Debreceni Egyetem

Informatika Kar

WINDOWS SZERVER 2008 HÁLÓZATI MEGOLDÁSAI

Témavezető:
dr. Krausz Tamás
Egyetemi adjunktus

Készítette:
Fazekas Ádám János
Programtervező
Informatikus

Debrecen

2009

Tartalomjegyzék

Bevezetés

A mai világban szinte el sem lehet képzelni egy munkahelyet számítógépek, számítógép-hálózatok és internet-hozzáférés nélkül. A munkáltatók és alkalmazottak számára mindennapos dolog, hogy feladataik elvégzéséhez igénybe vesznek különböző erőforrásokat, szolgáltatásokat amelyek földrajzilag akár teljesen más helyen is létezhetnek mint ahol ők éppen tartózkodnak, ezért elengedhetetlen egy korszerű vállalat számára, hogy megteremtse azokat a feltételeket amelyek segítségével a hálózati kommunikáció és szolgáltatások biztonságosan és hatékonyan megvalósíthatók.

A Microsoft cég következő generációs szerver operációs rendszere, a Windows Server 2008, éppen ezt a célt szolgálja, szilárd alapot biztosít a hálózati infrastruktúra kialakításához, magas rendelkezésre állás és kiemelkedő biztonság mellett.

Egy piacvezető cég számára az is fontos, hogy lépést tartson a mai korszerű technikával, ki tudja használni az egyre nagyobb teljesítményű hardvereszközöket, korszerű módszerekkel védje a hálózat egyes erőforrásait vagy éppen megpróbálja csökkenteni a kiadásait például fejlettebb energiagazdálkodási lehetőségekkel. A Windows Server 2008 számos olyan újdonságot vezet be amellyel mindezek kivitelezhetőek.

Azért választottam a Windows Server 2008-at a szakdolgozatom témájaként, mert úgy gondolom, hogy megfelelő kiindulópont az egyetemi tanulmányaim alatt megszerzett hálózati ismereteim kiszélesítésére, és néhány korszerű technológia megismerésére. A dolgozatom célja, hogy ismertessek néhány olyan új technológiát, amelyet a Windows Server 2008 kiszolgáló operációs rendszer vezet be.

A Windows Server 2008 termékcsalád

A Windows Server 2008 csakúgy mint elődei, a különböző igények kielégítése érdekében több termékváltozat formájában jelenik meg. A Windows Server 2008 termékcsaládnak 5 különböző tagja van, de ezek közül 3 a Hyper-V technológia nélkül is elérhető, ezért tulajdonképpen 8 változatról beszélhetünk. A következőkben ezeket szeretném bemutatni:

Windows Server 2008 Standard Edition:
Ez a változat a hálózaton belüli további rendszerek számára biztosít erőforrásokat, számos funkcióval és beállítási lehetőséggel rendelkezik. A rendszer eszközei segítségével a kiszolgálók hatékonyan ellenőrizhetők, a konfigurációs és felügyeleti feladatok pedig egyszerűen elláthatók. A SE lehetővé teszi az egyidejű folyamatok két vagy négy utas szimmetrikus feldolgozását, valamint a 32 bites rendszerekben legfeljebb 4 gigabyte, a 64 bites rendszerekben legfeljebb 32 gigabyte memória használatát.

Windows Server 2008 Enterprise Edition:
Nagyvállalati felhasználásra alkalmas platformot biztosít az üzleti szempontból kritikus fontosságú alkalmazások számára. Az Enterprise kiadás a SE szolgáltatásait egészíti ki, jobb skálázhatóságot és rendelkezésre állást biztosítva. A magas rendelkezésre állást segítik a fürtszolgáltatások és a processzorok működés közbeni telepítésének lehetősége. Az összevont identitáskezelői funkciók pedig fokozzák a rendszer biztonságát. A kiadás támogatja a melegcserére alkalmas RAM-okat és a nem egységes memória-hozzáférést(Non-Uniform Memory Access). 32 bites rendszereken 32 gigabyte memóriát, 64 bites rendszereken 2 terabyte RAM memóriát és 8 processzort képes kezelni.

Windows Server 2008 Datacenter Edition:
A nagyarányú virtualizációhoz és vertikálisan méretezhető munkaterhelésekhez ideális operációs rendszer. A licence korlátlan virtualizációs jogosultságot

biztosít, tehát korlátlan számú Windows Server vagy egyéb típusú kiszolgáló futtatható rajta. Fejlett fürtöző szolgáltatást kínál, és támogatja a nagy memóriás konfigurációkat. 32 bites rendszereken 64 gigabyte, 64 bites rendszereken 2 terabyte RAM memóriát képes kezelni, és képes akár 64 darab processzor kezelésére is.

Windows Web Server 2008:

Kifejezetten egy feladatra tervezték, webes alkalmazások és szolgáltatások kiszolgálása, ezért más szolgáltatásokat nem is tartalmaz, nem lehet például DNS vagy Active Directory tartományvezérlő.

A kiadás része a Microsoft .NET keretrendszer, a Microsoft Internet Information Services(IIS) 7.0 kiszolgáló és az ASP.NET technológia. Mindezek segítségével bármely vállalat vagy szervezet egyszerűen beüzemelheti a weblapjait, webalkalmazásait vagy webszolgáltatásait.

Ez a kiadás 32 bites rendszer esetén legfeljebb 4 gigabyte RAM memóriát, 64 bites rendszer esetén pedig maximum 32 gigabyte memóriát képes kezelni.

Windows Server 2008 for Itanium-Based Systems:

Nagy teljesítményt, megbízhatóságot és méretezhetőségi lehetőségeket nyújt, nagyméretű adatbázisok és üzleti célú alkalmazások kiszolgálására optimalizálták. Magas rendelkezésre állás mellett akár 64 processzor kezelésére is képes, nagy erőforrás-igényű és kritikus fontosságú feladatok elvégzésére.

A Standard, Enterprise és Datacenter kiadások elérhetők a Hyper-V virtualizációs technológia nélkül is, ezek megegyeznek a fent említettekkel leszámítva ezt a szolgáltatást.

A Standard, Enterprise és Datacenter kiadásokban elérhető a Server Core telepítési funkció, az Itanium és Web Server kiadásokban nem. A Server Core nem alkot önmagában önálló kiadást, csak egy szerepkör amit ezen kiadások támogatnak.

A Windows Server 2008 Újításai

A Windows Server 2008 számos újdonságot tartalmaz a korábbi Windows Server kiadásokhoz képest. Forradalmian új architektúrával rendelkezik, amely segíti a vállalatok, szervezetek működésének hatékonyabbá tételét, az üzleti eszközök és erőforrások felügyeletét és irányítását valamint a hálózati infrastruktúra biztonságosabbá tételét. Fejlett energiagazdálkodási technológiával rendelkezik, a kívánt teljesítmény eléréséhez optimalizálja az energiafogyasztást, aminek segítségével hozzájárul a vállalat költségeinek a csökkentéséhez. Maximális irányítási lehetőséget biztosít a rendszergazdák számára az infrastruktúra felett, ugyanakkor kimagasló rendelkezésre állást és felügyeleti lehetőséget kínál. A felvonultatott új technológiák segítségével egy minden eddiginél biztonságosabb, robusztusabb és megbízhatóbb kiszolgálói környezetet valósít meg. Ezek közül az új technológiák közül szeretnék néhányat bemutatni és később részletesebben is elemezni.

A Microsoft a Windows Server 2008-al egy teljesen új szintre emelte a hálózati biztonság fogalmát, az olyan új technológiák segítségével, mint például a Network Access Protectiont, amellyel korlátozni lehet, hogy mely gépek férhetnek hozzá a hálózathoz és melyek nem, a BitLocker technológia, melyel szektor szinten tudjuk titkosítani a számítógép köteteit vagy az írásvédett tartományvezérlők megjelenítése, aminek a segítségével megvédhetők a tartományvezérlők az illetéktelen módosításoktól például egy kihelyezett telephelyen, ahol a fizikai biztonság nem megfelelő.

Megjelenik egy új virtualizációs technika a Hyper-V, a Microsoft hypervisor alapú hardver virtualizációs technikája. Amely teljes egészében integrált a Windows Server 2008-al, annak egy szerepköreként telepíthető.
A Hyper-V egy type1-es(bare metal) hypervisor megoldás, ami annyit jelent, hogy a hypervisor közvetlenül a hardveren fut, és onnan szolgálja ki a virtuális gépek erőforrásigényeit.

