Mivel a hitelesítés minden esetben SSL-titkosított kapcsolaton keresztül kell, hogy történjen, a szolgáltatáshoz ajánlott külső, nyilvános tanúsítványszolgáltató által aláírt tanúsítvány használata. Egy ingyenes tanúsítványszolgáltatót bemutatunk a 21.14-es fejezetben.

Opcionálisan, ha lehetőség van rá, akkor érdemes mindkét szerepkört hálózati terheléselosztó fürtbe szervezni, mivel ha a szolgáltatás valamilyen okból nem érhető el, akkor az egyébként tökéletesen üzemelő felhőalapú levelezőrendszerbe se fognak tudni bejelentkezni a felhasználók. Ez azonban túlmutat ennek a fejezetnek a keretein.

21.4.2 Alternatív UPN-utótag hozzáadása

Erre a lépésre akkor van szükség, ha a levelezési domain nevünk (msiskola.hu) nem egyezik meg az Active Directory tartományunk alapértelmezett UPN-utótagával. A UPN (User Principal Name, magyar Windowsban: egyszerű felhasználónév) a felhasználónevet és a tartományt a következő formában adja meg: felhasznalonev@utotag

A példánkban a tartomány alapértelmezett UPN-utótagja *msiskola.local*, ami nem egyezik meg az Office 365-be felvitt domain nevünkkel (msiskola.hu). Ha ez így marad, az problémákat okozhat a bejelentkezésnél.

Ezt megelőzhetjük, ha a helyi Active Directory tartományunkhoz hozzáadjuk alternatív UPN-utótagként az Office 365-ben használt domain nevünket, és a felhasználóknál átállítjuk az utótagot erre.

1) Az egyik tartományvezérlőn nyissuk meg az Active Directory - tartományok és megbízhatósági kapcsolatok eszközt a Felügyeleti eszközök közül.
2) A megnyíló ablakban kattintsunk jobb gombbal az *Active Directory - tartományok és megbízhatósági kapcsolatok* elemre, és válasszuk a *Tulajdonságokat* a helyi menüből.
3) Az *Alternatív UPN-utótagok* mezőbe írjuk be az Office 365-ben használt domain nevünket – pl. msiskola.hu –, majd kattintsunk a *Hozzáadás* gombra.
4) A felhasználóknál át kell állítanunk az utótagot a most hozzáadott alternatív értékre. Ezt megtehetjük egyesével az *Active Directory – felhasználók és számítógépek* eszközzel, ha az adott felhasználó *Tulajdonságai* között a *Fiók* fülön a *Bejelentkezési név* mező mellett a legördülő listából kiválasztjuk a most hozzáadott értéket. Ez a megoldás azonban sok felhasználónál igencsak időigényes volna.

5) A másik megoldás a PowerShell használata. Ehhez a következő parancsot használhatjuk a könyv ezzel foglalkozó fejezetében ismertetett módon:

```
$regiUtotag = 'msiskola.local'           # a mostani utótag
$ujUtotag = 'msiskola.hu'                # az új, alternatív utótag
$dcCN = 'ou=Minta,dc=msiskola,dc=local'  # hol keresse a felhasználókat?
$tartomanyvezerlo = 'dc'                 # a tartományvezérlő neve

Get-ADUser -SearchBase $dcCN –SearchScope subtree -filter * | ForEach-
        Object {
    $ujUPN = $_.UserPrincipalName.Replace($regiUtotag,$ujUtotag)
    $_ | Set-ADUser -server $tartomanyvezerlo -UserPrincipalName $ujUPN
}
```

A fenti kódban az első 4 sort kell testre szabnunk. Az első két változó értékeként az aposztrófok közé be kell írnunk a jelenlegi és a most létrehozott alternatív UPN-utótagokat. A harmadik változó azt az objektumot határozza meg, amiben keresi a felhasználókat a szkript. Azaz jelen beállítások szerint a Minta nevű szervezeti egységben (OU) keres, az msiskola.local tartományban.

Ha az egész tartományban szeretnénk a keresést végezni, elhagyhatjuk az ou=Minta feltételt: $dcCN = 'dc=msiskola,dc=local'

Az utolsó változóba pedig a tartományvezérlő nevét kell írnunk.

21.4.3 Az ADFS 2.0 szerver telepítése

A példában a következő konfigurációt használjuk:

Levelezési domain név: msiskola.hu

ADFS szolgáltatás címe: fs.msiskola.hu

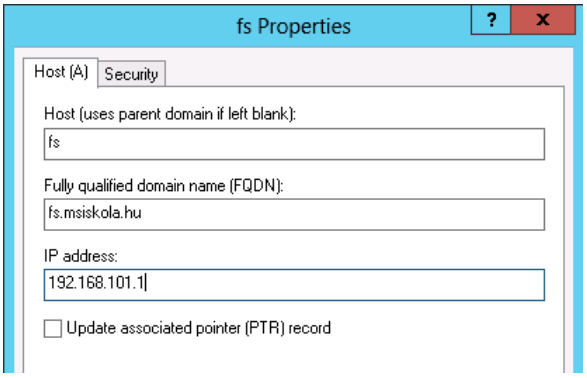
ADFS szerver (és tartományvezérlő): dc.msiskola.local, 192.168.101.1

ADFS proxy: proxy.msiskola.local, 192.168.101.2

1) Első lépésben a belső, tehát az AD tartomány által használt DNS szerverekbe kell felvinni az ADFS szolgáltatás címét, mégpedig úgy, hogy az az ADFS szerver belső IP címére mutasson. Ha az ADFS szolgáltatást fürtbe szerveztük, akkor természetesen a fürt IP címére kell mutatnia.

   Ehhez nyissuk meg a DNS beépülő modult a szerveren. Ha még nincs a kezelt zónák között az msiskola.hu, akkor kattintsunk a szerver nevére (DC) jobb gombbal, és válasszuk az Új zóna lehetőséget. A zóna típusa legyen Elsődleges, a replikáció céljaként hagyjuk meg az alapértelmezett tartományi DNS szerverek lehetőséget. A zóna típusa legyen Címkeresési zóna, a zóna neve pedig legyen a külső, levelezéshez használandó domain nevünk, a példa szerint msiskola.hu, majd kattintsunk a Befejezés gombra.

Ezután az újonnan létrehozott zóna nevére kattintsunk jobb gombbal, és válasszuk az *Új állomást* (A vagy AAAA) lehetőséget. A név mezőbe írjuk, hogy *fs*, az IP cím mezőbe pedig a szerver vagy fürt IP címét (192.168.101.1).



A belső DNS szerverek beállításai

2) Importáljuk az előbb létrehozott DNS rekordhoz tartozó tanúsítványt. A példában: fs.msiskola.hu
3) Ha Windows Server 2008 rendszerre (nem R2-re) telepítünk, akkor kezdés előtt telepítsük fel a *Webkiszolgáló (IIS)* szerepkört az alapértelmezett szerepkör-szolgáltatásokkal, és a *.NET keretrendszer 3.5-ös verziója* nevű szolgáltatást.
4) Hozzunk létre egy új felhasználói fiókot a tartományban, amit a szolgáltatás fog használni. Pl. `MSISKOLA\fs`
5) Töltsük le az ADFS 2.0 telepítőt, és a hozzá tartozó Update Rollup 2 frissítést:

   ADFS 2.0: http://www.microsoft.com/hu-hu/download/details.aspx?id=10909

   Update Rollup 2: http://support.microsoft.com/kb/2681584 (a letöltési linket e-mailben küldik)

   Megjegyzés: e könyv írásának idején a Windows Server 2012 Release Candidate állapotban van, ezért még nem készülhetett hozzá ADFS telepítő. A linkeken a Windows Server 2008 R2-es verziójához készült telepítők találhatók.
6) Telepítsük fel az ADFS 2.0 kiszolgálót. Ehhez indítsuk el az *AdfsSetup.exe*-t, majd a licencszerződés elfogadása után válasszuk ki az *Összevonási kiszolgáló* lehetőséget. A *Következő* gombra kattintva elindul a telepítés. A befejező képernyőn vegyük ki a pipát az *Induljon ez az ADFS 2.0 kezelő beépülő modulja a varázsló bezárása után* elől, majd zárjuk be a varázslót.

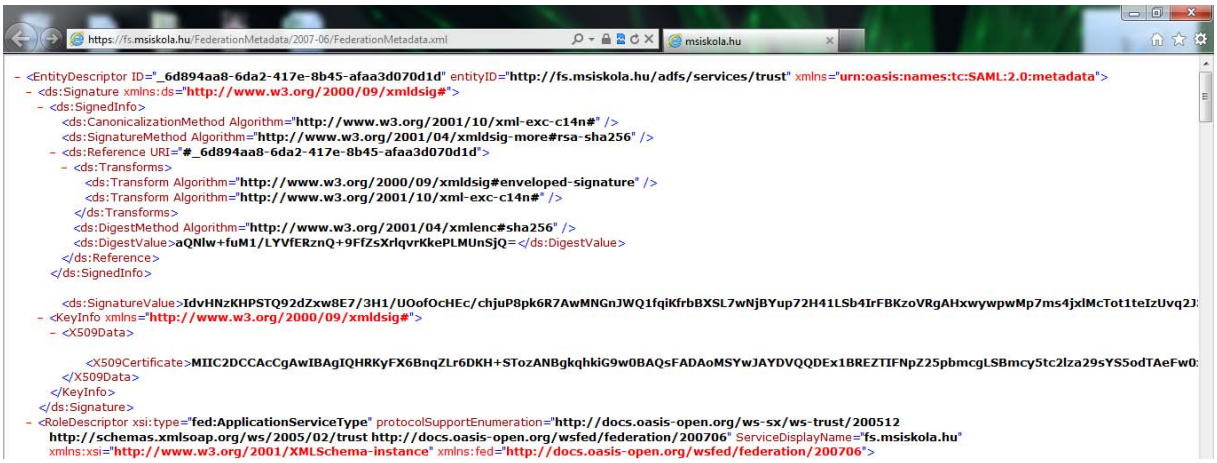
   Ezután telepítsük fel az Update Rollup 2 csomagot.
7) Indítsuk el az ADFS 2.0 kezelőt a *Start menü / Felügyeleti eszközök* alól. A főképernyőn kattintsunk az ADFS 2.0 összevonási kiszolgáló konfigurálása varázsló linkre. Az első lapon válasszuk az *Új összevonási kiszolgáló-farm* létrehozása pontot, majd kattintsunk a *Következő* gombra. A *Telepítéstípus* kiválasztása lapon válasszuk az *Új összevonási kiszolgáló-farm* pontot, majd kattintsunk a *Következő* gombra.

Az Összevonási szolgáltatás neve lapon megjelennek a telepített és érvényes tanúsítványok. Válasszuk ki a korábban importált fs.msiskola.hu-hoz tartozó tanúsítványt. A varázsló a tanúsítvány alapján rögtön kitölti az *Összevonási szoláltatás* neve mezőt is. Kattintsunk a *Következő* gombra.

A Szolgáltatásfiók megadása lapon ki kell választanunk a korábban létrehozott tartományi szolgáltatásfiókot, és meg kell adnunk a hozzá tartozó jelszót. A *Következő* gombra kattintva egy összegzést kapunk a műveletekről, amit a *Következő* gombra tett ismételt kattintással el is kezd a varázsló.

Ha minden pipa zöld, a *Bezárás*ra kattintva befejezhetjük a varázslót.

Ha eddig mindent jól csináltunk, akkor belső hálózatról megnyitva a https://fs.msiskola.hu/FederationMetadata/2007-06/FederationMetadata.xml címen egy XML formátumú fájlt találunk.



Ehhez hasonló képet kell látnunk a fenti URL-t megnyitva

21.4.4 Az ADFS 2.0 proxy telepítése

Most, hogy az ADFS szerver már lényegében működik, megtehetnénk, hogy a szervert közvetlenül kipublikáljuk az internetre. Lényegi probléma tulajdonképpen nem is lenne vele, hacsak az nem, hogy az internetes klienseknek is az NTLM hitelesítést használva kellene bejelentkezniük. Ez azon túl, hogy megjelenésre nem valami elegáns, azért is probléma, mert ennél a hitelesítési formánál a felhasználónév mezőbe nem elég magát a felhasználónevet írni, mindenképpen jelezni kell a tartományt is. Tehát ha *holczerj* felhasználó be szeretne jelentkezni, akkor a *Felhasználónév* mezőbe vagy *MSISKOLA\holczerj -t* vagy *holczerj@msiskola.local* –t kell írnia. Ez pedig jó eséllyel állandó hibaok lesz a felhasználók körében.

A proxy szerver telepítésével kiküszöbölhető ez a probléma, mert itt gond nélkül beállíthatunk webes űrlap alapú hitelesítést, amit egyrészt tetszőleges mértékben testre tudunk szabni, másrészt sokkal felhasználóbarátabb.

1) Először is ahhoz, hogy a proxykiszolgálón a névfeloldás megfelelően működjön, az ADFS szolgáltatás címét be kell jegyeznünk a proxykiszolgáló ún. `hosts` fájljába.

   Indítsunk rendszergazdaként egy *Jegyzettömb*öt, majd a *Megnyitás* ablakban navigáljunk el a `C:\Windows\system32\drivers\etc\` mappába. A *Megnyitás* dialógusablakban a fájltípus legördülő menüben válasszuk a *Szöveges dokumentumok* helyett a *Minden fájl* lehetőséget, hogy megjelenjenek a mappában található fájlok. Nyissuk meg a `hosts` nevű fájlt.

   A fájl végéhez, egy új sorban fűzzük hozzá a következő sort, természetesen a saját értékeinkkel:

   ```
   192.168.101.1 fs.msiskola.hu
   ```

   Ahol az IP cím helyére írjuk a saját ADFS szerverünk, vagy fürtünk IP címét, a cím helyére pedig a saját ADFS szolgáltatásnevünket.

2) Ha Windows Server 2008 rendszerre (nem R2-re) telepítünk, akkor kezdés előtt telepítsük fel a *Webkiszolgáló (IIS)* szerepkört az alapértelmezett szerepkör-szolgáltatásokkal, és a *.NET keretrendszer 3.5-ös verziója* nevű szolgáltatást.

3) Az ADFS szerver telepítéséhez használt telepítőt indítsuk el ezen a gépen is, azonban most a licenc elfogadása után az *Összevonási proxykiszolgáló* lehetőséget válasszuk.

   A *Következő* gombra kattintva elkezdődik a telepítés.

   A befejező képernyőn vegyük ki a pipát az *Induljon ez az ADFS 2.0 kezelő beépülő modulja a varázsló bezárása után* opció elől, majd zárjuk be a varázslót.

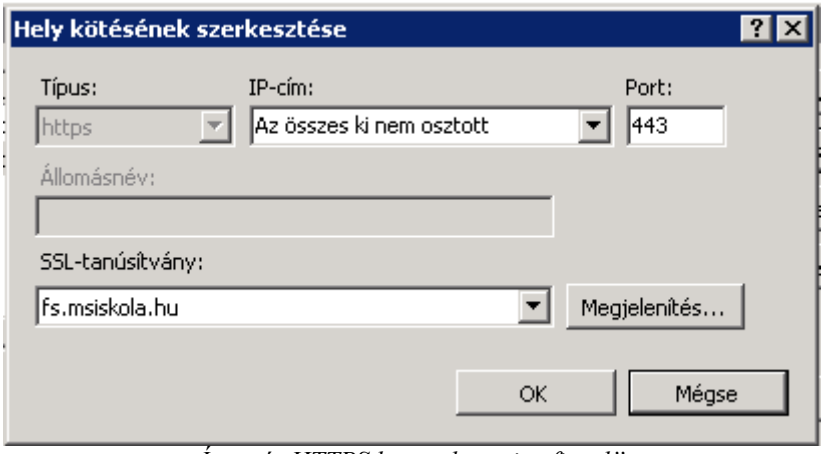
4) Az ADFS szerver telepítéséhez használt Windows Update frissítőfájlt futtassuk le ezen a gépen is az Update Rollup 2 telepítéséhez.

5) Az ADFS szerveren meglévő *fs.msiskola.hu* tanúsítványt importáljuk erre a szerverre is. Ezt legegyszerűbben az IIS management konzolon tudjuk megtenni. Kattintsunk a szerver nevére, és válasszuk ki a *Kiszolgálói Tanúsítványok* ikont. A jobb oldali panelen válasszuk az *Importálás* linket, tallózzuk a fájlt, és írjuk be a hozzá tartozó jelszót.

6) Állítsuk be, hogy az alapértelmezett weboldal HTTPS kapcsolatokat is fogadjon.

   Ehhez továbbra is az IIS konzolon nyissuk le a szerver nevét, majd azon belül a *Helyek* menüt. Kattintsunk jobb gombbal a *Default Web Site* elemre, és válasszuk a *Kötések szerkesztése* lehetőséget. A megnyíló ablakban kattintsunk a *Hozzáadás* gombra.

   A *Hely kötésének hozzáadása* ablakban a típusnál válasszuk a *https*-t, az *SSL tanúsítvány*nál pedig az előző pontban importált tanúsítványunkat. Kattintsunk az *Ok*, majd a *Bezárás* gombra.



Így már HTTPS kapcsolaton is „figyel”

7) Indítsuk el a Start menüből az ADFS 2.0 proxy kiszolgáló konfigurációs varázslóját.

   Az üdvözlőképernyőn kattintsunk a *Következő* gombra. Az *Összevonási szolgáltatás neve* lapon ellenőrizzük, hogy az alapértelmezett név azonos-e a mienkkel. Ha igen, kattintsunk a *Következő* gombra. A felugró azonosító ablakba írjuk be a tartományi rendszergazdai adatainkat, ezt fogja használni a varázsló az ADFS szerver és a proxy összerendeléséhez.

8) Állítsuk be, hogy a proxy szerver űrlap alapú azonosítást használjon.

   Ehhez az IIS menedzsment konzolon nyissuk le a *Default Web Site* elemet a bal oldali navigációs panelen. Keressük meg az *adfs* elemet, nyissuk le, majd kattintsunk az *ls* elemre. Miközben az *ls* elem van kiválasztva, kattintsunk a *Hitelesítés* ikonra. Tiltsuk le a *Windows hitelesítés*t, és engedélyezzük helyette az *Űrlapos hitelesítés*t.

21.4.5 Az ADFS 2.0 proxy publikálása az internet felé

Most, hogy az ADFS 2.0 proxykiszolgálónk is üzemkész, nincs más dolgunk, mint kipublikálni azt az internet felé.

1) A domain nevünk (msiskola.hu) fenntartójánál kérnünk kell, hogy hozzon létre egy új DNS rekordot `fs.msiskola.hu` néven, aminek arra a külső, interneten is elérhető IP címre kell mutatnia, amelyre most az ADFS szolgáltatást ki fogjuk publikálni.

   Amennyiben a domain nevet mi tartjuk fenn, ezt magunk is megtehetjük.

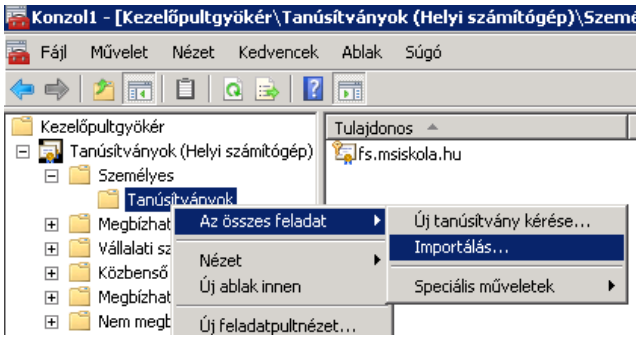
   Ha rendelkezünk tűzfallal, akkor azon is ki kell engednünk az ADFS weboldalt. Ennek mikéntje tűzfal szoftverenként eltérő lehet, általánosságban azonban elmondható, hogy egy egyszerű weboldalhoz hasonló módon kell eljárnunk (amely azonban minden esetben HTTPS protokollt használ), ahol a weboldal külső neve `fs.msiskola.hu`, a belső szerver pedig az ADFS proxy szerverünk címe, vagy ha fürtbe szerveztük a proxykiszolgálókat, akkor a fürt IP címe.

   Az alábbiakban a *Microsoft Forefront Threat Management Gateway* szoftverén részletesen is ismertetjük a szükséges lépéseket, mivel itt néhány specifikus lépésre is szükség van a helyes működéshez.

2) Importáljuk az fs.msiskola.hu címhez tartozó SSL tanúsítványunkat erre a gépre is.

   Ehhez a Windows és az R gombok lenyomása után megjelenő ablakba írjuk be: `mmc`, majd a megjelenő ablakban kattintsunk a *Fájl*, *Beépülő modul hozzáadása/eltávolítása* elemre. A bal oldali listából válasszuk a *Tanúsítványok* elemet, és kattintsunk a *Hozzáadás* gombra. A felugró ablakban válasszuk a *Számítógépfiók* lehetőséget, a következő lapon pedig a *Helyi számítógép*et. Végül kattintsunk a *Befejezés*, majd az *OK* gombra.

   Nyissuk le a bal oldali navigációs fát a *Tanúsítványok/Személyes/Tanúsítványo*k elemig. Kattintsunk erre az elemre jobb gombbal, és a helyi menüben válasszuk az *Összes feladat/Importálást*. Ebben a varázslóban tallózzuk a tanúsítvány privát kulccsal együtt exportált példányát, adjuk meg a hozzá tartozó jelszót, majd kattintsunk a *Befejezés* gombra.



A tanúsítvány importálása – fontos, hogy a helyi számítógép fiókjába importáljunk

3) Indítsuk el a *Forefront TMG* menedzsment konzolt. A *Tasks* oldalpanelen válasszuk a *Publish Web Sites* linket.
4) A megjelenő varázslóban nevezzük el az új szabályt, például „ADFS proxy publikálás”.
5) A következő három képernyőn fogadjuk el az alapbeállításokat, és kattintsunk a *Next* gombra.
6) Az *Internal Site Name* mezőbe írjuk be az ADFS szolgáltatás nevét, pl. `fs.msiskola.hu`, a *Computer Name or IP address* mezőbe pedig írjuk be az ADFS proxy szerver vagy fürt IP címét.
7) A következő lapon a *Path* mezőbe írjuk a következőt: `/*`

   A „Forward the original host header…” előtti pipát jelöljük be.
8) A *Public Name Details* lapon a *Public name* mezőbe írjuk be ismét az ADFS szolgáltatásunk címét: fs.msiskola.hu, majd lépjünk tovább.

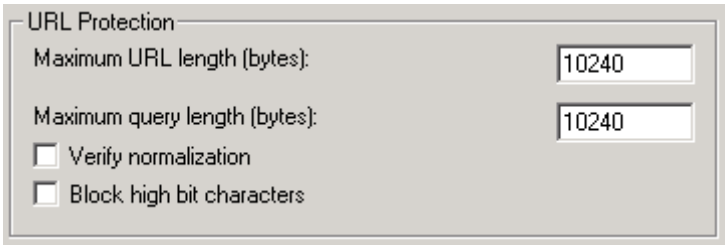
9) Létre kell hoznunk egy *Web listener*t. Ehhez kattintsunk a *New* gombra. Adjunk neki egy nevet, pl. `fs.msiskola.hu`, majd lépjünk tovább. Hagyjuk kiválasztva a *Require SSL* lehetőséget. A következő lapon pipáljuk ki az *External* melletti pipát. A *Select IP addresses* gombbal kiválaszthatjuk, melyik IP címen fogjuk fogadni a kapcsolatokat ezzel a listenerrel. Ennek akkor van gyakorlati jelentősége, ha több külső IP címünk is van.

   A következő lapon válasszuk a *Use a single certificate* lehetőséget, a *Select Certificate* gombra kattintva pedig válasszuk ki az első lépésben importált tanúsítványunkat, amely az fs.msiskola.hu címre szól, majd lépjünk a következő lapra.

   A legördülő menüből válasszuk a *No Authentication* lehetőséget, és lépjünk tovább, majd fejezzük be a varázslót.

   Visszatérve az előző varázslóra, válasszuk ki a most létrehozott *Web Listener*t a listából, és lépjünk a következő lapra.

10) Az Authentication Delegation lapon válasszuk a No delegation, but client may authenticate directly lehetőséget, majd lépjünk tovább.
11) A *Users* lapon hagyjuk meg az alapértelmezett *All Users* értéket, majd fejezzük be a varázslót.
12) Nyissuk meg a frissen létrehozott szabályt, lépjünk a *Link translation* fülre, majd vegyük ki a pipát az *Apply link translation to this rule* elől.
13) Még mindig a szabály tulajdonságainál lépjünk a *Traffic* fülre, és kattintsunk a *Filtering* gombra, majd a *Configure HTTP* lehetőségre. A megjelenő ablakban vegyük ki a pipákat a *Verify normalization* és a *Block high bit characters* opciók elől.



A helyes beállítás – nincsenek pipák

   Kattintsunk az *OK* gombra mindkét ablakban.

14) Végül alkalmazzuk az elvégzett beállításokat felső sárga csíkban található *Apply* gombra kattintva.

21.4.6 A Microsoft Online Services modul telepítése és konfigurálása

Ha az *Active Directory Federation Services 2.0* telepítve és konfigurálva van, valamint megfelelő módon működik, a következő lépés a domain név (tartomány) összekapcsolása az Office 365 szolgáltatással. Ehhez első lépésben telepítenünk kell a *Microsoft Online Services modul Windows PowerShell környezethez* nevű programot. A telepítő fájlhoz legegyszerűbben a *Személyre szabott terv* varázslóból juthatunk, az *Egyszeri bejelentkezés beállítása* alatti *Indítás most* linkre kattintva.

A modul futtatásához Windows 7, vagy Server 2008 R2 rendszerre van szükség, utóbbin szükséges bekapcsolni a *.NET-keretrendszer 3.5.1* nevű szolgáltatást. Válasszuk ki az operációs rendszerünknek megfelelő telepítő fájlt (32 vagy 64 bit), és kattintsunk a *Letöltés* gombra.

1) Töltsük le, és telepítsük a Microsoft Online Services bejelentkezési segéd (MOS SIA) informatikai szakembereknek nevű programot:
   http://www.microsoft.com/hu-hu/download/details.aspx?id=28177
2) Telepítsük fel a korábbiakban letöltött Microsoft Online Services modul Windows PowerShell környezethez programot.
3) Indítsuk el a programot az asztalon található parancsikonnal. Egy parancssort kell látunk.
4) Írjuk be a következő parancsokat, ebben a sorrendben:
   `$c = Get-Credential`

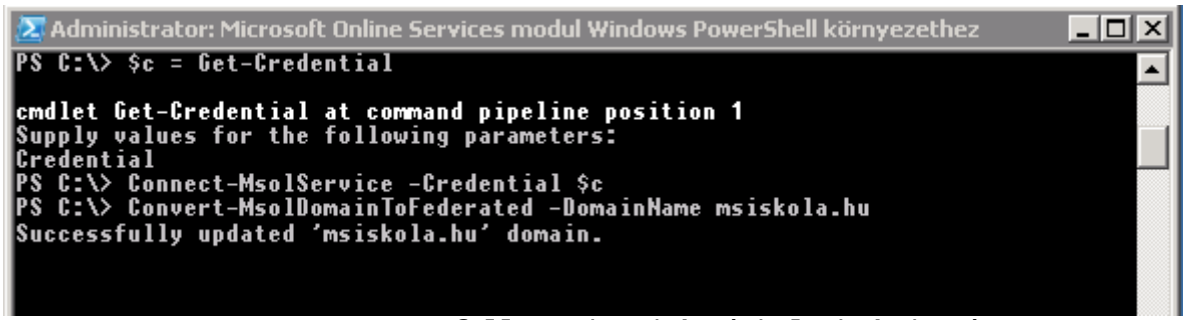
A megjelenő ablakban adjuk meg az Office 365 rendszergazdai felhasználónk azonosítóját és jelszavát! Pl.: *admin@msiskola.onmicrosoft.com*

```
Connect-MsolService -Credential $c
```

Ezzel a paranccsal kapcsolódunk az Office 365 szolgáltatáshoz.

```
Convert-MsolDomainToFederated -DomainName msiskola.hu
```

Ezzel pedig átalakítjuk az *msiskola.hu* domain nevet egyszeri bejelentkezést használó domain névvé.



Ha mindent jól csináltunk, a „`Successfully updated 'msiskola.hu' domain.`” üzenetnek kell megjelennie

Ellenőrizzük a művelet sikerességét az adminisztrációs felületen. Kattintsunk a bal oldali menüben a *Tartományok* linkre, majd a listában az imént átalakított domain nevünkre: *msiskola.hu*

Sikeres átalakítás esetén a *Tartománytípus*nál a „Egyszeri bejelentkezés: A tartomány egyszeri bejelentkezésre van konfigurálva.” szöveget látjuk.

21.5 Címtár-szinkronizáció beállítása

Az egyszeri bejelentkezés szolgáltatás minden valószínűség szerint már működik, de még nincsenek felhasználóink a felhőben, akik be tudnának vele jelentkezni. Ahhoz, hogy a helyi Active Directory felhasználóink megjelenjenek a felhőben is, szinkronizálnunk kell őket. Ehhez a *Microsoft Címtár-szinkronizáló eszköz*t kell telepítenünk.

21.5.1 Rendszerkövetelmények

A Címtár-szinkronizáló eszközt egy olyan szerverre kell telepítenünk, amely:

- Tartományi tag abban a tartományban, amit szinkronizálni szeretnénk
- Nem tartományvezérlő
- Telepítve van rajta a .NET keretrendszer 3.5.1-es verziója
- Operációs rendszer követelmények:
  - 32 bites: Windows Server 2003 vagy Windows Server 2008
  - 64 bites: Windows Server 2008 R2 vagy Windows Server 2008

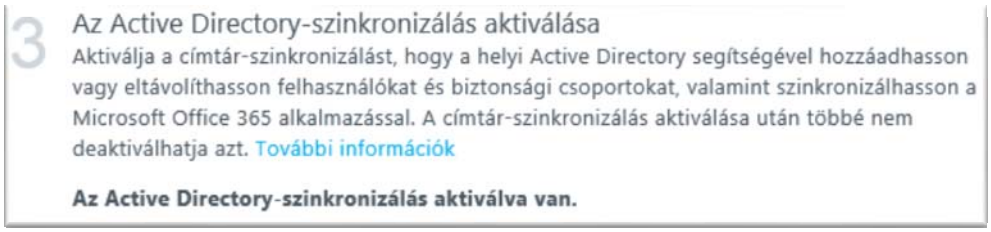
21.5.2 A Címtár-szinkronizáló eszköz telepítése és konfigurálása

1) Van néhány kizáró tényező, ami megakadályozhatja egy adott elem sikeres szinkronizációját. Ezeket szűrhetjük ki a *Microsoft Office 365 Deployment Readiness Tool*lal, amely megvizsgálja az összes AD-elemünket, és egy jelentés formájában részletes és konkrét elemekre mutat rá, amelyek hibát okozhatnak, és egyben javaslatot tesz a megoldásra.

   Az eszköz a következő címről tölthető le: http://community.office365.com/en-us/forums/183/p/2285/8155.aspx

2) Kapcsoljuk be az Active Directory szinkronizációt. Ehhez az adminisztrációs felületen kattintsunk a *Felhasználók* elemre, majd az *Active Directory-szinkronizáció* mellett kattintsunk a *Beállítás* linkre. Keressük meg az *Active Directory-szinkronizálás aktiválása* lépést, és kattintsunk az *Aktiválás* gombra.

   Az aktiválási folyamat akár 24 órát is igénybe vehet.



Ha az aktiválás befejeződött, ez az üzenet jelenik meg

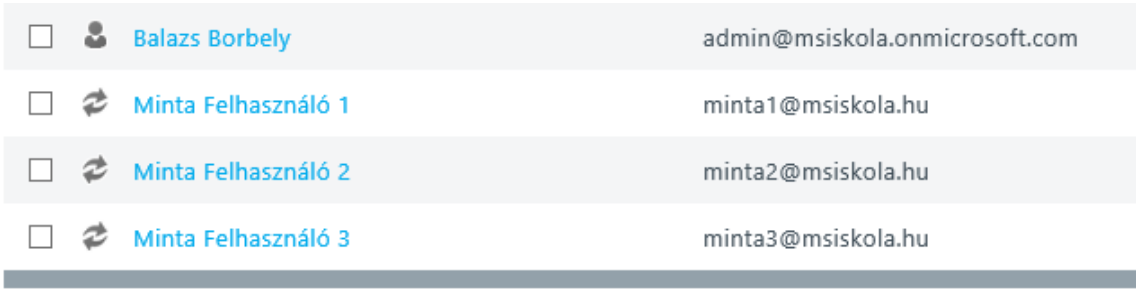
3) Töltsük le a *Címtár-szinkronizáló eszköz*t. A letöltési linket az előző pontban ismertetett oldalon találjuk, az AD szinkronizáció aktiváló gombja alatt.
4) Telepítsük fel a szinkronizáló eszközt egy olyan számítógépre, ami megfelel a fent részletezett rendszerkövetelményeknek.
5) Telepítés után alapértelmezés szerint automatikusan indul a konfigurációs varázsló.
   a) Meg kell adnunk az Office 365 adminisztrátori azonosítónkat és jelszavunkat. Pl.: *admin@msiskola.onmicrosoft.com*

      Ha a Tovább gombra kattintás után hibaüzenetet kapunk, miszerint az Active Directory szinkronizáció nincs engedélyezve a domainünkön, akkor lehetséges, hogy már elindítottuk az aktiválást, de még nem fejeződött be.

   b) A második lapon meg kell adnunk a tartományi adminisztrátori adatainkat. Ennek segítségével fogja a konfigurációs varázsló megadni a szinkronizációs szolgáltatásnak a megfelelő jogosultságokat.
   c) A következő lapon meg kell adnunk, hogy szeretnénk-e Exchange Hibrid konfigurációt beállítani a későbbiekben. Ha igen, akkor a varázsló írási jogosultságokat is be fog állítani magának az Active Directoryban, ellenkező esetben csak olvasási jogosultságokat fog kapni.

d) Végül rövid várakozás után alapértelmezés szerint azonnal elindul a szinkronizáció. A folyamatot az eseménynaplóból követhetjük, hiba esetén pedig e-mailt fogunk kapni a felhőbeli adminisztrátori fiókunkba.