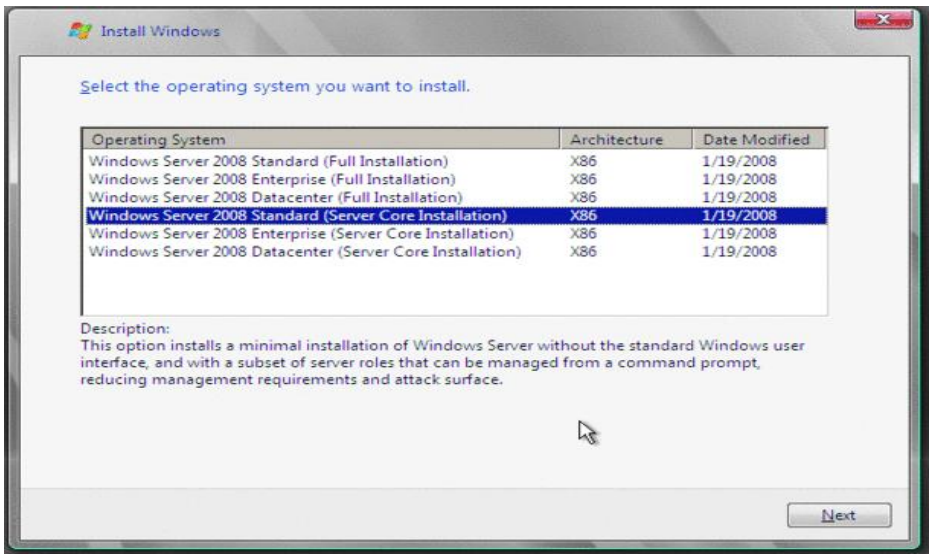
A Windows Server 2008 egy vadonatúj webkiszolgáló rendszerrel lett ellátva, amelynek neve Internet Information Services 7(IIS7). Az IIS7 még nagyobb biztonságot nyújt mint elődje, moduláris felépítésének köszönhetően. Csak azok a komponensei telepítődnek fel a gépre, amelyek szükségesek a neki szánt feladatkör elvégzéséhez, így még kevesebb támadási felületet nyújt a támadók számára. Egy hatékony és rugalmas webkiszolgálót alakíthatunk ki, amely segítségével közzétehetjük weboldalainkat, webalkalmazásainkat vagy webszolgáltatásainkat.

Természetesen még számtalan más új technológia is megjelenik ezzel az operációs rendszerrel kapcsolatban, de a dolgozat terjedelme miatt próbáltam azokat összeválogatni, amelyek talán a legfontosabbak a mai igényeknek megfelelően.

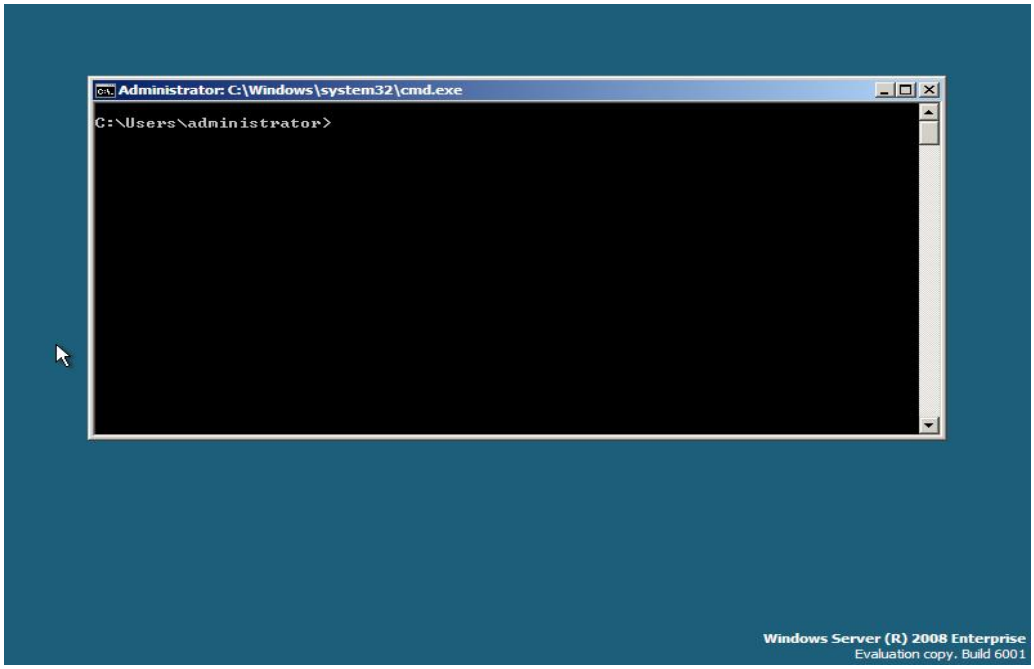
A Windows Server 2008 kódbázisa megegyezik a személyi számítógépeken használatos Windows Vista operációs rendszerrel, ezért ajánlatos ezt a rendszert használni a kliens számítógépeken a leghatékonyabb működés elérése érdekében. Ha a két terméket együtt használjuk számos fejlesztéssel találkozhatunk, amelyeknek köszönhetően javul a biztonság, a kezelhetőség, a rendszer általános teljesítménye, az akadályok nélküli tervezés és a telepítési folyamat.

Server Core

Már a telepítés során szembesülünk egy új opcióval, az úgynevezett Server Core telepítési változattal, melynek lényege, hogy az installáció során nem települ a grafikus felhasználói felület és az ehhez kapcsolódó funkciók, ezért a rendszer szinte teljes mértékben csak parancssori környezetben üzemeltethető(néhány elem a grafikus felületből azért megmarad, például a jegyzettömb és a Területi és nyelvi beállítások menü). Ennek a kiszolgálóverziónak is megvannak az előnyei és a hátrányai, előny, hogy lényegesen csökken a rendszer működéséhez szükséges hardverkövetelmény, kevesebb támadási felület lesz a rendszeren és kevesebb frissítést kell telepíteni. A hátránya, hogy mindezekért cserébe néhány dologról le kell mondanunk, csak 7 szerepkört képes ellátni, kevesebb funkciót és komponenst tartalmaz(ezt akár előnynek is felfoghatjuk, mivel ha kevesebb alkalmazás fut a szerveren kevesebb is tud elromlani), és néhány feladat elvégzése bonyolultabbá válik a parancssoros kezelőfelület miatt.
A Core verzió telepítése nem sokban különbözik a normál verzióétól, mindössze a megfelelő helyen a Server Core telepítési lehetőséget kell választanunk:



Miután sikeresen végeztünk a telepítési folyamattal a következő képernyő fogad minket:



Innentől kezdve majdnem minden feladatot parancssor segítségével kell megoldanunk.

Mielőtt megadnánk a kiszolgálónk által betöltendő szerepkört, először el kell végeznünk néhány alapbeállítást, mint például dátum és idő, számítógépnév és hálózati kapcsolat beállításai. Ezeket a következő módon tehetjük meg:

A Dátum és idő beállítások menü egyike a grafikusan is elérhető felületeknek, a következő parancs kiadásával: *Control timedate.cpl*

A Területi és nyelvi beállítások menü is elérhető grafikusan, a *Control intl.cpl* parancs használatával.

A számítógép nevének megváltoztatásához először kérjük le a jelenlegi nevét a *hostname* parancs kiadásával. Majd ezután megadhatjuk neki az új nevet a következő képen: *netdom renamecomputer <réginév> /newname:<újnév>*

Az IP cím beállítás a következő módon történik, ha például statikus IP-címet szeretnénk adni a gépnek, ami 192.168.0.99, alapértelmezett maszkkal, 192.168.0.1 átjáróval:

netsh interface ipv4 set address name="10" source="static"
address=192.168.0.99 mask=255.255.255.0 gateway=192.168.0.1

Ha végeztünk az alapbeállításokkal, akkor rendelhetünk szerepkört a kiszolgálóhoz.
A Core verzió a következő szerepköröket támogatja:

- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- DHCP Server
- DNS Server
- File Services
- Print Services
- Web Services

Az *oclist* parancs kiadásával ki tudjuk listázni, hogy a szerverünkön jelenleg milyen szerepkörök és képességek vannak telepítve.
Amennyiben a DHCP Server szerepkört szeretnénk feltelepíteni, akkor azt a *ocsetup DHCPServerCore* parancs segítségével egyszerűen megtehetjük. Szolgáltatások törlése a */uninstall* kapcsoló segítségével lehetséges, például *ocsetup DHCPServerCore /uninstall.*
A utasítások túlnyomó többsége megegyezik a korábbi Windows Server verziók parancssori utasításaival, így aki rendelkezik korábbi tapasztalatokkal egyszerűen eligazodik a rendszeren. Ha elvégeztük a szükséges beállításokat a szerveren, akkor lehetőségünk van távoli vezérlésre is, például távoli asztali kapcsolat használatával.
Ez a telepítési mód számos esetben hasznosnak bizonyulhat, amikor nincs feltétlenül szükségünk a grafikus felhasználói felület előnyeire.

Server Manager

A grafikus felület is számos újdonságot tartalmaz, ilyen például a Server Manager amely tulajdonképpen az egész rendszer központi komponense, itt egy egységes képet kapuk a szerverünk állapotáról, szerepköröket és képességeket telepíthetünk vagy távolíthatunk el a rendszerről, telepíthetjük a legújabb frissítéseket és módosíthatjuk a biztonsági beállításokat. Ez az eszköz tulajdonképpen a Windows Server 2003-ban megismert Manage Your Server és Security Configuration Wizard ötvözete amely egy logikusan felépített kezelőfelületet nyújt a rendszergazdának a szerver főbb funkcióinak a kezelésére.

A telepítés után a kiszolgálón alapértelmezés szerint semmilyen funkció nem szerepel, az üzemeltetőknek kell eldönteniük, hogy mit várnak el a rendszertől, milyen szolgáltatást kívánnak nyújtani a kiszolgáló segítségével, és ennek megfelelően kell szerepkört, szerepkör-szolgáltatást és képességet telepíteni a Server Manager segítségével.

Kiszolgálói szerepkör(Server Role): A kiszolgálói szerepkörök olyan szoftverösszetevők, amelyek lehetővé teszik, hogy a kiszolgáló egy meghatározott feladatot lásson el a hálózaton. Egy szerver lehet egyfunkciós is, de betölthet több szerepkört is.

Szerepkör-szolgáltatás(Role Services): A kiszolgálói szerepkörhöz szükséges funkciókat biztosítják, a legtöbb szerepkörhöz tartoznak szerepkör-szolgáltatások is, amelyek kapcsolatban állnak egymással. Azokhoz a szerepkörökhöz amelyek csak egy szolgáltatást látnak el, a telepítés során automatikusan ez a szolgáltatás is a kiszolgálóra kerül, más szerepkörökhöz több telepíthető szolgáltatás is kapcsolódik, ezek közül kiválaszthatjuk, hogy melyiket szeretnénk telepíteni.

Képesség(Feature): A képességek olyan rendszerkomponensek amelyek önmagukban nem határozzák meg a kiszolgáló szerepét, csak kiegészítő funkciókat nyújtanak. A szerepköröktől és szerepkör-szolgáltatásoktól függetlenül telepíthetőek és távolíthatóak el, beállítástól függően akár több

képességet is telepíthetünk, vagy akár egyet sem.

A szerepkörök, szerepkör-szolgáltatások és képességek között kapcsolat, függőség állhat fent, ezért telepítés és eltávolítás esetén előfordulhat, hogy más szerepköröket, szerepkör-szolgáltatásokat vagy képességeket is telepítenünk vagy törölnünk kell, ilyenkor a Server Manager figyelmeztet a függőségi viszonyra.

A Windows Server 2008 a következő szerepköröket támogatja:

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory FederationServices
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- DHCP Server
- DNS Server
- Fax Server
- File Services
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Terminal Services
- Universal Description Discovery Integration Services
- Web Server(IIS)
- Windows Deployment Services
- Windows Sharepoint Services

Active Directory

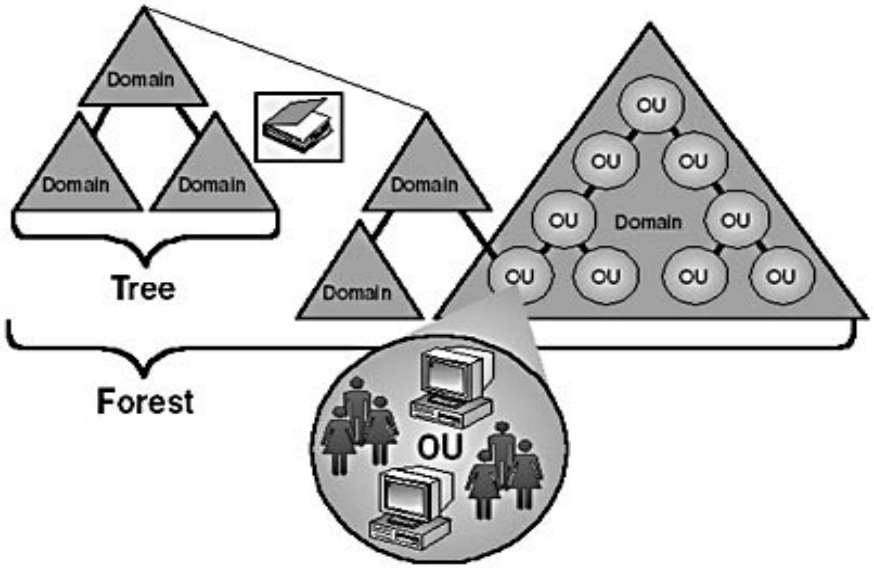
Az Active Directory lehetővé teszi a hálózat számítógépeinek központosított felügyeletét, házirendek előírását felhasználói vagy számítógép csoportok számára és alkalmazások központi telepítését. A hálózat objektumairól tárol információkat, amelyek lehetnek erőforrások, szolgáltatások, felhasználói fiókok vagy csoportok. Minden objektum egyedi névvel rendelkezik, és minden objektumhoz tulajdonságok, attribútumok tartoznak. Egyes objektumok más objektumokat tartalmazhatnak, ezeket konténereknek nevezzük. Azt hogy az Active Directory(AD) milyen objektumokat tartalmazhat, és azok hogyan épülnek fel az AD sémája határozza meg. A séma objektumosztályokból és attribútumokból áll, az objektumosztályok adják meg hogy milyen objektumokat tartalmazhat az AD, minden objektum egy objektumosztályhoz tartozik, az attribútumok pedig azt mondják meg, hogy az egyes objektumok milyen információkat tárolnak. Például a User objektumnak rendelkeznie kell vezetéknév, keresztnév, telefonszám stb. attribútumokkal. Egy séma bővíthető új osztályokkal és attribútumokkal, de körültekintőnek kell lenni, mert a sémár érő változások kihatnak a teljes hálózatra.
Az Active Directory rendelkezik logikai és fizikai struktúrával is, a logikai struktúra segítségével rendszerezhetők a címtár objektumok és könnyebben kezelhetők a hálózati fiókok és megosztott erőforrások, a fizikai struktúra pedig lehetővé teszi a hálózati kommunikációt és biztosítja a hálózati erőforrások fizikai kereteit.

Logikai struktúra:

- **Tartományok(Domains):** Számítógépek egy csoportja, melyek közös címtáradatbázissal rendelkeznek.
- **Szervezeti egységek(Orgnization Unit):** Tartományok egy alcsoportja, amely gyakran tükrözi egy cég vállalati vagy működési struktúráját.
- **Tartományfák(Domain Tree):** Egy vagy több tartomány, amelyek közös összefüggő névtérrel rendelkeznek. Tartományhierarchiát alkot, ahol a

szülő és gyermektartományok között bizalmi kapcsolat áll fent.

- **Tartományerdők(Domain Forest):** Egy vagy több tartományfa, amelyek közös címtár-információval rendelkeznek. A tartományerdőben lévő tartományfák között bizalmi kapcsolat áll fent.



Bizalmi kapcsolat: Kétirányú tranzitív bizalmi kapcsolat tartományok között, vagy egy fában vagy két vagy több fa között egy erdőben. A kétirányú bizalmi kapcsolat azt jelenti, hogy mindkét fél hozzáférést biztosít az erőforrásaihoz a másik fél számára. A tranzitivitás pedig azt jelenti, hogyha a D1 tartomány kétirányú bizalmi kapcsolatban áll a D2 tartománnyal és D2 pedig D3 is, akkor D1 is kétirányú bizalmi kapcsolatban áll D3-al.

Fizikai struktúra:

- **Helyek(Sites):** Számítógépek egy olyan csoportja, amelyek magas sávszélességű kapcsolatban állnak összeköttetésben. Nincs összefüggés a helyek és a tartományok között, egy helynek lehet több tartománya de egy tartomány akár le is fedhet több helyet. Egy hely egy vagy több alhálózatból áll. Az Active Directoryban hely-objektumként szerepelnek.
- **Tartományvezérlők(Domain Contorllers):** Olyan szerverek amelyek Active Directory szolgáltatásokat nyújtanak klienseknek vagy felhasználóknak. Rendelkeznek az Active Directory adatbázisának egy

másolatával. Mivel a Windows Server 2008 a többforrású replikációs modellt követi, nincs alá- fölérendeltségi viszony a replikációs partnerek között, ezért bármely tartományvezérlő kezdeményezhet replikációs folyamatot az adatbázisát ért változás miatt.

- **Globális katalógus(Global Catalog):** Egy szerepkör, amelynek feladata, hogy információt tároljon minden tartomány minden objektumáról. A saját tartományuk címtárában lévő objektumokat teljesen replikálják, a tartományerdő további tartományaiban szereplő objektumokat részlegesen replikálják, a hálózati terhelés és az adatbázis méretének csökkentése érdekében. A globális katalógusban nagyon hatékonyan lehet keresni, mivel a címtárkeresési kéréseket a hálózat egy másik tartománya helyett a helyi tartomány kezeli.

Replikáció: A címtáradatok terjesztésére szolgáló eljárás. A tartományadatok egy adott tartományon belül minden tartományvezérlőhöz replikálódnak. A címtáradatok bármilyen változását a rendszer a tartomány összes tartományvezérlőjére replikálja.