6) Ellenőrizzük a szinkronizáció eredményeit. A szinkronizálandó elemek számától függően néhány percen belül az adminisztrációs felület Felhasználók menüpontjának el kell kezdenie feltöltődni az AD-beli felhasználóinkkal.



A nevek melletti ikonok is jelzik, hogy az utolsó három felhasználó szinkronizálva van

Türelmetlenebbek a Windows eseménynaplójában részletesen láthatják a szinkronizáció lépéseit azon a gépen, amelyre a Címtár-szinkronizáló eszközt telepítettük.

A kezdeti szinkronizáció után 3 óránként inkrementális szinkronizáció történik, amikor csak a változásokat szinkronizálja a program. Ha a későbbiekben „kézzel” szeretnénk szinkronizációt indítani, akkor látogassunk el a *C:\Program Files\Microsoft Online Directory Sync* mappába, ahol találunk egy *DirSyncConfigShell.psc1* nevű fájlt. Ezt elindítva egy konfigurációs konzol nyílik meg, ahol a `Start-OnlineCoexistenceSync` parancs kiadásával azonnal szinkronizációt indíthatunk.

Ehhez a fájlhoz érdemes egy parancsikont is létrehozni az Asztalra, mivel a szinkronizációs hibák elhárítása során ez egy sűrűn használt parancs lehet.

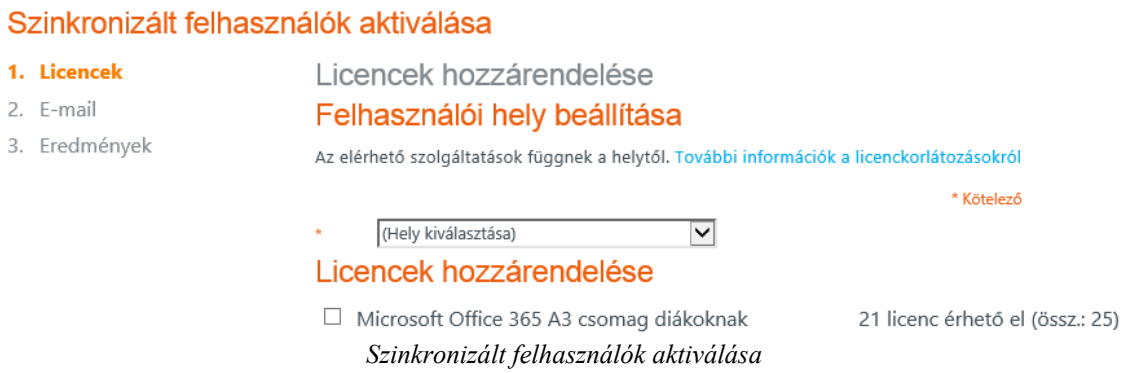
21.6 Szinkronizált felhasználók aktiválása

Az Office 365 szolgáltatásban az Active Directoryból szinkronizált felhasználókat aktiválni kell. Aktiválás alatt a szolgáltatás igénybevételi helyének megadását és a megfelelő licenc hozzárendelését értjük. Ezt a folyamatot elvégezhetjük a webes adminisztrációs felületről és PowerShellből is.

21.6.1 Aktiválás a webes felületről

Ezt a módszert akkor válasszuk, ha kevés felhasználót kell aktiválnunk, vagy ha a legtöbb felhasználónak ugyanazt a helyet és licenckonstrukciót kell beállítanunk.

1) Az adminisztrációs felületen kattintsunk a *Felhasználók* elemre. A felhasználólistában, a sor elején található jelölőnégyzetek segítségével válasszuk ki azokat a felhasználókat, akikre az adott beállításokat alkalmazni szeretnénk. Ha az aktuális oldalon az összes felhasználót ki szeretnénk jelölni, kattintsunk a táblázat címsorában lévő jelölőnégyzetre.
2) Kattintsunk a táblázat fölötti *Szinkronizált felhasználók aktiválása* linkre.
3) A *Hely kiválasztása* legördülő menüből válasszuk ki azt az országot, ahol a felhasználó a szolgáltatást igénybe fogja venni.



Szinkronizált felhasználók aktiválása

4) Alatta láthatjuk az elérhető licenceket. Kiválaszthatunk egy egész szolgáltatáscsomagot (pl. Microsoft Office 365 A3 csomag diákoknak), vagy csak bizonyos szolgáltatásokat (pl. Lync Online + Exchange Online).
5) A *Tovább* gombra való kattintás után megadhatunk egy e-mail címet, amire az aktiválás végén egy összesítő levelet fog küldeni a rendszer. Ez elsősorban akkor fontos, ha úgy konfiguráljuk a szolgáltatást, hogy a felhasználóknak az Office 365-höz külön jelszavuk lesz, mivel ebben az esetben a jelszavakat most fogja generálni a rendszer, és ez célszerű, ha e-mailben is megvan.
6) Az *Aktiválás* gombra kattintva a rendszer elvégzi a kért beállításokat a kijelölt felhasználókon. A folyamat végén megjelennek a műveletek eredményei.

21.6.2 Aktiválás PowerShell segítségével

Előfordulhat olyan helyzet, amikor a webes felületen csak nagyon nehezen oldható meg a megfelelő licencek kiosztása. A közoktatási Office 365-ben például háromféle licenc van: tanároknak és dolgozóknak, diákoknak, valamint öregdiákoknak.

Már a tanárok felhasználóit kijelölni is kihívás értékű lehet a webes felületen, hiszen adott esetben több száz diák között „bújhatnak meg" a tanárok. De az öregdiákokat szinte lehetetlen összegyűjteni a listából, míg eközben az Active Directoryban szerencsés esetben minden felhasználó szervezeti egységekbe vagy csoportokba van rendezve. Szerencsére ilyen esetekben használhatunk PowerShellt a felhasználók aktiválásához.

Először is le kell kérdeznünk, hogy milyen licenceink vannak, és ezeknek mi a rendszerben az azonosítójuk. Ehhez indítsuk el a *Microsoft Online Services modul Windows PowerShell környezethez* konzolt, amit az egyszeri bejelentkezés beállításakor telepítettünk. A konzolon írjuk be a következő parancsokat:

```
Import-Module ActiveDirectory
```

Ezzel importáljuk a konzolba az AD menedzseléséhez szükséges parancsokat.

```
Connect-MsolService -Credential $c
```

A megjelenő ablakban adjuk meg az Office 365-beli adminisztrátori adatainkat, pl.: *admin@msiskola.onmicrosoft.com*

```
Get-MsolAccountSku
```

Ez a parancs lekérdezi az elérhető licenccsomagokat, és ehhez hasonló kimenetet ad:

```
AccountSkuId                        ActiveUnits     WarningUnits     ConsumedUnits
msiskola:ENTERPRISEPACK_STUDENT          25              0                4
msiskola:ENTERPRISEPACK_FACULTY          25              0                0
msiskola:STANDARDWOFFPACK_FACULTY        10              0                0
msiskola:STANDARDWOFFPACK_STUDENT        10              0                0
```

Az első két sor az A3 szintű próbalicenceket jelzi, a második kettő pedig utólag igényelt A2 szintű közoktatási csomag.

Név	Érvényes	Lejárt	Kiosztott
Microsoft Office 365 A2 csomag diákoknak	10	0	0
Microsoft Office 365 A2 csomag testületeknek	10	0	0
Microsoft Office 365 A3 csomag diákoknak	25	0	4
Microsoft Office 365 A3 csomag testületeknek	25	0	0

A webes felület segíthet megfejteni a kódok jelentését

Ha egy AD-beli csoport tagjaira szeretnénk alkalmazni egy beállítást, akkor a következő szkriptet futtassuk:

```
$csoport = '2006d' # az AD-beli csoport neve
$licenc='msiskola:STANDARDWOFFPACK_STUDENT' # a hozzárendelendő licenc neve
Get-ADGroupMember -Identity $csoport | Get-ADUser | ForEach-Object {
    $_ | Set-MsolUser -UsageLocation HU  # felhasználás helye Magyarország
    $_ | Set-MsolUserLicense -UserPrincipalName $_.UserPrincipalName
         -AddLicenses $licenc  # licenc hozzárendelése
}
```

Ha az Active Directoryban nem csoportokban, hanem szervezeti egységekben (OU) vannak a felhasználóink, akkor ez a szkript fog segíteni:

```
$keresesHelye = 'ou=Minta,dc=msiskola,dc=local'  # a keresendő OU
$licenc = 'msiskola:STANDARDWOFFPACK_STUDENT'    # a hozzárendelendő licenc
Get-ADUser -SearchBase $keresesHelye -filter * | ForEach-Object {
    $_ | Set-MsolUser -UsageLocation HU  # felhasználás helye Magyarország
    $_ | Set-MsolUserLicense -UserPrincipalName $_.UserPrincipalName
         -AddLicenses $licenc  # licenc hozzárendelése
}
```

21.7 Hibrid e-mail konfiguráció

Hibrid Exchange telepítés esetén a jelenleg már létező Exchange telepítésünk is megmarad az Office 365 felhőalapú szolgáltatás mellett. A postaládák egy része így helyben maradhat, miközben a másik részük a felhőben van. A globális címlista, az elérhetőségi információk, a keresés a postaláda helyétől függetlenül működik, a felhasználó számára teljesen transzparens módon.

21.7.1 Rendszerkövetelmények

A hibrid Exchange konfiguráció kínálja a migrációs típusok közül a legszélesebb körű funkcionalitást, ugyanakkor ezek eléréséhez teljesülniük kell bizonyos rendszerkövetelményeknek:

- Exchange 2010 Service Pack 2 szerver, melyre telepítve van az Update Rollup 3 csomag
- Lennie kell legalább egy írható Windows Server 2003 SP1 vagy újabb rendszerű tartományvezérlőnek
- Az AD erdő működési szintjének legalább Windows Server 2003-asnak kell lennie
- Címtár-szinkronizáló működik (lásd korábban)
- Egyszeri bejelentkezés szolgáltatás működik (ADFS 2.0, lásd korábban)
- Külső tanúsítványok a webes és SMTP címekhez

A következő példában feltételezzük, hogy van egy működő, a fenti rendszerkövetelményeknek megfelelő Exchange levelezőrendszer, mely az alábbi címeken érhető el:

Outlook Web App: mail.msiskola.hu

SMTP: smtp.msiskola.hu

Feltételezzük továbbá, hogy mindkét címhez és szolgáltatáshoz be van állítva a megfelelő, külső tanúsítványszolgáltatótól származó tanúsítvány. Amennyiben nincs, a 21.14-es fejezetben bemutatunk egy ingyenes tanúsítványszolgáltatót, amivel ez megoldható.

21.7.2 Előkészületek

1) Első lépésben, a korábbiakban már ismertetett módon be kell állítanunk két DNS rekordot, vagy meg kell kérnünk a domain nevünk fenntartóját, hogy állítsa be nekünk. Természetesen ezekre csak akkor van szükség, ha még nincs konfigurálva az adott szolgáltatás az Exchange környezetünkben.

   Az első az autodiscover.msiskola.hu. Ennek a rekordnak annak az Exchange szervernek a külső IP címére kell mutatnia, amelyik a Client Access szerepkört birtokolja. Erre a címre az Outlook Autodiscover szolgáltatást konfiguráljuk. Ez az IP cím általában ugyanaz, mint amin az Outlook Web App-ot is elérjük.

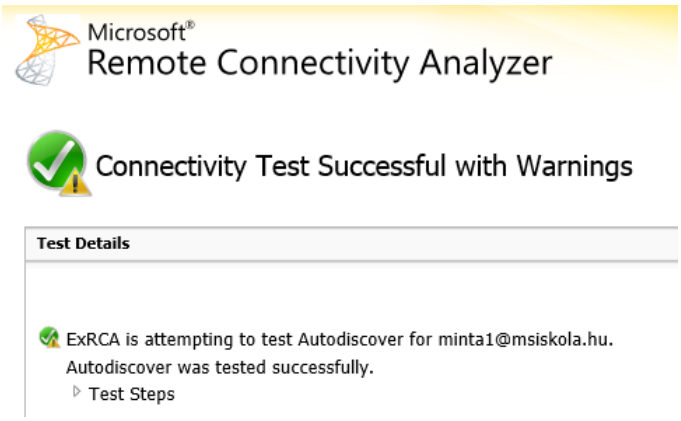
   Amennyiben tűzfalat használunk, létre kell hoznunk egy új weboldal-publikációs szabályt, amely az Exchange Client Access szerverünkre irányítja az erre a címre érkező forgalmat, és engedélyezi a /AutoDiscover/* útvonalú oldalak elérését.

   A második létrehozandó rekord egy ún. SPF rekord, ami a spamek elkerülését segíti. Beállítása nem kötelező, csak ajánlott. Ez egy TXT típusú rekord, aminek az értéke a következő:

```
v=spf1 include:outlook.com include:spf.messaging.microsoft.com ~all
```

2) Ellenőrizzük az AutoDiscover szolgáltatás működését. Ehhez látogassunk el a https://www.testexchangeconnectivity.com/ weboldalra, válasszuk az *Outlook Autodiscover* menüpontot, és kattintsunk a *Next* gombra. Adjuk meg egy érvényes felhasználó bejelentkezési adatait, és az ellenőrző kódot, majd kattintsunk a *Perform Test* gombra.

A program elkezdi ellenőrizni a szolgáltatás működését, és ha problémát észlel, azt részletesen jelzi, és javaslatot is tesz a megoldásra.

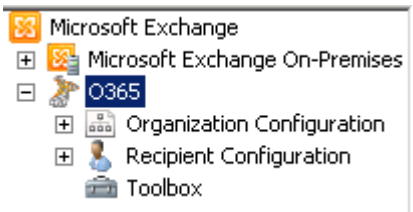


Egyszerűen meggyőződhetünk az AutoDiscover működőképességéről

3) A postaládák mozgatása a felhő és a helyi Exchange között a Mailbox Replication Service segítségével történik. Ahhoz, hogy ezt az interneten keresztül el tudja érni az Exchange Online, lehetséges, hogy módosítanunk kell a tűzfal szabályainkon. A szolgáltatás címe, amit publikálnunk kell:
   a) /EWS/mrsproxy.svc/WSSecurity
   b) /EWS/Exchange.asmx/WSSecurity
4) Adjuk hozzá az Office 365 szervezetünket az Exchange 2010 menedzsment konzoljához.

   Ehhez nyissuk meg a konzolt, és kattintsunk jobb egérgombbal a Microsoft Exchange elemre a navigációs fában. Válasszuk ki az *Add Exchange forest* elemet a helyi menüből. A megjelenő ablakban adjunk egy tetszőleges nevet a felhőbeli szervezetünknek, a *Specify the FQDN or URL of the server running the Remote PowerShell instance* legördülő menüből válasszuk az *Exchange Online* elemet, majd kattintsunk az *OK* gombra. A megjelenő ablakban adjuk meg a felhőbeli adminisztrátori adatainkat, pl.: admin@msiskola.onmicrosoft.com

   Ha az adatok helyesek voltak, a helyi Exchange telepítésünk mellett megjelenik egy új Exchange erdő a navigációs fában, amit a helyi telepítéshez hasonló módon kezelhetünk.



Az Exchange Online úgy kezelhető az EMC-ből, mintha helyi telepítés lenne

21.7.3 Hibrid telepítés létrehozása és konfigurálása

Ha teljesül a Hibrid konfiguráció összes előfeltétele, akkor elkezdhetjük létrehozni magát a konfigurációt.

1) Indítsuk el az Exchange menedzsment konzolt, és kattintsunk a *Microsoft Exchange On-Premises/Organization Configuration* elemre.
2) Az első fül a *Hybrid Configuration*, de a lista még üres. Ezért kattintsunk az üres részre jobb gombbal, és válasszuk a *New Hybrid Configuration* menüpontot.

3) A megjelenő varázsló összefoglalja a végrehajtandó parancsokat. A végrehajtáshoz kattintsunk a *New* gombra.