Műveleti főkiszolgáló szerepkör(Flexible Single Master Operation): Kizárólag egy-egy kitüntett tartományvezérlőn fordulhatnak elő. Feladatuk az egységesség biztosítása, a címtár ellentmondásos(ütköző) részeinek a megszüntetése, és az olyan feladatkörök elvégzése, amelyekhez a normál tartományvezérlőknek nincsen jogosultságuk, mint például a séma-frissítés, amelyet a Schema Master szerepkörrel rendelkező műveleti főkiszolgáló képes elvégezni.

Active Directory szerepkörök a Windows Server 2008-ban

A Microsoft a Windows Server 2008 fejlesztése közben több fontos változtatást vezetett be az Active Directory szolgáltatásokkal kapcsolatban. Ezek alapja, hogy át lett szervezve a címtár működése, és egy új szolgáltatáscsalád jött létre, amely számos rokon szolgáltatást tartalmaz.

Ezek a következők:

- Active Directory Domain Services
- Active Directory Certificate Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services

Az új szerepkörökön kívül megjelenik egy teljesen új tartományvezérlő-típus az írásvédett tartományvezérlő(Read-Only Domain Controller), valamint lehetőség újraindítható címtárszolgáltatás készítésére.

Active Directory tartományi szolgáltatások(AD Domain Services)

Az Active Directory tartományi szolgáltatások kiszolgálói szerepkört használva egy felhasználó és erőforrás kezeléshez méretezhető biztonságos infrastruktúrát hozhatunk létre, amely támogatja az olyan címtárbarát alkalmazásokat is mint például a Microsoft Exchange Server.

Egy olyan elosztott adatbázist használ, amely a hálózat objektumairól tárol és tesz elérhetővé információkat. Lehetőséget ad a hálózati elemek hierarchikus struktúrába rendezésére, mely struktúra az AD erdőből, az erdő tartományaiból és a tartományokban található szervezeti egységekből áll, megkönnyítve ezáltal hatáskörök delegálását és nagyszámú objektum kezelését.

A megfelelő biztonságot a bejelentkezési hitelesítés és a címtárban található erőforrások hozzáférés-szabályozása biztosítja. A hálózati felhasználók és számítógépek részére az Active Directory tartományvezérlői biztosítanak hozzáféréseket az engedélyezett hálózati erőforrásokhoz.

Active Directory tanúsítványszolgáltatások(AD Certificate Services)

A nyilvános kulcsú technológiát alkalmazó szoftverbiztonsági rendszerekben használt nyilvánoskulcs-tanúsítványok kiállításához és kezeléséhez biztosítanak testreszabható szolgáltatásokat.

Biztosítja a digitális tanúsítványoknak a felhasználók, ügyfelek, számítógépek és kiszolgálók részére történő kibocsátásához és visszavonásához szükséges

funkciókat, tanúsítványszolgáltatók(Certificate Authority) segítségével, amik felelősek a tanúsítványok kibocsájtásáért és érvényességének ellenőrzéséért. A tartományokban találhatunk úgynevezett vállalati gyökér-tanúsítványszolgáltatókat, amelyek a tartományi tanúsítványhierarchia gyökerénél helyezkednek el, ezek a vállalat legmegbízhatóbb tanúsítványkiszolgálói, valamint alárendelt tanúsítványszolgáltatókat, amelyek egy adott vállalati tanúsítványhierarchia tagjai.

További szerepkör-szolgáltatások még a webalapú tanúsítvány igénylés(CA Web Enrollment), amely segítségével a felhasználók webböngészőből kapcsolódhatnak a tanúsítványszolgáltatóhoz, tanúsítvány igénylés vagy visszavonás céljából. Az Online válaszadó szolgáltatás(Online Responder Service), amely Online Certificate Status Protocoll alapján dekódolja az adott tanúsítvány visszavonási állapotának lekérdezéseit, kiértékeli a tanúsítvány állapotát, majd visszaküldi a kért információt a tanúsítván állapotáról egy hitelesített üzenetben. A hálózati eszközök tanúsítványigénylési szolgáltatása(Network Device enrollment Service), amely lehetővé teszi forgalomirányítók és egyéb hálózati berendezések számára tanúsítványok beszerzését, Simple Certificate Enrollment Protocoll alapján.

Active Directory egyesített szolgáltatások(AD Federation Services)

Az egyesített szolgáltatások segítségével nagymértékben kiterjeszthető, internetre méretezhető és biztonságos hozzáférést nyújtó megoldást hozhatunk létre, amely többféle platformon, windows és nem windows-alapú környezetben is működik.

Az AD tartományi szolgáltatások hitelesítési és hozzáférés-kezelési szolgáltatásait egészíti ki azzal, hogy kiterjeszti a szolgáltatásokat a világhálóra. Hozzáférést biztosít egy vagy több védett, internetes felülettel rendelkező alkalmazáshoz, még akkor is, ha a felhasználói fiókok és az alkalmazások teljesen más hálózatokban vagy szervezetekben találhatóak.

Az AD egyesített szolgáltatások szerepkör tartalmaz összevonási, proxy-, és webügynök-szolgáltatásokat.

Az adott követelményektől függően a következő szerepkör-szolgáltatásokat lehet üzembe helyezni a rendszeren:

Egyesített szolgáltatás: Egy vagy több közös megbízhatósági házirenddel rendelkező kiszolgálót von össze.

Egyesített szolgáltatás proxy: A kérelmeket az egyesítési szolgáltatásnak továbbító, külső hálózatban elhelyezett proxy. Feladata a felhasználói hitelesítő adatok összegyűjtése, és a hitelesítési információk továbbítása az egyesített szolgáltatásnak.

Jogcímbarát ügynök(Claimsaware Agent): Lehetővé teszi jogcímbarát alkalmazásokat futtató kiszolgálók számára az AD egyesített szolgáltatások jogcímeinek lekérdezését.

Active Directory egyszerű címtárszolgáltatások(AD Lightweight Directory Services)

Az AD LDS, korábbi nevén Active Directory Application Mode(ADAM), egy Lightweight Directory Access Protocol(LDAP) alapú címtárszolgáltatás, amely adattárat biztosít a címtárak kezelésére képes alkalmazások számára, az AD tartományi szolgáltatásokban megkövetelt függőségek nélkül. Működése hasonló az AD DS-hez, csak nincsen szüksége tartományok vagy tartományvezérlők telepítésére. Nem az operációs rendszer szolgáltatásaként fut, és használható mind tartományi mind munkacsoport környezetben. Egy kiszolgálón az AD LDS több példánya is futtatható egyszerre, ekkor minden AD LDS-példányhoz egymástól függetlenül kezelhető séma tartozik.

Ehhez a szerepkörhöz nem tartoznak szerepkör-szolgáltatások.

Active Directory tartalomvédelmi szolgáltatások(AD Rights Management Services)

Az AD RMS egy információvédelmi megoldások létrehozására alkalmas szolgáltatásokat biztosító alkalmazásfüggetlen technológia. Adatok védelmére szolgál, és lehetővé teszi különböző dokumentumok, e-mailek, intranetes webhelyek és egyéb tartalmak védelmét jogosulatlan hozzáféréssel szemben. A megbízható felhasználókat, csoportokat tartalomvédelmi fióktanúsítványokkal

azonosítja, melynek segítségével hozzáférhetnek a védett tartalmakhoz. A különböző védett tartalmakhoz jogosultságok rendelhetők, amelyek meghatározzák, hogy mely felhasználók vagy csoportok férhetnek hozzá az információhoz és mire használhatják azokat(például olvasás, módosítás vagy nyomtatás). Tehát a használati jogok magukba a dokumentumokba vannak zárva. Titkosítással biztosítja, hogy a felhasználók a védett adatokat a vállalaton kívül és belül is csak ellenőrzött formában érhessék el.
Bármely alkalmazás alkalmassá tehető az AD RMS használatára, és más kiszolgálók is beállíthatók úgy, hogy a kényes információk védelme érdekében együttműködjenek az AD RMS rendszerrel.