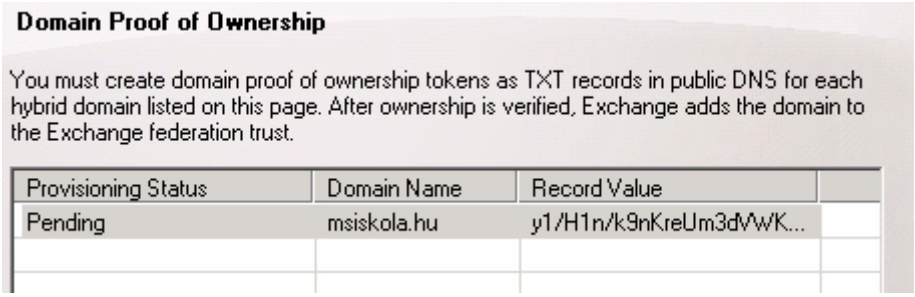
   Ezzel a varázsló létrehozta a Hibrid konfigurációs objektumot. Ennyire azért nem egyszerű a dolgunk, mert ezt az objektumot konfigurálnunk is kell.

4) Ehhez kattintsunk duplán a *Hybrid Configuration* elemre.

5) A *Credentials* lapon meg kell adnunk először a helyi, alatta pedig a felhőhöz tartozó adminisztrátori adatainkat. Írjuk be ezeket, majd kattintsunk a *Next* gombra.

6) A *Domains* lapon a levelezéshez használt domain nevet vagy neveket kell megadnunk. A hibrid konfiguráció létrehozásához legalább egy domain nevet ki kell választanunk.

7) A *Domain Proof of Ownership* lapon minden kiválasztott domainhez generál a rendszer egy kódot. Ezt a kódot az adott domain DNS zónájába, egy TXT rekord értékeként kell elhelyeznünk. A kódot a Ctrl-C billentyűk lenyomásával másolhatjuk ki az ablakból.



A jobb oldali kód jóval hosszabb, a teljes kódot Ctrl-C-vel másolhatjuk ki az ablakból

   Helyezzük el a kódot, vagy kérjük meg a domain fenntartóját, hogy hozza létre a szükséges rekordokat helyettünk. Ha ez minden domain névhez megtörtént, pipáljuk be az oldalon lévő jelölőnégyzetet, hogy továbbléphessünk.

8) A *Servers* lapon válasszuk ki azt a szervert, vagy azokat a szervereket, amelyek az Online szolgáltatással fognak kommunikálni. Meg kell adnunk legalább egy *Client Access* szervert, amely az adatok megosztását és a postafiókok mozgatását fogja végezni, és legalább egy *Hub Transport* szervert, amely a helyi és az online postafiókok közötti levélforgalmat bonyolítja.

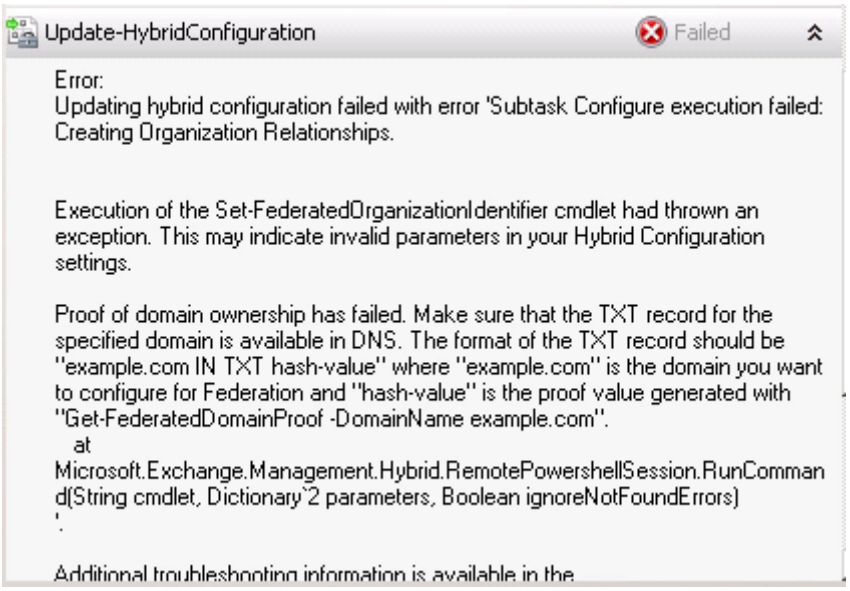
9) A *Mail Flow Settings* lapon adjuk meg a *Hub Transport* szerver(ek) külső, internet felől látható IP címét vagy címeit, és ugyanennek a szervernek a teljes címét, pl.: smtp.msiskola.hu

10) A *Mail Flow Security* lapon ki kell választanunk az előbb megadott teljes címhez tartozó, korábban igényelt vagy importált tanúsítványt. A varázsló csak a külső tanúsítványszolgáltatóktól származó, érvényes tanúsítványokat jeleníti meg.

Ezen a lapon kell kiválasztanunk azt is, hogy az Exchange Online-on tárolt postafiókokból kimenő levelek milyen úton jussanak el a címzetthez.

- *Deliver Internet-bound messages directly using the external recipient's DNS settings*: a leveleket a rendszer a helyi telepítés megkerülésével, közvetlenül a címzetthez továbbítja (ajánlott)
- *Route all Internet-bound messages through your on-premises Exchange servers*: a leveleket a rendszer minden esetben a helyi Exchange-en keresztül fogja továbbítani

11) A *Progress* lapon találunk egy összefoglalót a futtatandó parancsokról, amiket a *Manage* gombbal el is indíthatunk. A folyamat akár 15 percig is tarthat, és csak akkor fog sikeresen végződni, ha az ellenőrző kód már szerepel a domain DNS-ében.



Ha a DNS rendszeren még nem futott át a TXT rekord, ilyen hibaüzenetet kapunk

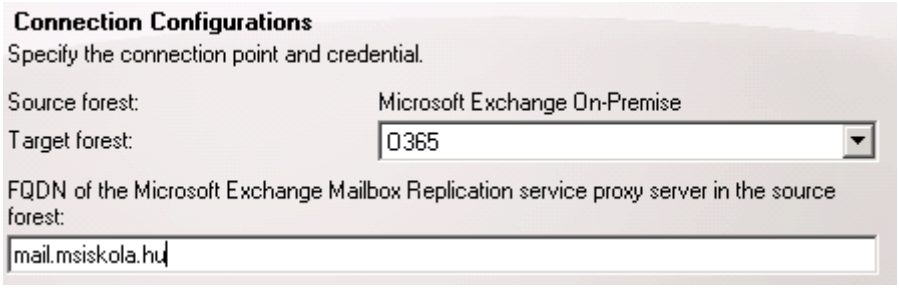
12) Hozzunk létre egy teszt postafiókot! Kattintsunk az *Exchange On-Premises/Recipient Configuration* elemre, majd a jobboldali műveletek panelen válasszuk a *New Remote Mailbox* lehetőséget.
13) Az *Introduction* lapon válasszuk a *User* mailbox típust, és kattintsunk a *Next* gombra.
14) A *User Information* lapon adjuk meg a szükséges adatokat. A UPN-utótag legördülő listából a *@msiskola.hu* értéket válasszuk.
15) Az *Archive Mailbox* lapon ne jelöljük be a jelölőnégyzetet, csak kattintsunk a *Next* gombra.
16) A *Progress* lapon kapunk egy összefoglalót a lefuttatandó parancsokról. Kattintsunk a *New* gombra a végrehajtáshoz.
17) A címtár-szinkronizáció alapértelmezés szerint 3 óránként megy végbe. Megvárhatjuk, amíg automatikusan megtörténik, vagy kézzel is elindíthatjuk. Ehhez részletes útmutatót a Címtár-szinkronizálás beállítása fejezetben találunk.
18) A webes adminisztrációs felületen aktiváljuk a frissen létrehozott felhasználót, rendeljünk hozzá licencet.
19) Próbáljunk meg bejelentkezni a friss felhasználóval a http://mail.office365.com oldalon.

21.7.4 Postaládák mozgatása

A hibrid telepítés konfigurálása után nincs más hátra, mint átmozgatni a postaládákat, vagy egy részüket a felhőbe.

1) Jelentkezzünk be az online adminisztrációs felületen, és aktiváljuk a felhőbe áttelepíteni kívánt felhasználókat.
2) Az Exchange menedzsment konzolon navigáljunk a helyi Exchange telepítés *Recipient Configuration* elemére, azon belül pedig a Mailbox pontra.
3) Jelöljünk ki egy vagy több postafiókot, amit át szeretnénk helyezni a felhőbe.
4) A jobb oldali műveletek panelen válasszuk a *New Remote Move Request* lehetőséget.
5) A megjelenő *New Remote Request* varázsló *Introduction* lapján ellenőrizzük az áthelyezendő felhasználók listáját, és hagyjuk kijelölve a *Move only the user mailbox* opciót, majd lépjünk tovább.

6) A *Target Forest* legördülő listából válasszuk ki az Office 365 szolgáltatás általunk megadott becenevét, az *FQDN of the Microsoft Exchange Mailbox Replication service proxy server in the source forest* mezőbe pedig írjuk be a *Client Access* szerverünk külső domain nevét, pl.: mail.msiskola.hu



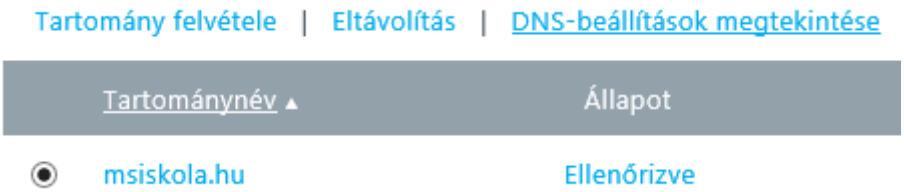
A Mailbox Replication szolgáltatás segítségével helyeződnek át a postaládák

A Use the following source forest's credentials jelölőnégyzetet jelöljük be, és adjuk meg a helyi telepítéshez tartozó adminisztrátori felhasználó adatait, akinek joga van a postafiókokat áthelyezni.

7) A *Target Delivery Domain* mezőbe a *Browse* gomb segítségével válasszuk ki a hibrid telepítés domain nevét, pl.: *msiskola.hu*
8) A következő lapon egy összefoglalót láthatunk a végrehajtandó parancsokról, amiket a *New* gombbal le is futtathatunk.
9) A gombra való kattintással létrejön egy új *Move Request*, ami az azonos nevű menüpont alatt jelenik meg, postafiókonként egy darab. Itt figyelhetjük az áttelepítési folyamatot.
10) Az áttelepítés befejeztével nem helyezhetjük át újból a postaládát mindaddig, amíg a hozzá tartozó *Move Request*et ki nem töröltük.

21.7.5 Konfiguráció befejezése

Nem maradt más hátra, mint véglegesíteni a konfigurációt a domain nevünk MX rekordjának átállításával. Így az új levelek már a Forefront Online Protection rendszeren keresztül fognak jönni, ami elvégzi a spam- és vírusszűrést, majd továbbítja a levelet a megfelelő postaládába, legyen az akár az Exchange Online-on, akár a helyi telepítésünkön.



A pontos DNS beállításokat itt találjuk meg

A pontos MX beállításokat megtaláljuk az adminisztrációs felület *Tartományok* menüpontján belül, ha kijelöljük a levelezési domain nevünket, és a táblázat feletti *DNS beállítások megtekintése* linkre kattintunk. Általánosságban elmondható, hogy az MX rekord értékének <*domain*>*.mail.eo.outlook.com* formátumúnak kell lennie, ahol a <*domain*> részt a levelezési domain nevünkkel kell behelyettesíteni úgy, hogy a pontokat kötőjelekre cseréljük. Az msiskola.hu domainhez tartozó MX rekord értéke például:

msiskola-hu.mail.eo.outlook.com

21.8 Átállásos e-mail migráció

Az átállásos e-mail migráció során egy ütemben állítjuk át az összes postaládát az Exchange Online használatára. Az egyik legkedveltebb módszer, köszönhetően egyszerű beállításának. Az átállítás után a helyi Exchange telepítés eltávolítható.

Az átállítás 4 lépésben foglalható össze:

1) A szolgáltatás minden felhasználóhoz létrehoz egy postafiókot az Exchange Online szolgáltatásban. A terjesztési csoportok, kapcsolattartók szintén másolásra kerülnek.
2) Minden egyes postafiók tartalmát és beállításait átmásolja a felhőbeli postafiókba.
3) 24 óránként növekményes szinkronizációt végez, ami azt jelenti, hogy az újonnan érkezett üzeneteket is átmásolja a felhőbe, hogy a két postaláda ismét teljesen megegyezzen.
4) Amikor beállítjuk, hogy az új levelek már a felhőbe érkezzenek, és úgy döntünk, hogy a migráció lezárható, még egyszer utoljára szinkronizálja a hiányzó elemeket a rendszer, és ezzel az áttelepítés befejeződik.

21.8.1 Rendszerkövetelmények

A hibrid telepítéshez hasonlóan itt is van néhány feltétel a módszer használatához:

- Maximum 1000 postafiók telepíthető át ezzel a módszerrel
- Exchange 2003, 2007, vagy 2010 rendszer szükséges a használatához
- Ha a címtár-szinkronizálás aktív, akkor előbb ki kell kapcsolni, és az átállás befejeztével lehet újra aktiválni
- Az Outlook Anywhere szolgáltatásnak működnie kell

21.8.2 Előkészületek

1) Ha be van kapcsolva a címtár-szinkronizálás, nem fogunk tudni átállásos migrációba kezdeni, ezért ideiglenesen ki kell kapcsolnunk. Ehhez jelentkezzünk be az adminisztrációs felületre, és a menüből válasszuk a *Felhasználók* pontot. Az *Active Directory®-szinkronizálás* mellett kattintsunk az *Inaktiválás* linkre.
2) A szolgáltatás a postaládák szinkronizálására az Outlook Anywhere szolgáltatást használja, ezért ezt mindenképpen engedélyeznünk és konfigurálnunk kell, ha még nem tettük meg.
   a) Ehhez indítsuk el az Exchange menedzsment konzolt, és navigáljunk a *Server Configuration, Client Access* pontra.
   b) A jobb oldali műveletek panelen kattintsunk az *Enable Outlook Anywhere* linkre.
   c) A megjelenő varázsló *External host name* mezőjében adjuk meg azt a kívülről is elérhető domain nevet, amit a szolgáltatáshoz használni szeretnénk. Célszerű azt a címet használni, amin a *Web App*ot is publikáltuk, mivel így nem szükséges új tanúsítványt igényelnünk.
   d) Válasszunk egy hitelesítési módot. Az NTLM hitelesítés biztonságosabb, azonban nem minden tűzfal szoftver támogatja. Forefront TMG esetén használhatjuk ezt is.
   e) Kattintsunk az *Enable* gombra az Outlook Anywhere engedélyezéséhez.
   f) Publikáljuk a tűzfalunkon a szolgáltatást. Ha a Web App hosztnevét adtuk meg az előbbiekben, akkor elegendő annak a tűzfal szabályát módosítanunk úgy, hogy a `/rpc/*` útvonalat is engedélyezze.

g) Ellenőrizzük a szolgáltatás működését! Megpróbálhatunk Outlookból kapcsolódni a szerverhez, vagy használhatjuk a http://testexchangeconnectivity.com weboldalt.

3) Hozzunk létre egy tartományi felhasználót, aminek nevében az Exchange Online kapcsolódni fog a helyi szervezetünkhöz, pl.: MSISKOLA\migracio

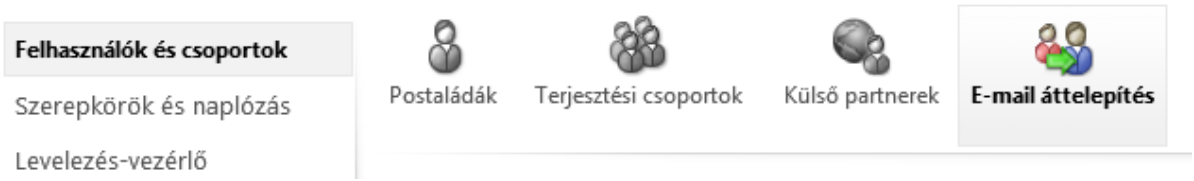
4) Az előbb létrehozott felhasználónak meg kell adnunk minden jogosultságot a postafiókokhoz, hogy a másolás sikeres legyen. Ehhez indítsuk el az *Exchange Management Shell*-t, és futtassuk a következő PowerShell parancsokat (két parancs, egy-egy sorba írandó):

```
Get-Mailbox | Add-MailboxPermission -User MSISKOLA\migracio
          -AccessRights FullAccess
Get-MailboxDatabase | Add-ADPermission -User MSISKOLA\migracio
          -ExtendedRights Receiver
```

21.8.3 Migráció

Most, hogy minden előfeltételt teljesítettünk, elkezdhetjük magát a migrációt.

1) Jelentkezzünk be az adminisztrációs felületre, és a *Rendszergazdai áttekintés* oldalon kattintsunk az Exchange felirat alatti *Kezelés* linkre. Ezzel az Exchange Online kezelőfelületére jutunk.
2) A *Felhasználók és csoportok* lapon kattintsunk az *E-mail áttelepítés* ikonra, majd az *Új* gombra.



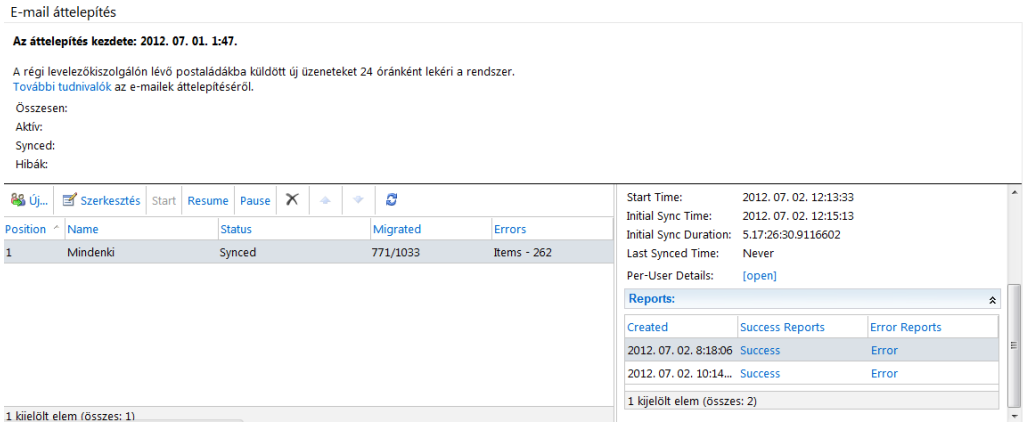
Az E-mail áttelepítés menüpont

3) Az új ablakban megnyíló *E-mail áttelepítés varázsló*ban ki kell választanunk, hogy milyen rendszerről telepítjük át a postafiókokat.
4) A következő lapon adjuk meg a korábban létrehozott, és jogosultságokat kapott felhasználó e-mail címét, pl.: migracio@msiskola.hu. Adjuk meg a felhasználói nevét és jelszavát is. Az egyidejűleg másolandó postafiókok számát az Exchange szerverünk internetkapcsolata és teljesítménye alapján válasszuk meg.
5) A *Tovább* gombra való kattintás után a szolgáltatás megpróbál kapcsolatot létesíteni a helyi Exchangeünkkel. Ha nem sikerül automatikusan megtalálnia a beállításokat, akkor további beállítások megadását kérheti. Az *Exchange-kiszolgáló* mezőben a helyi szerverünk belső domain nevét kell megadnunk, pl.: exchg.msiskola.local. Az *RPC-proxykiszolgáló* címe az Outlook Anywhere külső domain neve, pl.: mail.msiskola.hu. A *Hitelesítés* mezőben pedig válasszuk ki azt a hitelesítés típust, amit az Outlook Anywhere engedélyezésekor választottunk.
6) A harmadik lépés lapon el kell neveznünk az áttelepítési köteget. A *Köteg neve* mezőbe írjuk be az áttelepítési köteg nevét. Ha azt szeretnénk, hogy a köteg eredményeit más felhasználó is megkapja e-mailben, ne csak az, akinek neve alatt a köteget létrehoztuk, válasszuk ki a felhasználót a *Tallózás* gombra kattintva.

   Ha ezen a lapon egy CSV fájlt kér tőlünk a rendszer, az azt jelenti, hogy a címtárszinkronizálás még be van kapcsolva. Amíg ki nem kapcsoljuk, nem fogunk tudni átállásos áttelepítést végrehajtani.

7) A varázsló a *Tovább* gombra kattintva létrehozza a köteget, és összefoglalásképpen megjeleníti annak beállításait. Zárjuk be a varázslót a *Bezárás* gombra kattintva.
8) Ezzel visszakerülünk az Exchange Online adminisztrációs felületéhez, ahol már megjelenik az újonnan létrehozott áttelepítési kötegünk, melynek állapota *Létrehozva*.

   Indítsuk el ezt a köteget az Indítás linkre kattintva!



Az áttelepítés folyamata folyamatosan frissül

9) Indítás után a köteg állapota először *Várakozás* lesz. Ez azt jelenti, hogy várólistán van a szerveren, rövidesen elindul a szinkronizálás, amit a *Fut* állapot jelez. Végül, ha a szinkronizálás megtörtént, az állapot *Szinkronizálva* értékre változik.
10) A szinkronizálás befejeztével letölthetővé válik a szinkronizálási jelentés és hibalista. Ezek alapján orvosoljuk az esetlegesen felmerülő hibákat, és indítsuk újra a szinkronizációt mindaddig, amíg minden postaláda sikeresen át nem települ.

    Sikeres szinkronizáció után 24 óránként frissíti a rendszer a postafiókokat. Ha készen állunk a véglegesítésre, akkor állítsuk át a domain nevünk MX rekordját. A pontos beállításokat megtaláljuk az adminisztrációs felület Tartományok menüpontján belül, ha kijelöljük a levelezési domain nevünket, és a táblázat feletti DNS beállítások megtekintése linkre kattintunk. Általánosságban elmondható, hogy az MX rekord értékének `<domain>.mail.eo.outlook.com` formátumúnak kell lennie, ahol a `<domain>` részt a levelezési domain nevünkkel kell behelyettesíteni úgy, hogy a pontokat kötőjelekre cseréljük. Az msiskola.hu domainhez tartozó MX rekord értéke például:

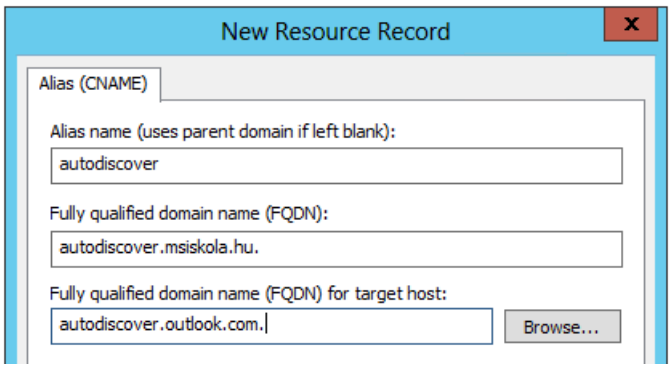
    msiskola-hu.mail.eo.outlook.com
11) Várjunk 24-72 órát, hogy a beállítások végigfussanak a DNS rendszeren, és biztosan minden új levél az online postafiókokba érkezzen.
12) Ha megbizonyosodtunk arról, hogy a beállítások érvénybe léptek, töröljük ki az áttelepítési köteget az adminisztrációs felületen. Ezzel egy utolsó szinkronizáció is elindul, hogy az összes levél átkerüljön a felhőbeli postafiókokba.

21.8.4 Konfiguráció befejezése

Néhány kiegészítő lépést még szükséges megtennünk a működés érdekében.

1) Ha még nem tettük meg, társítsunk licenceket a felhasználókhoz. A kezdeti türelmi időszak után a postafiókok elérhetetlenné válnak, ha nincsen hozzájuk megfelelő licenc társítva.
2) A megfelelő működés érdekében létre kell hoznunk, vagy módosítanunk kell az AutoDiscover rekordot a domainünk DNS bejegyzései között. Az

autodiscover.msiskola.hu CNAME típusú rekordnak az *autodiscover.outlook.com* címre kell mutatnia.



A rekord beállításai Microsoft DNS szerver használata esetén

3) Opcionálisan beállíthatunk egy könnyebben megjegyezhető címet az Outlook Web Appnak is. Alapbeállításként a felhasználók a http://mail.office365.com vagy a http://outlook.com/owa/msiskola.hu oldalon tudnak bejelentkezni a levelezésükbe, de mindkettőn egyszerűsíthetünk, ha létrehozunk egy CNAME rekordot a domainünk DNS-ében, amelynek neve pl. mail.msiskola.hu, értéke pedig *mail.office365.com*

   Ilyenkor, ha a felhasználók a mail.msiskola.hu címet írják a böngészőjükbe, rögtön az egyszeri bejelentkezési oldalunkra jutnak.

4) Ha az összes postafiók áttelepült, akár el is távolíthatjuk a helyi Exchange telepítésünket.

   Ezzel kapcsolatban bővebb információt a következő TechNet oldalon találhatunk: http://technet.microsoft.com/en-us/library/ee332361(EXCHG.141).aspx

21.9 Szakaszolt Exchange áttelepítés

Az előzőekben bemutatott eszközzel, azaz az Exchange Online adminisztrációs felületének E-mail áttelepítés eszközével a postaládák egy része is áttelepíthető.

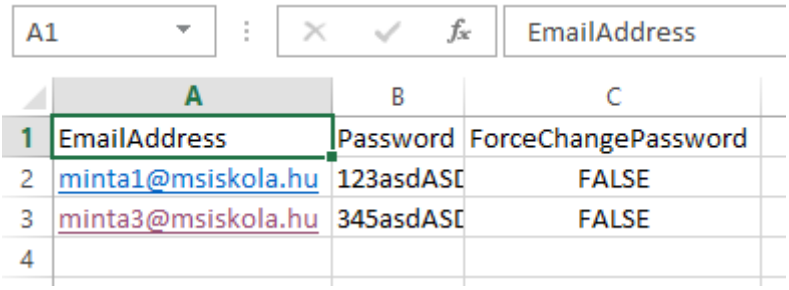
21.9.1 Rendszerkövetelmények

- Exchange Server 2003 vagy 2007 (2010 nem támogatott)
- Működő Outlook Anywhere (beállítását lásd korábban)
- Működő címtár-szinkronizálás (beállítását lásd korábban)

21.9.2 Előkészületek

1) A szakaszos áttelepítés során az áttelepítendő felhasználók körét egy CSV formátumú fájl segítségével kell megadnunk a szolgáltatásnak. Az áttelepítés a fájlban megadott sorrend szerint történik. Egy fájlban maximum 1000 postafiókot adhatunk meg, de több fájlt is feltölthetünk. A fájlnak a következő oszlopokat kell tartalmaznia:
   - *EmailAddress*: a helyi postaládához tartozó elsődleges SMTP cím. Fontos, hogy mindenképpen az elsődleges cím legyen itt megadva.
   - *Password*: az új postaláda jelszava. Ha egyszeri bejelentkezést használunk, akkor ezt a paramétert nem kötelező megadni.
   - *ForceChangePassword*: értéke *True* vagy *False* lehet. Azt adja meg, hogy a felhasználónak meg kell-e változtatnia a jelszavát az első belépéskor. Ha egyszeri bejelentkezést használunk, az értéke *False* legyen.

A CSV fájlt elkészíthetjük táblázatkezelő szoftver segítségével, mint amilyen például a Microsoft Excel, vagy használhatunk PowerShellt is.



A fájlt Excellel is elkészíthetjük, ha a mentéskor fájltípusnak a CSV fájlt adjuk meg

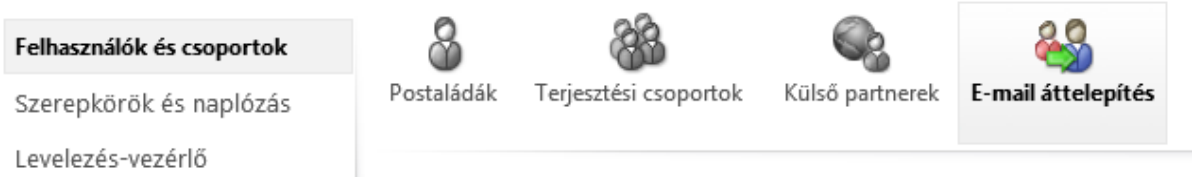
2) Hozzunk létre egy tartományi felhasználót, aminek nevében az Exchange Online kapcsolódni fog a helyi szervezetünkhöz, pl.: MSISKOLA\migracio
3) Az előbb létrehozott felhasználónak meg kell adnunk minden jogosultságot a postafiókokhoz, hogy a másolás sikeres legyen. Ehhez indítsuk el az Exchange Management Shell-t, és futtassuk a következő PowerShell parancsokat (két parancs, egy-egy sorba írandó):

```
Get-Mailbox | Add-MailboxPermission -User MSISKOLA\migracio
         -AccessRights FullAccess
Get-MailboxDatabase | Add-ADPermission -User MSISKOLA\migracio
         -ExtendedRights Receiver
```

21.9.3 Migráció

Most, hogy minden előfeltételt teljesítettünk, elkezdhetjük magát a migrációt.

1) Jelentkezzünk be az adminisztrációs felületre, és a *Rendszergazdai áttekintés* oldalon kattintsunk az Exchange felirat alatti *Kezelés* linkre. Ezzel az Exchange Online kezelőfelületére jutunk.
2) A *Felhasználók és csoportok* lapon kattintsunk az *E-mail áttelepítés* ikonra, majd az *Új* gombra.

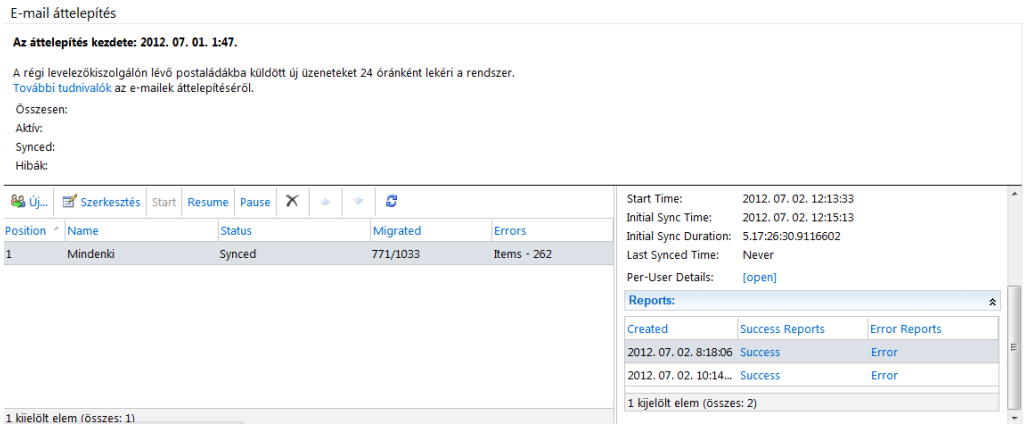


Az E-mail áttelepítés menüpont

3) Az új ablakban megnyíló *E-mail áttelepítés varázsló*ban ki kell választanunk, hogy milyen rendszerről telepítjük át a postafiókokat.
4) A következő lapon adjuk meg a korábban létrehozott és jogosultságokat kapott felhasználó e-mail címét, pl.: migracio@msiskola.hu. Adjuk meg a felhasználói nevét és jelszavát is. Az egyidejűleg másolandó postafiókok számát az internetkapcsolatunk és az Exchange szerverünk sebessége alapján válasszuk meg.
5) A *Tovább* gombra való kattintás után a szolgáltatás megpróbál kapcsolatot létesíteni a helyi Exchangeünkkel. Ha nem sikerül automatikusan megtalálnia a beállításokat, akkor további beállítások megadását kérheti. Az *Exchange-kiszolgáló* mezőben a helyi szerverünk belső domain nevét kell megadnunk, pl.: exchg.msiskola.local. Az *RPC-*

proxykiszolgáló címe az Outlook Anywhere külső domain neve, pl.: mail.msiskola.hu. A *Hitelesítés* mezőben pedig válasszuk ki azt a hitelesítés típust, amit az Outlook Anywhere engedélyezésekor választottunk.

6) A következő lapon tallóznunk kell a korábban létrehozott CSV típusú fájlunkat, és elnevezni az áttelepítési köteget, amit most létrehozunk.
7) A Tovább gombra kattintva a rendszer ellenőrzi a feltöltött fájlt. Ha problémát talál, részletes leírást ad, és javaslatot tesz a megoldásra.
8) A varázsló bezárása után visszakerülünk az E-mail áttelepítés eszköz oldalára. Ha voltak problémás elemek, akkor dönthetünk úgy, hogy kitöröljük a köteget, és a problémák javítása után újra feltöltjük, de el is indíthatjuk a köteget, és a kihagyott elemeket később egy új kötegben külön is áttelepíthetjük.
9) Indítsuk el ezt a köteget az *Indítás* linkre kattintva!



Az áttelepítés folyamata folyamatosan frissül

10) Indítás után a köteg állapota először *Várakozás* lesz. Ez azt jelenti, hogy várólistán van a szerveren, rövidesen elindul a szinkronizálás, amit a *Fut* állapot jelez. Végül, ha a szinkronizálás megtörtént, az állapot *Szinkronizálva* értékre változik.
11) A szinkronizálás befejeztével letölthetővé válik a szinkronizálási jelentés és hibalista. Ezek alapján orvosoljuk az esetlegesen felmerülő hibákat, és indítsuk újra a szinkronizációt mindaddig, amíg minden postaláda sikeresen át nem települ.
12) Az áttelepítés befejeztével ajánlott a helyi postafiókok átalakítása levelezésre jogosult felhasználókká. Erre azért van szükség, mert az áttelepítés után a felhasználónak van egy felhőbeli és egy helyi postaládája is. Az új levelek automatikusan továbbítva lesznek a felhőbeli postafiókjába, ugyanakkor, ha Outlook használatával szeretne kapcsolódni, az AutoDiscover szolgáltatás a helyi postaládára fogja irányítani a felhasználót. Másrészt, ha nem alakítjuk át a postafiókokat, akkor az Exchange szerver esetleges későbbi eltávolítása nem várt következményekkel járhat.