Írásvédett tartományvezérlő(Read-Only Domain Controller)

A címtár tartományvezérlőkön keresztül valósul meg, ezek adminisztrálják és tárolják a címtár adatait, emiatt sok ügyfelet kell kiszolgálniuk, gyakran nem csak a lokális hálózaton belülről, hanem például külső telephelyekről érkező igényeket is, és mivel igen kényes adatokat is tárolnak, mint például felhasználónevek, jelszavak, garantálni kell a biztonságukat is.
Az írásvédett tartományvezérlők olyan kiegészítő tartományvezérlők, amelyek csak olvasható másolatot tartalmaznak az Active Directory adattáráról. Ezért ideálisak az összes tartományvezérlői feladat ellátására, olyan helyeken, ahol a tartományvezérlő fizikai biztonsága nem megfelelő, például egy védett szerverszobát nélkülöző telephelyen. Ha például megpróbálják az adott szervert feltörni vagy eltulajdonítani, nem férhetnek hozzá kritikus adatokhoz(például jelszavakhoz), mivel helyben ezek alapértelmezés szerint nem tárolódnak, és nem tudják illetéktelenek módosítani a címtár adatait sem, megelőzve ezzel az egész erdőt negatívan érintő adatbázis változásokat.
Az írásvédett tartományvezérlők a jelszavak kivételével ugyan azokat az objektumokat és attribútumokat tartalmazzák, mint írható társaik. Változásokat azonban nem tárolhatja el, még a szükségeseket sem, így egy kérelmet kell küldeni egy írható tartományvezérlőhöz, amely képes végrehajtani a kért módosításokat, majd egy frissítést követően visszakerülnek a módosítások a

RODC címtár példányába, ez egy egyirányú replikáció.
Mivel ez a tartományvezérlő típus alapértelmezés szerint a saját számítógépfiókja és a Kerberos Target(krbtgt) fiók kivételével semmilyen más hitelesítési adatokat vagy jelszavakat nem tárolnak, ezért a felhasználókat és számítógépeket hitelesítő adatokat az írható tartományvezérlőkről töltik le, de lehetőség van rá, hogy ezeket az adatokat gyorsítótárazzuk. Így nem kell minden egyes hitelesítés vagy beléptetés esetén a központi tartományvezérlőket igénybe venni, csökkentve ezzel a hálózat leterheltségét. Azt hogy milyen hitelesítési adatokat gyorsítótárazhatunk a RODC-ken az írható tartományvezérlő dönti el a Password Replication Policy alapján. Az hogy mely fiókokat engedélyezünk gyorsítótárazásra a PRP-ben a mi döntésünk, ha az összes felhasználói és rendszergazda fiókot engedélyezzük, akkor gyors lesz a beléptetés, de a jelszavak ugyan úgy veszélybe kerülhetnek egy támadás esetén, ezért érdemes csak néhány helyi felhasználó fiókját engedélyezni, a biztonsági kockázat csökkentése érdekében.

Újraindítható Active Directory tartományi szolgáltatások

Az újraindítható tartományi szolgáltatások lehetővé teszik, hogy leállítsunk vagy elindítsunk Active Directory szolgáltatásokat. Elsősorban ennek az az előnye, hogy nem kell az egész rendszert újraindítanunk, bizonyos a címtárat érintő frissítések, vagy Active Directory karbantartása esetén. Ilyen esetek lehetnek például Active Directory-adatbázisának kapcsolat nélküli töredezettségmentesítése vagy az operációs rendszer frissítése. Az Active Directory tartományi szolgáltatások megállításakor a kiszolgálón futó egyéb szolgáltatások, melyek működése nem függ az AD tartományi szolgáltatásoktól(plddául DHCP szerver), elérhetőek maradnak az ügyfélkérések teljesítéséhez. Alapértelmezés szerint az összes Windows Server 2008 rendszert futtató tartományvezérlőn elérhető ez a szolgáltatás, és használatához semmilyen előfeltétel nem kapcsolódik.
Az újraindítható Active Directory miatt a Windows Server 2008 rendszert futtató tartományvezérlőknek három állapota lehetséges:

Active Directory-szolgáltatás elindítva: Ez az az állapot, amelyben az AD-szolgáltatás fut. Az ebben az állapotban lévő Windows Server 2008 tartományvezérlő megegyezik egy a Windows Server 2000 vagy Windows Server 2003 rendszert futtató tartományvezérlő állapotával. Ebben az állapotban a tartományvezérlő képes hitelesítési és bejelentkezési szolgáltatásokat biztosítani.

Active Directory-szolgáltatás lállítva: Ebben az állapotban az Active Directory-szolgáltatások le vannak állítva. Ez az üzemmód ötvözi a tagkiszolgálók és címtárszolgáltatások helyreállítási módjában futó tartományvezérlők egyes jellemzőit. Ahogyan a címtárszolgáltatások helyreállítási módjánál, az Active Directory adatbázisa a helyi tartományvezérlőn offline állapotú. A felhasználók a gyorsítótárban lévő hitelesítési adatok, intelligens kártyák vagy biometrikus bejelentkezési eljárások segítségével tudnak bejelentkezni, vagy ha elérhető egy másik tartományvezérlő, akkor annak segítségével hálzaton keresztül is be tudnak jelentkezni.
Ahogyan a tagkiszolgáló esetében, a kiszolgáló csatlakozva van a tartományhoz, a csoportházirend és egyébb beállítások továbbra is érvényben vannak. De nem tud replikálni más tartományvezérlőket, ezért nem érdemes huzamosabb ideig ebben az állapotban hagyni.

Címtárszolgáltatások helyreállítási módja: Az üzemmód lehetővé teszi az Active Directory hiteles vagy nem hiteles helyreállítási módját. Állapota megeggyezik a Windows Server 2003 rendszert futtató tartományvezérlő helyreállítási állapotával.
Amikor az Active Directory tartományi szolgáltatásokat újraindítjuk, ügyeljünk arra, hogy a függő szolgáltatások is leállnak, mint például a fájlreplikációs szolgáltatás, vagy a Kerberos kulcsszolgáltató.

Network Acces Protection

A Network Access Protection egy teljesen új technológia, amelynek segítségével biztonságosabbá tehetjük a hálózatunkat, azáltal, hogy csak olyan eszközöket engedünk meg csatlakozni, amelyek megfelelnek egy általunk felállított követelményrendszernek.
Ez a szolgáltatás a vállalatok számára különösen fontos, mivel egy munkahelyi hálózathoz nem csak az irodákba telepített munkaállomások csatlakoznak, hanem például a dolgozók laptopjai vagy kézi számítógépei amelyeket otthon is használhatnak, aminek következtében nincsen garantálva, hogy nem tartalmaz kártékony szoftvereket, melyek később kárt tehetnek a vállalat hálózatán belül is. Ennek elkerülése érdekében létrehozhatunk egy feltételrendszert, aminek meg kell felelnie minden egyes a hálózathoz csatlakozni kívánó berendezésnek, különbem nem kap jogosultságot a hálózat erőforrásainak a használatára.
Amikor egy eszköz csatlakozni próbál a hálózathoz, először egy karantén zónába kerül, és átesik egy vizsgálaton (health checks) ami ellenőrzi, hogy megfelel-e a NAP házirend kritériumainak, ha megfelelt akkor átkerül a védett zónába, ahol hozzáférhet a hálózat „egészséges” elemeihez. Ha nem felel meg valamelyik feltételnek, akkor egy köztes zónába kerül, ekkor az „egészséges” kliensek vagy visszautasítják a kapcsolatot vagy korlátozott hozzáférést kap a hálózathoz, amellyel lehetősége van olyan állapotba hozni a rendszerét, amely megfelel a kritériumoknak, például különböző rendszerfrissítések letöltése vagy víruskereső program vírusdefiníciós adatbázisának a frissítése. Létrehozható egy úgynevezett remeditation szerver, ami automatikusan elvégzi a szükséges beállításokat az eszközön, ilyen szerver lehet egy WSUS (Windows Server Update Services). Miután eleget tett a feltételeknek átkerül a védett zónába, de a szükséges előírásoknak ezután is meg kell felelnie, mert amint olyan változás következik be a rendszer állapotában, ami nem felel meg a NAP házirendben szereplő előírásokkal, a gép azonnal a karanténzónába kerül át.
Ez a Network Access Protection 4 fő irányelve:

- A hálózathoz csatlakozó számítógépek „egészségi” állapotának ellenörzése(health checks)

- A nem megfelelő állapotú gépek izolálása a hálózat többi részétől(restriction)
- Lehetőség az automatikus javításra(remeditation)
- Az egészségi állapot folyamatos betartásának kikényszerítése(Ongoing Compliance)

Network Access Protection részegységei

A network Access Protection rendszer több alkotóelemből áll össze, melyek mind fontosak a hatékony működés érdekében. A főbb komponensek a következők:

- IPSec kényszerítés
- 802.1X kényszerítés
- VPN kényszerítés
- DHCP kényszerítés
- Network Policy Server
- NAP Agent
- System Health Agent
- NAP Administration Server
- System Health Validator
- Health Policy
- Accounts Database
- Health Registration Authority
- Remeditation Server

IPSec kikényszerítése(enforcement):

Internet Protocol security kikényszerítése az X.509 hitelesítő szabványt használja a hálózat elérésének kezelésére. Az érvényes health certificate-el nem rendelkező kliensek nem kommunikálhatnak a hálózat azon elemeivel, amelyek viszont rendelkeznek ezzel a tanúsítvánnyal. A módszer a következő képen működik, amikor egy számítógép csatlakozni kíván a hálózathoz, először egy tanúsítványt kell igényelnie a Health Registration Authority(HRA) rendszertől, ami jelzi, hogy az adott gép megfelel a NAP házirend biztonsági

követelményeinek, ez a tanúsítvány a health certificate. A HRA megvizsgálja, hogy megfelel-e a rendszer a kritériumoknak, ha igen, akkor megkapja a tanúsítványt a Certification Authority-től, ami feljogosítja a kommunikációra a health certificate-el rendelkező rendszerekkel. Ha nem felel meg a vizsgálaton, akkor nem kapja meg a tanúsítványt, csak egy limitált hozzáférést a hálózathoz, amivel képes elérni a remeditation(„gyógyító") szervert, hogy alkalmassá tegye magát a hálózat használatára. Miután lezajlott a folyamat, újabb vizsgálaton megy keresztül, ha még mindig nem felel meg akkor újra limitált hozzáférést kap, és a folyamat addig tart amíg nem kerül rendszer a NAP házirend által elfogadott állapotba.