    A konvertáláshoz szükséges PowerShell szkriptek a következő oldalról tölthetőek le:

    Exchange 2007: http://community.office365.com/en-us/wikis/exchange/845.aspx

    Exchange 2003: http://community.office365.com/en-us/wikis/exchange/834.aspx

    Az átalakítás menete:

    a) Másoljuk az ExportO365UserInfo.ps1, Exchange2007MBtoMEU.ps1 fájlokat, és az áttelepítéshez használt csv fájlt egy új könyvtárba az Exchange szerverünkön.
    b) Nevezzük át a CSV fájlt *migration.csv*-re.
    c) Indítsuk el az Exchange Management Shellt, lépjünk az előbb létrehozott mappába, és futtassuk le a `.\ExportO365UserInfo.ps1` parancsot.

d) A szkript meg fogja kérdezni, hogy új kapcsolatot szeretnénk-e létrehozni, vagy egy meglévőt fogunk használni. Írjunk egy `n` betűt az új kapcsolat létrehozásához, majd adjuk meg a felhőbeli adminisztrátori adatainkat. A szkript futtatása során létrehoz egy Cloud.csv fájlt.

e) Ha az előző szkript futtatása befejeződött, ugyanabba az ablakba írjuk be a következőt:
`.\Exchange2007MBtoMEU.ps1 dc.msiskola.local`

Ahol a dc.msiskola.local helyére a tartományban található egyik írható tartomány-vezérlő címét írjuk.

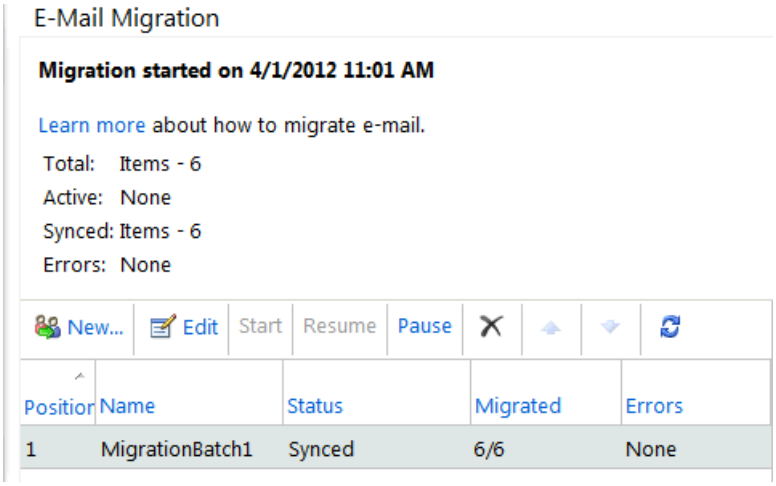
Ez a szkript elvégzi az átalakítást.

f) Ezt a folyamatot hajtsuk végre az összes áttelepítési köteg CSV fájljával.

Exchange 2003 esetén a folyamat hasonló, azonban a második szkript nem PowerShell, hanem VBScript. Ezért a parancs a következőre változik:

```
cscript Exchange2003MBtoMEU.vbs –c .\Cloud.csv dc.msiskola.local
```

13) Ha az áttelepítési köteg sikeresen áttelepítette a felhasználókat, és azokat át is alakítottuk levelezésre jogosult felhasználókká, az áttelepítési köteget törölhetjük.



Az áttelepítési köteg az X ikonnal törölhető

21.9.4 Konfiguráció befejezése

Néhány kiegészítő lépést még szükséges megtennünk a működés érdekében.

1) Ha még nem tettük meg, társítsunk licenceket a felhasználókhoz. A kezdeti türelmi időszak után a postafiókok elérhetetlenné válnak, ha nincsen hozzájuk megfelelő licenc társítva.

Ha már az összes felhasználót áttelepítettük a felhőbe, a helyi Exchange eltávolítása előtt néhány lépést még meg kell tennünk:

2) A megfelelő működés érdekében létre kell hoznunk, vagy módosítanunk kell az AutoDiscover rekordot a domainünk DNS bejegyzései között. Az *autodiscover.msiskola.hu* CNAME típusú rekordnak az *autodiscover.outlook.com* címre kell mutatnia.

3) Opcionálisan beállíthatunk egy könnyebben megjegyezhető címet az Outlook Web Appnak is. Alapbeállításként a felhasználók a http://mail.office365.com vagy a http://outlook.com/owa/msiskola.hu oldalon tudnak bejelentkezni a levelezésükbe, de

mindkettőn egyszerűsíthetünk, ha létrehozunk egy CNAME rekordot a domainünk DNS-ében, amelynek neve pl. mail.msiskola.hu, értéke pedig mail.office365.com

Ilyenkor, ha a felhasználók a mail.msiskola.hu címet írják a böngészőjükbe, rögtön az egyszeri bejelentkezési oldalunkra jutnak.

4) Be kell állítanunk, hogy az új levelek közvetlenül a felhőalapú postaládákba érkezzenek. Ehhez állítsuk át a domain nevünk MX rekordját!

   A pontos beállításokat megtaláljuk az adminisztrációs felület Tartományok menüpontján belül, ha kijelöljük a levelezési domain nevünket, és a táblázat feletti DNS beállítások megtekintése linkre kattintunk. Általánosságban elmondható, hogy az MX rekord értékének `<domain>.mail.eo.outlook.com` formátumúnak kell lennie, ahol a `<domain>` részt a levelezési domain nevünkkel kell behelyettesíteni úgy, hogy a pontokat kötőjelekre cseréljük. Az msiskola.hu domainhez tartozó MX rekord értéke például:

   msiskola-hu.mail.eo.outlook.com

   Várjunk 24-72 órát, hogy a beállítások végigfussanak a DNS rendszeren, és biztosan minden új levél az online postafiókokba érkezzen.

5) Ezek után a helyi kiszolgáló eltávolítható.

   Ezzel kapcsolatban bővebb információt a következő TechNet oldalon találhatunk: http://technet.microsoft.com/en-us/library/ee332361(EXCHG.141).aspx

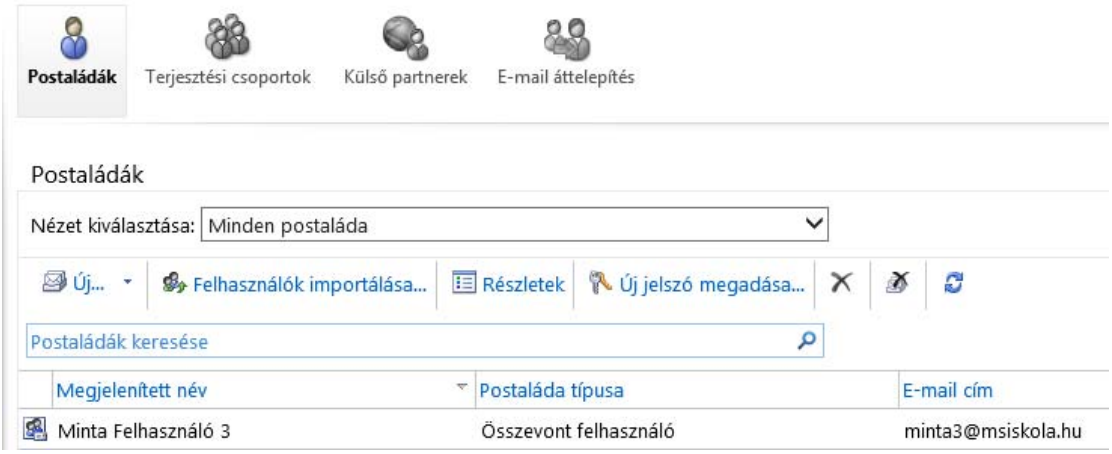
21.10 E-mail áttelepítés IMAP protokoll használatával

Ha Exchange 2003 előtti, vagy nem Microsoft gyártmányú levelezőrendszert használunk jelenleg, lehetőségünk van a szabványos IMAP protokoll használatával áttelepíteni a postafiókokat.

21.10.1 Előkészületek

1) Létre kell hoznunk minden áttelepítendő felhasználónak egy postafiókot az Exchange Online rendszerben.

   Jelentkezzünk be az adminisztrációs felületre, és a Rendszergazdai áttekintés oldalon kattintsunk az Exchange felirat alatti Kezelés linkre. Ezzel az Exchange Online kezelőfelületére jutunk.



Az Exchange Online Postaládák eszközének felülete

A postafiókok létrehozására két lehetőség áll rendelkezésünkre. Létrehozhatjuk őket egyesével, kézzel, vagy készíthetünk egy CSV fájlt, amit feltöltünk a Felhasználók importálása varázslóba, ami létrehozza a szükséges postafiókokat.

Ha a kézi módszert választjuk, az Exchange Online Postaládák eszközének felületén válasszuk az Új lehetőséget. A megjelenő ablakban töltsük ki az űrlapot, és ismételjük ezt meg az összes áttelepítendő felhasználó adataival.

Ha sok postaládát szeretnénk áttelepíteni, a kézi megoldás rendkívül időigényes, ráadásul nagy a hibalehetőség is. Ilyen esetben hozzunk létre egy CSV fájlt. Ehhez sokféle programot használhatunk, pl. a Jegyzettömböt, vagy a Microsoft Excelt. A fájlban a következő oszlopokat kötelező használnunk:

- *Name*: a felhasználó egyedi azonosítója
- *EmailAddress*: a felhasználó teljes e-mail címe
- *FirstName*: a felhasználó keresztneve
- *LastName*: a felhasználó vezetékneve
- *Password*: a felhasználó kezdeti jelszava

Minta fájl:

```
Name,EmailAddress,FirstName,LastName,Password
minta1,minta1@msiskola.hu,Kis,József,abc123
minta2,minta2@msiskola.hu,Nagy,István,bcd345
```

Ezeken kívül használhatunk egy sor nem kötelező tulajdonságot, például: *DisplayName, ForceChangePassword, Company, City*

2) A varázsló a fájl tallózása után egy szintaktikai ellenőrzést végez a fájlon, hogy az formailag megfelel-e a követelményeknek. Ha igen, akkor az *Importálás* gombra kattintva kezdődik meg a postafiókok létrehozása.

   Az importálás folyamata alatt a Postaládák lapon megjelenik egy új állapotablak, amelyben folyamatosan nyomon követhetőek a sikeres és sikertelen importálási kísérletek.

   A feldolgozás befejeztével a fájlt feltöltő adminisztrátor e-mailben kap összefoglalót az importálás eredményéről.

3) Engedélyezzük a meglévő levelezőrendszerünkben az IMAP protokoll használatával történő postaláda-hozzáférést, és a tűzfalunkat is állítsuk be, hogy az internet felől is elérhető legyen ezen a módon a levelezőszerver.

4) A felhasználók importálásához hasonló módon létre kell hoznunk még egy CSV fájlt, amelyben minden felhasználóhoz megadjuk a hozzáférési adatokat. Lehetőségünk van megadni minden felhasználóhoz a hozzá tartozó jelszót, vagy használhatunk minden postafiókhoz egy adminisztrátori felhasználót, akinek hozzáférése van a postafiókokhoz.

   A fájlban a következő kötelező oszlopokat kell megadnunk:

   EmailAddress: a felhasználó teljes e-mail címe

   Username: a felhasználó vagy az adminisztrátor felhasználói neve

   Ha egy adminisztrátori felhasználóval szeretnénk hozzáférni a postaládákhoz, akkor a *felhasználónevet a következő formátumban kell megadni:*

   Exchange IMAP esetén:

   Tartomány/admin_felhasználónév/felhasználó_felhasználónév

   SASL protokollt támogató IMAP szerver esetén (pl.: Dovecot):

   admin_felhasználónév*felhasználó_felhasználónév

   Mirapoint Message Server esetén:

#felhasználó@tartomány#admin_felhasználó#

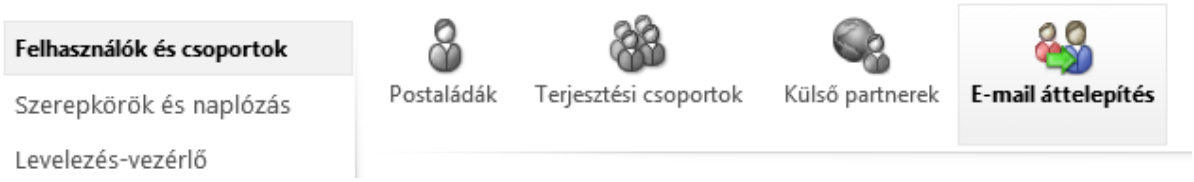
Password: a felhasználó, vagy az adminisztrátor jelszava

Courier IMAP kiszolgáló esetén a felhasználónév és a jelszó mezőkbe az adminisztrátor nevét és jelszavát kell megadni, és egy új, UserRoot oszlopba kell megadni egy ún. virtuális megosztott mappa útvonalat, amelyen a kívánt postafiók elérhető. Erről bővebb információ a Courier levelezőszerver weboldalán található: http://www.courier-mta.org/imap/README.sharedfolders.html

5) Ha az előbb létrehozott CSV fájlban rendszergazdai adatokkal kapcsolódunk a postafiókokhoz, akkor győződjünk meg róla, hogy ennek a felhasználónak van jogosultsága olvasni az áttelepítendő postaládákat.

21.10.2 Migráció

1) Jelentkezzünk be az adminisztrációs felületre, és a *Rendszergazdai áttekintés* oldalon kattintsunk az Exchange felirat alatti *Kezelés* linkre. Ezzel az Exchange Online kezelőfelületére jutunk.
2) A *Felhasználók és csoportok* lapon kattintsunk az *E-mail áttelepítés* ikonra, majd az *Új* gombra.



Az E-mail áttelepítés menüpont

3) Az új ablakban megnyíló *E-mail áttelepítés varázsló*ban ki kell választanunk, hogy milyen rendszerről telepítjük át a postafiókokat. Itt válasszuk az IMAP lehetőséget, és kattintsunk a *Tovább* gombra.
4) A következő lapon meg kell adnunk az IMAP kiszolgáló beállításait:

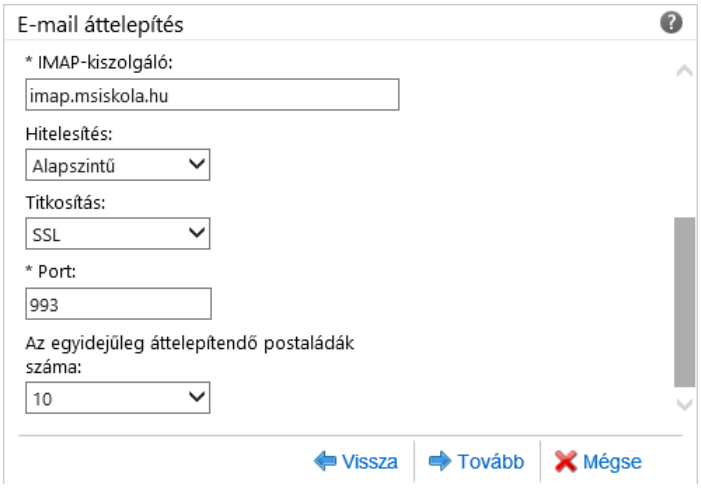
   IMAP kiszolgáló: az IMAP kiszolgáló internet felőli címe, pl.: imap.msiskola.hu

   Hitelesítés: a szerver által támogatott hitelesítési módszer. Az NTLM módszert többnyire Microsoft rendszerek támogatják.

   Titkosítás: a kiszolgáló által támogatott titkosítási módszer

   Port: a kapcsolódáshoz használt port. Az alapértelmezett IMAP port a 143, de ha SSL-titkosított kapcsolatot használunk, ez általában 993.

   Egyidejűleg áttelepítendő postaládák száma: válasszuk ki a szerver és az internetkapcsolat kapacitásának figyelembevételével.



IMAP áttelepítési beállítások

5) A *Tovább* gombra való kattintás után a rendszer megpróbál kapcsolódni a megadott beállításokkal. Ha a kapcsolódás sikeres volt, a következő lapon ki kell választanunk az előbbiekben létrehozott postaláda adatokat tartalmazó CSV fájlt.