Tehát az Ipsec kikényszerítése lehetővé teszi, hogy a hálózaton jelen lévő számítógépeknek, csak egy bizonyos köre tudjon kommunikálni egymással, azok amelyek megfelelnek az általunk előírt biztonsági előírásoknak.

802.1X kikényszerítése(enforcement):

A 802.1X szabvány vezetékes és vezeték nélküli hálózatok esetén is képes szabályozni a hozzáférést a hálózathoz. A Network Access Protection alatt ez a szolgáltatás a következőképpen zajlik le, a hálózatban működik egy 802.1X-et támogató switch vagy vezeték nélküli access point, ami a Network Policy Server (NPS) felügyelete alatt áll, amikor egy eszköz csatlakozni próbál a hálózathoz, egy elkülönített zónába kerül, izolálják a hálózat többi részétől Virtual LAN(VLAN) vagy IP filterek segítségével, amíg az NPS által definiált biztonsági ellenőrzésen át nem esik. Ekkor derül ki, hogy az eszköz egészségi állapota(State of Health) megfelelő-e ahhoz, hogy hozzáférést kapjon a hálózathoz, ha megfelelt, akkor a hálózat védett elemei közé kerül, ha nem akkor csak az úgynevezett gyógyító szerverekhez fér hozzá, amik segítségével elérheti a megfelelő egészségi állapotot.

VPN kikényszerítés(enforcement):

A Virtual Private Network arra alkalmas, hogy a dolgozó hozzáférjen a vállalati hálózathoz távolról is, például az otthonából. Az interneten keresztül biztonságos alagút építhető ki a dolgozó és a vállalat VPN szervere között. A

vállalati hálózat szempontjából a VPN kapcsolatok alkotják a legtöbb olyan elemét a hálózatnak, amely fölött a rendszergazdának nincsen közvetlen felügyelete. Erre a problémára nyújt segítséget a VPN kikényszerítés, amely kiterjeszti a Network Access Protectiont a virtuális privát hálózatokra úgy, hogy megvizsgálja a távolról kapcsolódó kliensek egészségi állapotát, ami alapján engedélyezi vagy letiltja a kapcsolódást a hálózathoz.
Amikor egy VPN kliens csatlakozik a VPN szerverhez, az megpróbálja azonosítani Protected Extensible Authentication Protocol(PEAP) vagy MS-CHEAP(Challenge Handshake Authentication Protocol) alapján. A beazonosított klienseknek ezután át kell küldeniük az egészségi állapotukat tartalmazó tanúsítványukat(SoH) a Network Policy Servernek(NPS). Ezután a kliens a SoH alapján vagy megkapja a hozzáférést a hálózathoz, vagy a szerver csomagszűrőket alkalmaz amelyek karanténba zárják a klienst és csak egy korlátozott hálózathoz engedik hozzáférni, ahol lehetősége van igénybe venni a gyógyítószervert. Ha a kliens állapota már megfelelő a szűrők eltávolításra kerülnek, és szabadon hozzáférhet a hálózathoz.

DHCP kikényszerítés(enforcement):

Ez a legegyszerűbb és legkevésbé biztonságos megoldás. A DHCP (Dynamic Host Configuration Protocol) szolgáltatást használja fel a kliensek hozzáférésének szabályozására, oly módon, hogy a NAP házirendben lefektetett kritériumoknak nem megfelelő gépeknek vagy nem oszt IP címet vagy csak olyat amivel egy korlátozott hálózathoz van hozzáférése ahol a remeditation szerver található. Amint a rendszer egészséges állapotba kerül, hozzáférést kap a teljes hálózathoz. Ez a megoldás nem annyira hatékony mint a fent említettek, mivel könnyen megkerülhető, ha valaki ismeri a hálózatot.

Network Policy Server:

A Network Policy Server, egy olyan Windows Server 2008 kiszolgáló, amelyen NPS szolgáltatás fut, segítségével létrehozhatjuk és kikényszeríthetjük a hálózat eléréséhez szükséges feltételeket, azonosíthatjuk a klienseket és engedélyezhetjük, hogy csatlakozzanak a hálózathoz.

Az NPS feladata felváltani a régebbi Internet Authentication Service-t is, ezért Remote Authentication Dial-In User Service(RADIUS) kiszolgáló és VPN házirendi központ is egyben.

NAP Agent:

Ezen szolgáltatás segítségével képes egy számítógép Network Access Protection kliens funkciót felvenni. Összegyűjti a rendszer egészségére vonatkozó adatokat a System Helath Agent(SHA) rendszerektől, és továbbítja azokat a NAP Enforcement Client(EC) rendszerekhez kiértékelésre.

System Health Agent:

Ez a komponens kezeli a számítógép egészségi állapotát meghatározó elemeket. Lehet például egy SHA ami a víruskereső program állapotát ellenőrzi, vagy egy másik ami az operációs rendszer frissítéseit figyeli. Egy-egy SHA összekapcsolható egy gyógyító(remeditation) szerverrel, ami például egy víruskereső program esetén tartalmazza a legújabb frissítéseket, amik segítségével napra késszé tehető a program. A fő feladata tehát összegyűjteni és továbbítani a rendszer egészségügyi állapotát leíró adatokat.

NAP Administration Server:

Az Administration Server begyűjti az adatokat a System Health Validator-tól és meghatározza, hogy a kliens milyen jogosultságot kapjon a hálózathoz, csak részlegest a gyógyítószerverhez, vagy teljes hozzáférést.

System Health Validator:

A Network Policy Server-hez tartozó modul, feladata eldönteni egy kliensről, hogy egészséges vagy nem, a kliens System Health Agent komponensei által küldött információ alapján. Majd a döntést a kliens tudomására hozni Statement of Health Response küldésével.

Health Policy:

Ezek az egészség előírások tartalmazzák a hálózat védett részéhez való hozzáférés feltételeit. Ez több dolgot is magában foglalhat, például víruskereső program megléte és naprakészsége, vagy rendszerfrissítések telepítése illetve tűzfal futása, a kliens rendszeren. Többféle Health Policy is létrehozható, attól függően, hogy melyik kikényszerítési eljáráshoz szeretnénk használni, akár mindegyik kikényszerítési módhoz definiálhatunk külön egészség előírásokat.

Accounts Database:

Ez az adatbázis tartja nyilván egy felhasználó vagy egy számítógép azonosításához szükséges adatokat a Network Access Protection számára. Tulajdonképpen az Active Directory részegysége.

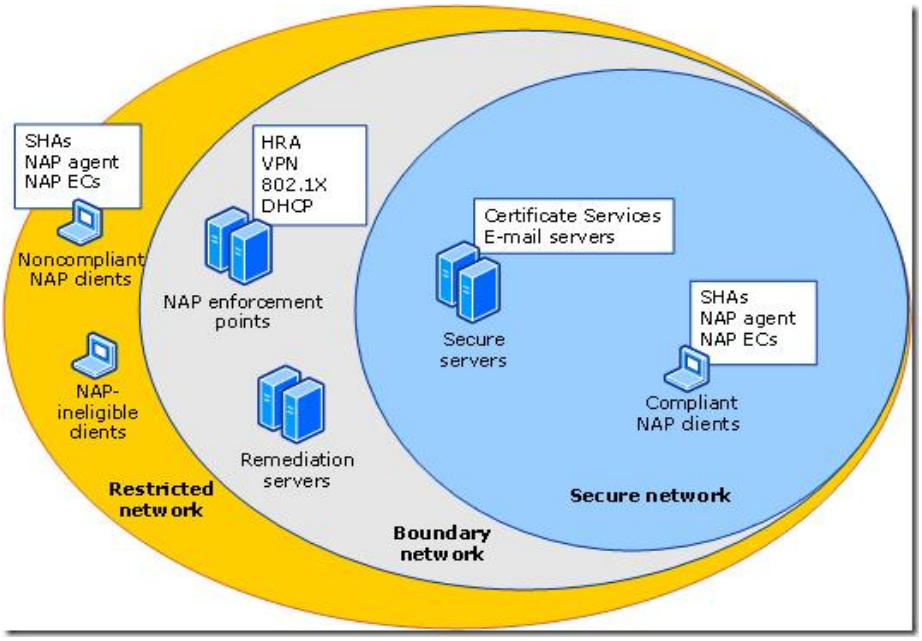
Health Registration Authority:

Szerepe, hogy közvetítő szerepet játsszon a kliensek között, begyűjti a kliensek egészségi állapotára vonatkozó tanúsítványait, amennyiben nem rendelkezik egy rendszer ezzel a tanúsítvánnyal nem kap engedélyt a kommunikációra a hálózat védett elemeivel.