   Nevezzük el a kötetet, majd adjuk meg azokat a mappákat, amelyeket nem szeretnénk átmásolni az új postaládába. Ilyen lehet például a Levélszemét. A nyilvános és megosztott mappákat sem ajánlott átmásolni, mivel ezek többé nem nyilvános mappaként fognak működni, hanem minden postaládába külön-külön átmásolódik a tartalmuk. A „/” (per) jelet tartalmazó mappák nem másolódnak át.

   Megadhatunk továbbá más felhasználókat is, akiknek az áttelepítés jelentést el szeretnénk küldeni.

6) Ha a CSV fájllal minden rendben volt, az E-mail áttelepítés oldalról indítsuk el az áttelepítési köteget.

7) A postaládák első szinkronizálása után a rendszer 24 óránként növekményes szinkronizálást hajt végre, ami azt jelenti, hogy a postaládákon történt változásokat átmásolja a felhőbeli postaládába is.

   Ha az összes postaláda sikeresen szinkronizálódik, és készen állunk a véglegesítésre, akkor állítsuk át a domain nevünk MX rekordját. A pontos beállításokat megtaláljuk az adminisztrációs felület Tartományok menüpontján belül, ha kijelöljük a levelezési domain nevünket, és a táblázat feletti DNS beállítások megtekintése linkre kattintunk. Általánosságban elmondható, hogy az MX rekord értékének <domain>.mail.eo.outlook.com formátumúnak kell lennie, ahol a <domain> részt a levelezési domain nevünkkel kell behelyettesíteni úgy, hogy a pontokat kötőjelekre cseréljük. Az msiskola.hu domainhez tartozó MX rekord értéke például:

   msiskola-hu.mail.eo.outlook.com

8) Várjunk 24-72 órát, hogy a beállítások végigfussanak a DNS rendszeren, és biztosan minden új levél az online postafiókokba érkezzen.

9) Ha megbizonyosodtunk arról, hogy a beállítások érvénybe léptek, töröljük ki az áttelepítési köteget az adminisztrációs felületen. Ezzel egy utolsó szinkronizáció is elindul, hogy az összes levél átkerüljön a felhőbeli postafiókokba.

21.10.3 Konfiguráció befejezése

Néhány kiegészítő lépést még szükséges megtennünk a működés érdekében.

1) Ha még nem tettük meg, társítsunk licenceket a felhasználókhoz. A kezdeti türelmi időszak után a postafiókok elérhetetlenné válnak, ha nincsen hozzájuk megfelelő licenc társítva.
2) A megfelelő működés érdekében létre kell hoznunk, vagy módosítanunk kell az AutoDiscover rekordot a domainünk DNS bejegyzései között. Az *autodiscover.msiskola.hu* CNAME típusú rekordnak az *autodiscover.outlook.com* címre kell mutatnia.
3) Opcionálisan beállíthatunk egy könnyebben megjegyezhető címet az Outlook Web Appnak is. Alapbeállításként a felhasználók a http://mail.office365.com vagy a http://outlook.com/msiskola.hu oldalon tudnak bejelentkezni a levelezésükbe, de mindkettőn egyszerűsíthetünk, ha létrehozunk egy CNAME rekordot a domainünk DNS-ében, amelynek neve pl. *mail*, értéke pedig *mail.office365.com*
4) Ilyenkor, ha a felhasználók a mail.msiskola.hu címet írják a böngészőjükbe, rögtön az egyszeri bejelentkezési oldalunkra jutnak.
5) Ezek után a helyi telepítésű levelezőrendszert akár el is távolíthatjuk.

21.11 A levelezés adminisztrációja

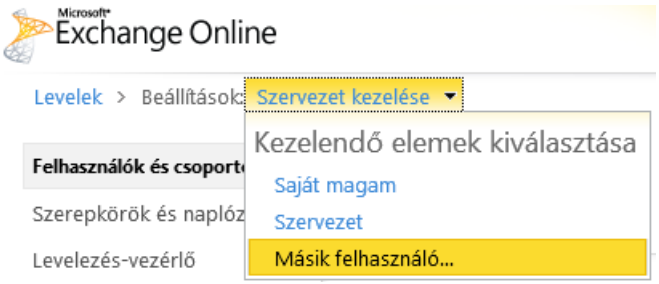
Az Office 365 alapú levelezőrendszerünk most már gyakorlatilag működőképes, azonban néhány finomhangolás még hátra lehet. A levelezés adminisztrálására két fő felületünk van: az *Exchange Control Panel* (továbbiakban ECP), és a *Forefront Online Protection for Exchange* (továbbiakban FOPE) adminisztrációs felülete. Ezeken kívül használhatunk PowerShellt is az Exchange Online adminisztrációjára, ami szintén ismerős lehet a „telepítős” Exchangeből, igaz, az Online-on a parancsoknak csak egy része érhető el.

21.11.1 Exchange Control Panel

Az ECP-vel nagy valószínűséggel az áttelepítés közben is találkoztunk már, és szinte teljesen megegyezik a helyileg telepített Exchange szerver hasonló felületével.

Tipp: az ECP-t az egyszerűség kedvéért eddig mindig az Office 365 adminisztrációs felületén keresztül értük el. Van egy másik módszer is, ami néha jobban kézre esik. Ha be vagyunk jelentkezve az adminisztrátori jogú felhasználónk Web App-jába, kattintsunk a nevünk alatti *Beállítások* linkre, azon belül pedig a *Minden beállítás megjelenítése* linkre. Ha az Outlook Web App logó alatt a *Saját magam kezelése* link fölé visszük az egeret, jogosult felhasználóknak megjelenik a *Szervezet* link, amivel ugyanarra a felületre juthatunk el, amire eddig a másik módszerrel.

Ha egyébként itt a *Másik felhasználó kezelése* linkre kattintunk, akkor megfelelő jogosultságok megléte esetén megnyithatjuk egy másik felhasználó beállításait, és módosításokat hajthatunk létre rajta, pl. átirányíthatjuk a leveleit.



Egyszerűen szerkeszthetjük más felhasználók beállításait

A *Felhasználók és csoportok* lapon kezelhetjük az egyes postafiókokat, terjesztési csoportokat és kapcsolattartókat. Az E-mail áttelepítés eszköz már ismerős lehet.

A *Szerepkörök és naplózás* lapon rendszergazdai és felhasználói szerepköröket állíthatunk be, azonban ezt ajánlott az Office 365 adminisztrációs felületén intézni. A *Naplózás* fülön különböző biztonsági és hozzáférési naplófájlokat tudunk megtekinteni és letölteni.

A *Levelezés-vezérlő* lapon belül a *Szabályok* fülön a levélforgalom egy részét vagy egészét befolyásolhatjuk. Beállíthatjuk például, hogy egy adott csoport tagjainak küldött leveleket először küldje el a rendszer jóváhagyásra egy bizonyos személynek, ha az üzenet mellékleteket is tartalmazott. A *Naplózás* fülön beállíthatjuk, hogy a rendszer naplóba rögzítse az összes kommunikációt, ami a szervezeten keresztül zajlik, a *Kézbesítési jelentések* eszközzel pedig üzenetek sorsa felől szerezhetünk információkat.

21.11.2 A FOPE adminisztrációs felület

A FOPE, hasonlóan a telepíthető Forefront Protection for Exchange (FPE) termékhez, egy spam- és vírusszűrő rendszer. Az adminisztrációs felület elérésére két lehetőségünk van. Vagy az ECP-n keresztül jutunk el ide a *Levelezés-vezérlő* lapon lévő *„A biztonságos IP-címek, a személyhálózati üzenetkövetés és az e-mail házirendek beállítása.”* linkre kattintva, vagy közvetlenül az https://admin.messaging.microsoft.com címet látogatjuk meg.

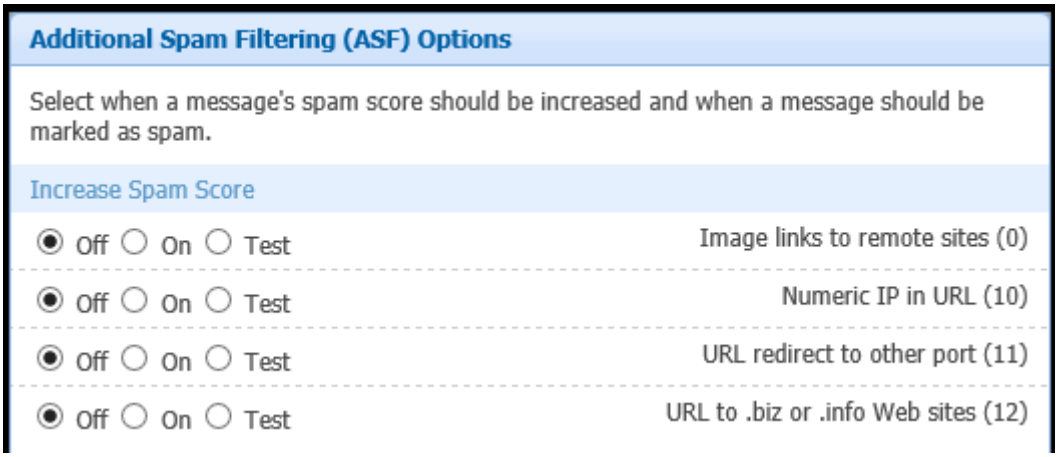
A termékről fontos tudni, hogy az Office 365-től függetlenül is elő lehet rá fizetni, így vannak bizonyos beállítások, amelyek számunkra nem lesznek relevánsak, mert a FOPE és a levelezőszerverünk közötti kapcsolat Office 365 esetén automatikusan konfigurálva van, hiszen a levelezőszerver is a felhőben, sőt, ugyanúgy a Microsoftnál van. Hibrid konfiguráció esetén ez már csak félig igaz, de ebben az esetben a szükséges beállítások automatikusan megtörténnek.

Belépés után az *Information* fülre kerülünk. Itt a bal és jobb oldali oszlopokban grafikonokon mutatja be a rendszer, hogy mennyi ártalmas levéltől óvott meg minket, és az összes felhasználót, aki ezt használja, középen pedig a rendszert érintő frissítésekről, karbantartásokról értesítenek bennünket, illetve a fenti linkek segítségével váltogathatunk többféle információs nézet között. Megtudhatjuk például, hogy milyen IP címeket használ a rendszer, illetve egy helyen össze vannak gyűjtve a technikai segédanyagok is.

Az *Administration* fül alatt a *Company* lapon beállíthatjuk a felület nyelvét (magyar sajnos nincs), illetve az időzónát. Korlátozhatjuk ezen kívül az adminisztrációs felület elérhetőségét bizonyos IP címekre, ha maximális biztonságra törekszünk.

A *Domains* lapon a domain kiválasztása után a *Domain Settings* ablakban megadhatjuk, hogy hova küldjön titkos másolatot a rendszer a kimenő, gyanús üzenetekről. A Spam Action me-

zőben megmondhatjuk, mi történjen az észlelt spam üzenetekkel. Az *Additional Spam Filtering (ASF) Options* mezőben beállíthatjuk, hogy bizonyos tényezők, pl. ha egy levélben IP címre mutató link van, növeljék-e a levél spam-kockázati értékét. Ezeket a beállításokat végleges beállítás előtt tesztelni is tudjuk. Az *Outbound E-mail Footer* beállítás segítségével minden kimenő üzenet végére beszúrhatunk egy szöveges vagy HTML üzenetet.



Növelhetjük a spamszűrő érzékenységét

A *Users* lap Office 365 felhasználók számára nem érdekes, mivel a felhasználóink itt nem fognak megjelenni.

Annál érdekesebb viszont a *Policy Rules* lap. Ezen a lapon különböző szabályokat hozhatunk létre, amelyek segítségével irányíthatjuk és szűrhetjük a levélforgalmat. A bal oldali *Rules Settings* ablakban kell megadnunk, hogy melyik domain névre érkező, milyen irányú levéllel mit szeretnénk kezdeni. Lehetőségünk van többek között elvetni, engedélyezni, karanténba helyezni, átirányítani, titkos másolattal továbbítani az üzenetet. A szűrést többek között az üzenet fejlécei, a küldő IP címe, domain neve, e-mail címe, a címzett hasonló tulajdonságai és még egy sor egyéb feltétel alapján tudjuk finomítani.

A *Filters* lapon szótárakat tudunk feltölteni. Egy szótár tartalmazhat kulcsszavakat, IP címeket, domain neveket, ami alapján egy szabályban szűrni tudjuk az üzeneteket.

A *My Reports* fülön jelentéseket készíthetünk és futtathatunk különböző témakörökben.

A *Tools* fülön belül a *Message Trace* oldalon üzeneteket kereshetünk meg, és megtudhatjuk, milyen okból (nem) kapta meg a címzett, míg az *Audit Trail* lapon az adminisztrációs felületen keresztül végrehajtott módosításokat követhetjük nyomon.

21.11.3 Exchange Management Shell

A felhőbeli Exchange szervezetünket a helyi telepítéshez hasonlóan PowerShell felületen keresztül is tudjuk adminisztrálni. Ehhez csak annyit kell tennünk, hogy nyitunk egy PowerShell ablakot, és beírjuk a következő parancsokat:

```
$LiveCred = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
         ConnectionUri https://ps.outlook.com/powershell/ -Credential
         $LiveCred -Authentication Basic -AllowRedirection
Import-PSSession $Session
```

Az adminisztrátori hitelesítő adataink megadása után ebből az ablakból úgy kezelhetjük a levelezésünket kiszolgáló távoli Exchange szervert, mintha a helyi telepítésünk volna. Természetesen nem minden parancs érhető el, ami helyi telepítés esetén viszont igen.

Az engedélyezett parancsok listája, és rövid használati útmutatója ezen a címen található: http://help.outlook.com/hu-hu/140/dd575549.aspx

21.12 SharePoint Online

A Microsoft SharePoint Server egy web alapú csoportmunka szoftver, amely fájlok megosztására, a kommunikáció és az együttműködés elősegítésére szolgál. Nagymértékű integrációval rendelkezik az Office alkalmazásokkal.

A SharePoint Online a SharePoint Server felhőben fenntartott változata, amely része az Office 365 csomagnak is. A SharePoint szoftver teljes bemutatására külön könyvek témája, így értelemszerűen ennek a fejezetnek nem ez a célja.

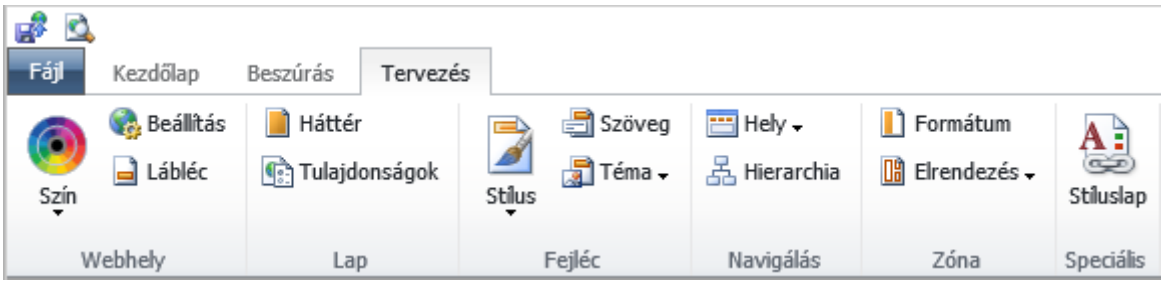
A SharePoint szolgáltatásnak – az Exchangehez hasonlóan – saját adminisztrációs felülete van az Office 365-ön belül, amelyet elérhetünk az Office 365 portálról, vagy a megnyithatjuk közvetlenül, a https://msiskola-admin.sharepoint.com címet használva.

Ezen az oldalon, a *Webhelycsoportok kezelése* linkre kattintva van lehetőségünk 1 db *nyilvános webhely*, és akár 300 db *magánwebhelycsoport* létrehozására.

21.12.1 Nyilvános webhelyek

A telepített változatához hasonlóan a SharePoint Online is kínál nyilvános webhely szolgáltatást. A jelenlegi verzióban azonban ennek a funkcionalitása jelentősen korlátozott. A nyilvános webhely jelenleg néhány előre elkészített minialkalmazáson túl csak statikus tartalmat tartalmazhat.

Ugyanakkor a szerkesztés böngészőből, egyszerűen kezelhető szalagos felületen keresztül történik. Számos előre elkészített sablonból állíthatjuk össze a weboldalunk kinézetét. A színeket és a stíluslapokat testre szabhatjuk, de a SharePoint Designer használata nem támogatott.



Ismerős felületen szabhatjuk testre az oldal kinézetét

A szolgáltatással jelenleg profi weboldalakat ugyan nem lehet készíteni, de az egyszerű kezelhetőségéhez mérten igen jól testre szabható a végeredmény, így ha egy egyszerűen elkészíthető és karbantartható weboldalt szeretnénk készíteni, nem fogunk csalódni.

21.12.2 Intranet webhelyek

Az intranet webhelyek már sokkal nagyobb hasonlóságot mutatnak a SharePoint Server 2010-zel, itt már a szokásos felületet kapjuk, mindössze néhány ritkábban használt szolgáltatás nem érhető el – egyelőre.

A legnagyobb különbség talán a külső fejlesztésű programok futtatásában van. Mivel a SharePoint Online-on egy szerveren több szervezet oldalai is futnak, ezeket a lehető legjobban el kell különíteni egymástól. Ezért a fejlesztők ún. homokozókba (sandboxokba) tölthetik fel a saját alkalmazásaikat, és ezek az oldal „SharePointos” részétől elkülönítve futnak.

Ezeknek a sandboxoknak webhelycsoportonként van egy ún. erőforrás-használati kvótájuk. Amikor egy ilyen program processzoridőt használ, kivételt dob, vagy más műveletet végez, ebből a kvótából használ el. A kvóta a felhasználói licencek száma alapján számítódik, és naponta áll rendelkezésre.

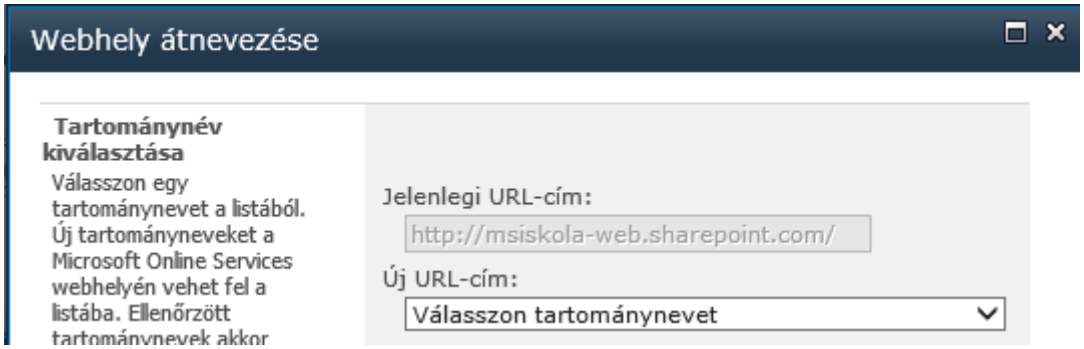
A kiosztott kvótákat az adminisztrációs felületen láthatjuk

A felhasználható tárterület szintén felhasználónként számítódik. A szervezet kiindulási 10 Gigabájt tárhelyéhez minden nem-kioszk felhasználó után jár 500 Megabájt hely. Ezen kívül természetesen külön is vásárolható tárhely.

21.12.3 DNS beállítások

A publikus webhelyünk esetén lehetőségünk van saját domain nevet használni a webhely elérésére. A rendszer megkötése szerint azonban ugyanazt a domain nevet nem használhatjuk a SharePoint rendszerhez, amit már használunk az Exchange vagy Lync szolgáltatásokhoz.

Lehetőségünk van ugyanakkor létrehozni egy új harmadszintű domaint (pl. www.msiskola.hu), amit már társíthatunk a SharePoint szolgáltatáshoz. Ezt a domaint a másodszintűhöz hasonlóan fel kell vinnünk az adminisztrációs felület *Tartományok* lapján, majd a SharePoint Online adminisztrációs felületén hozzá kell rendelnünk a publikus weboldalunkhoz a *Webhelytartományok* ikon segítségével, majd létrehozni a megfelelő DNS rekordokat a *DNS-adatok* ikon megnyomásával megjelenő ablakban látható információk szerint.



A publikus webhelyet a SharePoint vezérlőpultján nevezhetjük át

Belső, intranetes SharePoint webhelycsoportok esetén a szolgáltatás jelen verziójában sajnos nincs lehetőségünk saját domain név hozzárendelésére.

21.12.4 Migráció

Hivatalos Microsoft eszköz vagy módszer a szolgáltatás jelenlegi verziójában sajnos nem áll rendelkezésre, amellyel egy helyi SharePoint Server 2010 alapú webhelycsoportot át lehetne költöztetni a SharePoint Online szolgáltatásba, azonban számos külső gyártó készített szoftvereket, amelyek megkönnyítik az átállást.

Ezek közül a *Quest Migration Suite for SharePoint* már próbaverzióban is képes webhelyeket átköltöztetni, ugyanakkor az eredmény a legtöbb esetben kézi finomhangolást igényel, különösen a bonyolultabb intranetes oldalak esetében.

A szoftver a http://www.quest.com/migration-suite-for-sharepoint/ oldalról tölthető le.

21.13 Lync Online

A Lync Online a Microsoft felhőben hosztolt kommunikációs szoftvere, amelynek segítségével az azonnali üzenetek küldésén kívül lehetőségünk van hang- és videokonferencia szervezésére szervezeten belüli és kívüli felhasználók részvételével. Online bemutatókat, előadásokat tarthatunk, melyek során megoszthatjuk az asztalunk tartalmát, vagy egy programot, virtuális táblára rajzolhatunk, vagy éppen szavazást kezdeményezhetünk a résztvevők között.

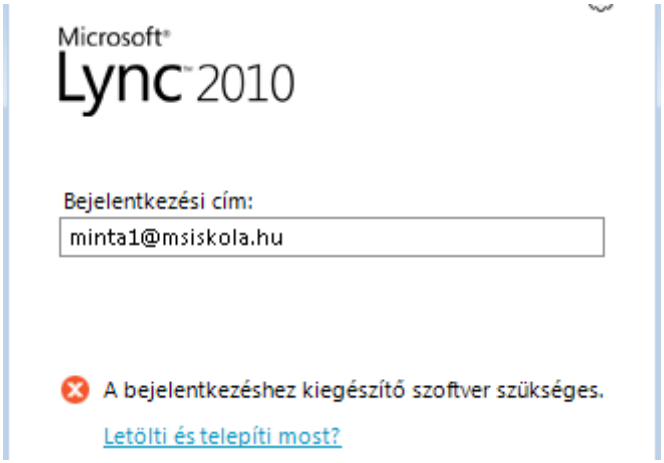
21.13.1 DNS beállítások

Ahhoz, hogy a kliensek a felhasználó azonosítója alapján automatikusan megtalálják a szolgáltatást nyújtó szervert, be kell állítanunk néhány DNS rekordot a domain nevünkön. A szükséges rekordok részletes leírását az Office 365 adminisztrációs felületének *Tartományok* oldalán találjuk meg, miután kijelöltük a domain nevünket, és a *DNS beállítások megtekintése* linkre kattintottunk a táblázat felett.

21.13.2 Klienstelepítés

A Lync azonnali üzenetküldési funkcióját már az Outlook Web App-ba való belépés után elérjük, a teljes funkcionalitást azonban csak az asztali alkalmazás feltelepítésével kaphatjuk meg. A letöltési link minden felhasználó számára elérhető az Office 365 *Kezdőoldal*án, ahol a *Lync* címsor alatt rögtön ott van a *Lync telepítése* hivatkozás.

Az első bejelentkezés előtt lehetséges, hogy telepítenünk kell a Microsoft Online Services Bejelentkezési segédet is. Ha így van, akkor a program értesíteni fog minket erről, és a letöltési linket is megjeleníti.



Le kell töltenünk a Bejelentkezési segédet

21.13.3 Kapcsolatok

Amikor először bejelentkezünk a rendszerbe, egy üres kapcsolati lista fog fogadni. Itt azonban a publikus üzenetküldőktől – amilyen például a Live Messenger – eltérően nem szükséges mások valamilyen azonosítóját tudni a kapcsolatfelvételhez. Egyszerűen kezdjük el írni a nevét a keresősávba, és a program a szervezetünk összes felhasználója között keres. A leggyakoribb kapcsolatainkat hozzáadhatjuk a kedvenceink listájához, így legközelebb már a kezdőképernyőn lesznek.

Az Office 365 adminisztrációs felületén keresztül elérhető Lync vezérlőpulton lehetőségünk van engedélyezni a külső partnerek felvételét is. Ilyenkor a felhasználók nem csak vállalaton belül kommunikálhatnak, hanem felvehetik a kapcsolatot más szervezetek Lync felhasználóival, sőt, akár Live Messenger felhasználókkal is. Várhatóan a jövőben a Skype felhasználók is kapcsolhatóak lesznek.

21.14 SSL tanúsítványok

Ahogyan azt az előző fejezetekben is láthattuk, manapság egyre több szolgáltatásnál nem csak elegáns, hanem elvárt és kötelező az SSL titkosított kapcsolat használata. Ennek megfelelően egyre több tanúsítványszolgáltató jelent meg a piacon, ami az árakat is lejjebb szorította, ennek ellenére sokan nem engedhetik meg maguknak a tanúsítvány éves költségét. Különösen igaz ez a közoktatási intézményekre.

21.14.1 Az ingyenes tanúsítványszolgáltatók – pro és kontra

Sok helyen találkozni az interneten különböző hirdetésekkel, melyek ingyenes tanúsítványt ígérnek. Ezek a helyek általában valóban ingyen adnak tanúsítványt, de a tanúsítvány csak akkor ér valamit, ha azt a másik fél megbízhatóként elfogadja. Azt pedig a legtöbb helyen már nem, vagy csak apró betűvel említik meg, hogy az általuk kibocsájtott tanúsítványt különösebb barkácsolás nélkül is megbízhatónak tekintik-e az egyes operációs rendszerek és böngészők.

A legtöbb ingyenes tanúsítvány használata esetén ugyanis a felhasználó egy ugyanolyan tanúsítványhiba figyelmeztetést fog látni, amikor felkeresi az oldalunkat, mintha egy önaláírt tanúsítványt használnánk. Legjobb tudomásom szerint jelenleg egyetlen olyan ingyenes tanúsít-

ványszolgáltató létezik, amelynek hitelességét a legtöbb operációs rendszer – köztük a Windows – minden beállítás nélkül elfogadja, ez pedig a StartSSL.

Természetesen az ingyenesség érdekében el kell fogadnunk bizonyos vállalható kompromisszumokat, mint például, hogy a tanúsítványokat csak díj ellenében vonják vissza. Részletes ismertető a http://startssl.com oldalon érhető el.

21.14.2 Regisztráció

A tanúsítványok igényléséhez regisztrálnunk kell magunkat a StartSSL oldalán.

1) Látogassunk el a http://startssl.com weboldalra, és kattintsunk a bal felső sarokban található *Sign-up* feliratú képre.

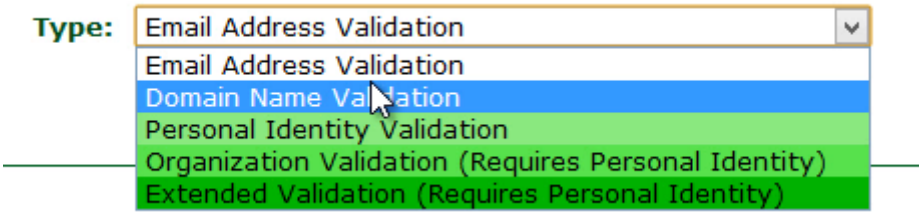
Az oldal több nyelven is elérhető – magyarul sajnos egyelőre nem

2) Töltsük ki a megjelenő űrlapban az adatainkat. Minden mező kitöltése kötelező.
3) A *Continue* gombra kattintva elfogadjuk a felhasználási feltételeket, amelyeket érdemes valóban megnézni, különösen, ha cég számára szeretnénk tanúsítványt igényelni.
4) E-mailben kapunk egy regisztrációs kódot, amit a következő oldalon meg kell adnunk.
5) Ezután az oldal generál számunkra egy privát kulcsot. Ez a generálás valójában a saját számítógépünkön történik, így a privát kulcs nem kerül ki a gépünkről eközben sem. Így ez eltarthat néhány másodpercig.
6) Következő lépésben telepítenünk kell a most generált kliensazonosító tanúsítványt a számítógépünkre. Az Install gomb megnyomásával ez automatikusan megtörténik.
7) Ezt a tanúsítványt **erősen ajánlott** exportálni, és egy biztonságos helyen tárolni, mivel a jövőben ezzel léphetünk be a StartSSL oldalára, és ezzel adminisztrálhatjuk a későbbiekben igényelt többi tanúsítványunkat. Úgy kell elképzelnünk ezt a kliens tanúsítványt, mint a felhasználói nevünket és jelszavunkat. Az exportáláshoz instrukciókat a *FAQ* oldalon találunk.

21.14.3 Domain név ellenőrzése

A regisztráció befejeztével a *Control Panel* oldalra kerülünk. A tanúsítványigénylés a StartSSL-nél a következő módon működik: először igazolnunk kell annak a domain névnek a tulajdonjogát, amelyre a tanúsítványt igényelni szeretnénk. Az igazolás a *postmaster*, *webmaster* vagy *hostmaster@domainnév* címre küldött ellenőrző kód segítségével történik teljesen automatizált módon. Egy igazolás 30 napig érvényes, ezen idő alatt bármennyi tanúsítványt igényelhetünk erre a domainre.

1) A *Control Panel* oldalon kattintsunk a *Validations Wizard* fülre.
2) A *Type* mezőben válasszuk a *Domain Name Validation* lehetőséget



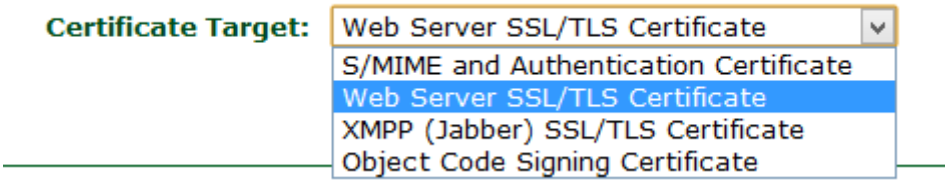
A többi hitelesítési módszer nagyobb biztonságú, „fizetős" tanúsítványhoz szükséges

3) A következő oldalon adjuk meg a domain nevet, amit ellenőrizni szeretnénk.
4) Válasszuk ki, hogy a három lehetőség közül melyik e-mail címre küldje a rendszer az ellenőrzőkódot.
5) A kapott e-mailből másoljuk be a kódot az oldalon látható mezőbe. Ezzel az ellenőrzés megtörtént.

21.14.4 Tanúsítványigénylés

Maga a tanúsítványigénylés történhet tanúsítványkérelemből, amit valamilyen program, például IIS generál, vagy történhet teljesen önállóan, ilyenkor a privát kulcsot a böngésző generálja, hasonlóan a regisztrációkor generált kliens tanúsítvány privát kulcsához.

1) Készítsük el a tanúsítvány kérelmünket a kívánt programmal. Végeredményként általában egy .req kiterjesztésű fájlt kapunk.
2) A StartSSL Control Panel oldalán kattintsunk a *Certificates Wizard* fülre.
3) A *Certificate Target* listából válasszuk a *Web Server SSL/TLS Certificate* lehetőséget (feltételezve, hogy IIS vagy bizonyos Exchange szolgáltatásokhoz igényeljük a tanúsítványt)



A Web Server tanúsítvány nem csak webszerverhez használható

4) Mivel a tanúsítványt kérelemből fogjuk igényelni, ezért a következő oldalon a privát kulcs generálását ki kell hagynunk. Kattintsunk a *Skip* gombra.
5) Nyissuk meg egy szövegszerkesztő programmal (pl. a Jegyzettömb tökéletesen megfelelő) a kérelem generálásakor kapott .req fájlt, és az elejétől a végéig jelöljük ki, majd másoljuk be a StartSSL *Submit Certificate Request* oldalán található mezőbe. Ügyeljünk rá, hogy véletlenül se módosítsuk a kódot, egyetlen szóköz is hibát okozhat.
6) A következő oldal tájékoztat, hogy a kód feltöltése sikeres volt, és most újból meg kell majd adnunk az adatokat.
7) A *Continue* gombra való kattintás után válasszuk ki azt a domaint, amihez a tanúsítványt igényelni szeretnénk. A listában csak azok a domainek jelennek meg, amit az elmúlt 30 napban érvényesítettünk.

8) Írjuk be, hogy milyen harmadszintű domaint szeretnénk a tanúsítványhoz hozzáadni. Megadhatjuk például a www-t, ilyenkor, ha az msiskola.hu domainhez igénylünk tanúsítványt, akkor az érvényes lesz a www.msiskola.hu és az msiskola.hu címekre is.
9) A következő oldalon egy összefoglalót olvashatunk a megadott adatokról. A *Continue* gombra kattintva benyújthatjuk a kérelmet.
10) Ha ez az első tanúsítványkérelmünk, akkor az aláírt tanúsítványt nem kapjuk meg azonnal, előtte a StartSSL munkatársai manuálisan ellenőrzik a megadott adatokat. A második kérelemtől kezdve azonban ilyenkor rögtön megkapjuk a tanúsítványt. Másoljuk ki a kapott kódot a mezőből, illesszük be egy szövegszerkesztőbe, és mentsük el .cer kiterjesztéssel. Ezt a fájlt importáljuk a szerveren a tanúsítványaink közé.
11) Végül minden esetben exportáljuk a kapott tanúsítványt a privát kulccsal együtt, és tároljuk biztos helyen!