Remeditation Server:

Ha egy kliens nem felel meg a felállított egészségügyi előírásnak akkor lehetősége van kapcsolódnia egy olyan szerverhez ami biztosítja a Network Access Protection házirendjében lefektetett követelményeknek való megfelelést, például úgy, hogy biztosítja a megfelelő frissítéseket és javításokat. Ezek a szerverek általában köztes zónában helyezkednek el a védett tartomány és a karantén zóna között, éppen azért, hogy a karanténba lévő gépek is elérjék őket.

A következő ábra jól szemlélteti, hogy az egyes komponensek milyen zónában helyezkednek el:



A Network Access Protection architektúrája

A Network Access Protection platform három komponensből tevődik össze, a kliens oldali architektúrából, a szerver oldali architektúrából és a két oldal közötti kommunikációból.

A kliens oldali architektúra:

A NAP kliensek olyan számítógépek, amelyek rendelkeznek a NAP kliens oldali komponenseivel, azaz elő tudják állítani az egészségi állapotukról szóló tanúsítványt(SoH), a rajtuk futó NAP Agent segítségével, a System Health Agent (SHA) rendszer ellenőrzi a kliens állapotát(például a tűzfalra vonatkozó SHA figyeli, hogy aktiválva van e tűzfal és hogy megfelelően van e frissítve), és az is az ő feladata, hogy felvegye a kapcsolatot a gyógyító szerverrel, amely segít egészséges állapotba hozni a klienst ha az nem felel meg egy előírásnak. Rendelkezik a kliens egy Enforcement Client(EC) komponenssel is, ami a kliens kapcsolódási metódusát jelöli, minden kapcsolattípushoz van egy-egy külön NAP Enforcement Client. Ha például DHCP alapú kikényszerítéssel szeretnénk

csatlakozni, akkor a DHCP Enforcement Client-et kell engedélyeznünk. Ezek a komponensek küldik el az egészségi állapotra vonatkozó tanúsítványokat is a szerver oldali komponensekhez.

Szerver oldali architektúra:

A Network Access Protection szerverek, minden kikényszerítési típushoz, Enforcement Server komponenseket tartalmaznak, amelyek összeillenek a nekik megfelelő Enforcement Clients-ekkel. Az Enforcement Serverek-hez érkeznek a System State of Health üzenetek a megfelelő Enforcement Client-ektől, amelyeket továbbítanak a Health Policy Server-nek. A Health Policy Server három komponensből áll, a *NPS Service* fogadja a SSoH adatokat tartalmazó üzeneteket és továbbítja a *NAP Administration Server*-nek, amelynek feladata szétbontani az egy-egy kliens egész rendszerére vonatkozó egészségi állapot leírását(SSoH) a részrendszerekre vonatkozó állapotokévá(SoH), és ezeket továbbítani a megfelelő System Health Validator-nak. Majd összegyűjteni a System Health Validátoroktól származó State of Helath Response válaszokat, és továbbítani azokat a Network Policy Servernek kiértékelésre.

A *System Health Validator* komponensek megkapják a kliens egy adott részére vonatkozó állapotleírást(például a tűzfalra vonatkozó SHV megkapja, hogy aktiválva van-e a tűzfal vagy sem), és ellenőrzik, hogy megfelel-e ez az állapot a házirendben lefektetett követelményeknek, és ez alapján válaszolnak (State of Health Response).

Kommunikáció a NAP szerver és a NAP kliens között:

A NAP Agent kliens komponens a NAP Administration Server-rel kommunikál következő módon:

- A NAP Agent elküldi a rendszer állapotára vonatkozó információkat(SSoH) a NAP Enforcement Client komponensnek.
- A NAP EC továbbítja ezeket az információkat a NAP Enforcement Servernek.
- A NAP ES átadja a Network Policy Server-nek.
- A NPS pedig eljuttatja az adatokat a NAP Administration Servernek.

Miután a kliens egészségügyi állapotának a kiértékelése befejeződött, az eredményt a kliens tudomására kell hozni:

- A NAP Administration Server a Network Policy Servernek továbbítja a választ(SoHR)
- Az NPS átadja a NAP Enforcement Servernek.
- A NAP Enforcement Server a NAP Enforcement Client-nek
- És végül a NAP EC továbbítja a választ a NAP Agent-nek, ami így el tudja dönteni, hogy kapott e jogosultságot, vagy igénybe kell vennie egy Remeditation Servert, hogy frissítse a rendszerét.

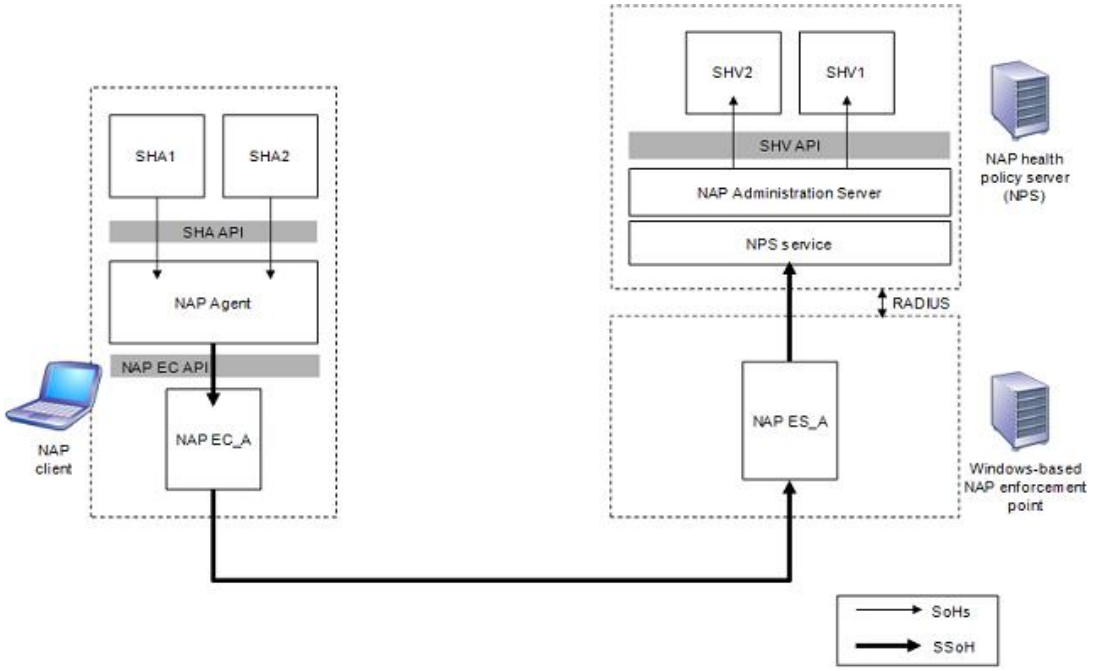
Az előbbi kommunikációs láncon a rendszer egészére vonatkozó egészségügyi adatok(SSoH) mozogtak a szerver oldalig, és a szerver oldal felől is a kliens rendszer egészére vonatkozó válasz továbbítódott a kliensnek. Ezeket az adatokat mind a kliens mind a szerver oldalon szét kell bontani, a kliens különböző részegységeinek az állapotára, hogy tudjuk, hogyha valami nem felel meg a követelményeknek, akkor miket kell esetlegesen frissíteni, javítani.
Ez a következő úton megy végbe, kliens:

- A SHA elküldi a State of Health üzenetet a NAP Agent-nek.
- A NAP Agent összegyűjti a SoH üzeneteket és előállítja belőle az egész rendszerre vonatkozó egészségi állapotot(SSoH), és továbbítja az Enforcement Client-nek.

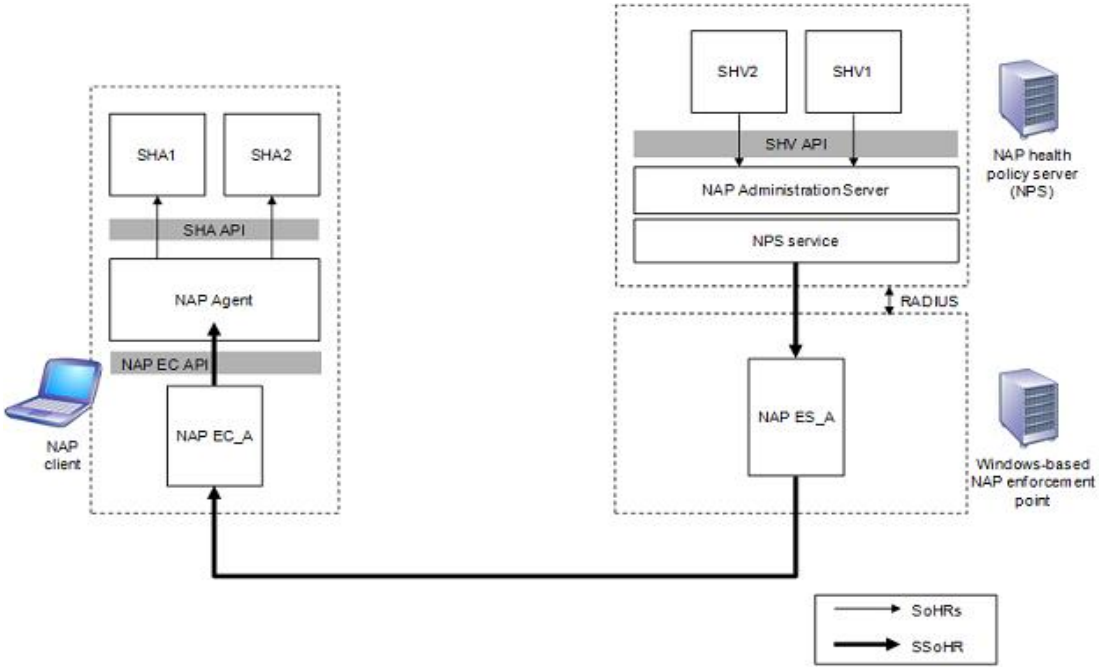
A szerver oldalon pedig:

- A System Health Validator előállítja a SoHR választ a kliens számára, amit továbbít a NAP Administration Servernek
- A NAP Administration Server továbbytja a Network Policy Servernek
- A Network Policy Server összegyűjti ezeket az „egészségügyi válaszokat”(SOHR) és egyetlen üzenetként(SSoHR) továbbítja azokat a NAP Enforcement Servernek.

A következő ábrák jól szemléltetik a folyamatot, a vastag nyilak jelölik az egész kliensre vonatkozó üzenet haladását, a vékony nyilak pedig a részrendszerek állapotának a továbbítását.



Kommunikáció a klienstől a szerver irányába



A szerver válasza a kliens számára

BitLocker Meghajtótitkosítás (BitLocker Drive Encryption)

Nem minden helyen garantálható a szerver számítógépek fizikai biztonsága, például egy kisebb telephelyen ahol nincsenek meg a megfelelő biztonsági követelmények, ki van szolgáltatva az adott rendszer egy esetleges fizikai támadásnak(például Live CD-ről vagy pendrive-ról való bootolással könyeddén hozzáférhetnek a gépen tárolt bizalmas információkhoz). A BitLocker meghajtótitkosítás olyan technológia, amely segítségével titkosíthatjuk a számítógép köteteit, megvédve így bizalmas adatainkat például eltulajdonított merevlemez vagy egyéb fizikai támadás esetén.
Ez a biztonsági szolgáltatás a Windows Server 2008 operációs rendszeren kívül megtalálható a Windows Vista Ultimate és Enterprise kiadásaiban is.

A BitLocker működése:
A BitLocker képes titkosítani egész köteteket, beleértve a rendszerpartíciót is. Ezért szükség van egy indítópartícióra amely tartalmazza az indításhoz szükséges fájlokat titkosítás nélkül, az innen elindított operációs rendszer már képes lesz visszafejteni a rendszerpartíciót. Az adatok titkosítva tárolódnak a merevlemezen, de mivel a processzornak titkosítatlan adatokra van szüksége a feladata elvégzéséhez, ezért a rendszernek folyamatosan titkosítania és visszafejtenie kell az adatokat minden írási és olvasási művelet előtt illetve után. Ez a folyamat 5-10%-os teljesítmény csökkenést okoz, bár ez nagyban függ a hardver elemektől és a felhasználás módjától is.
A technológia támogatja a TPM(Trust Platform Modul) hardveres kriptográfiai eszközöket, amelyek segítségével a korai rendszerindítási összetevőket ellenőrzi. Ez azért fontos, mert mivel ezek az összetevők titkosítatlanul vannak tárolva, ezért a támadó ezen rendszerindítási összetevők módosításával könnyen hozzáférhet a számítógéphez. Még ha a lemezen lévő adatok titkosítva is vannak, a támadó hozzáférhet a BitLocker-kódokhoz vagy felhasználói jelszavakhoz, amelyekkel megkerülheti a BitLocker védelmet. A TPM chipet első indítás előtt inicializálni kell, ekkor meg kell adnunk egy jelszót, utána pedig a Windows

elmenti a jelenlegi rendszerindítási összetevőkre vonatkozó adatokat a TPM memóriájába. Ezután minden indításkor összehasonlításra kerülnek a TPM memóriájában lévő, és a rendszer indításakor fennálló adatok, és a rendszerpartíciót csak akkor fejti vissza, ha ezek az értékek megegyeznek. A TPM-et a *tpm.msc* felügyeleti konzollal kezelhetjük, ki illetve bekapcsolhatjuk, inicializálhatjuk, törölhetjük a tartalmát és megváltoztathatjuk a hozzátartozó jelszót.

BitLocker üzemmódok

A BitLockert háromféle üzemmódban használhatjuk:

- *Láthatatlan mód(Transparent Operation Mode):* Ilyenkor a felhasználó a hagyományos módon indítja és használja a rendszert, észre sem veszi, hogy titkosítva vannak a meghajtók. A lemeztitkosításhoz használt kulcsot a TPM biztosítja, és csak akkor fejti vissza rendszerinduláskor, ha nem történt változás a letárolt és a jelenlegi adatokhoz képest. Például ha a merevlemezt átrakjuk egy másik számítógépbe, vagy kicseréljük az alaplapot, akkor az adatok nem fognak egyezni és a rendszer nem indul el, ha csak nem adunk meg helyreállítási kulcsot. Ezzel a módszerrel a számítógépet bárki elindíthatja, de ha a felhasználói fiókok jelszóval vannak védve, akkor az adatokhoz csak a felhasználói fiókokkal rendelkező személyek férhetnek hozzá.

- *Felhasználói hitelesítési mód(User Authentication Mode):* Ekkor a felhasználnak hitelesítenie kell magát rendszerindítás előtt, ezt megteheti rendszer bootolás előtt egy PIN kóddal, egy USB adattárolón lévő kulccsal vagy mind a kettővel egyszerre. Ennek a módszernek is szüksége van TPM chipre, ami azonosítja a felhasználót a megadott PIN kód vagy az adattárolón lévő kulcs alapján, és csak azután fejti vissza az adatokat.

- *USB-kulcs mód(USB Key Mode):* Ekkor a felhasználónak rendszerindítás előtt egy rendszerindító kulcsot tartalmazó pendrive-ot kell csatlakoztatnia a számítógéphez, amely a titkosított adatok tartalmának

visszafejtéséhez szükséges. Ebben az esetben nincsen szükség TPM chipre, de a számítógépnek támogatnia kell az USB-s eszközök rendszerindítás előtti kezelését.

Ezeket a hitelesítési módszereket együtt is lehet használni, a következő párosítások lehetségesek:

- Csak TPM
- TPM és PIN kód
- TPM + PIN kód + USB kulcs
- TPM + USB kulcs
- USB kulcs

A BitLocker üzembeállításakor létre kell hoznunk egy helyreállítási jelszót(Recovery Password), amely segítségével feloldható a BitLocker-rel zárolt kötet. Erre azért van szükség, mert ha esetleg elvesznek a titkosítási kulcsok, az adatokat a segítségével még mindig meg lehet menteni. Arra az esetre, hogy a felhasználók ne tudják elveszíteni a helyreállítási jelszavukat is, lehetőségünk van az Active Directory-ban tárolnunk azokat.

Összefoglalva BitLocker technológia segít megvédeni a vállalat bizalmas információit vagy üzleti titkait, azzal hogy a merevlemezen található adatokat egy olvashatatlan adathalmazzá változtatja, amit csak az a számítógép tud visszafejteni amely a titkosítást elvégezte. Ha az egész számítógépet eltulajdonítják akkor is védve vannak az adatok, ha megköveteljük a rendszerindítás előtti hitelesítést a felhasználóktól.

Internet Information Services 7

A Windows Server 2008 webkiszolgálója az Internet Information Services 7, amelyet mint sok más szolgáltatást is kiszolgálói szerepkörként telepíthetünk a szerverre. Számos architektúrális újdonságot hordoz, amelyek közül a legfontosabb, hogy a webkiszolgáló már nem egyetlen nagy monolit rendszer, hanem közel 40 kisebb komponensből tevődik össze, amelyek között a függőségeket automatikusan a rendszer kezeli. Már elődjénél az Internet Infomation Services 6-nál is csak azok a szolgáltatások voltak engedélyezve, amelyek szükségesek voltak a feladatköre elvégzéséhez, de az IIS 7-esre fel sincsenek telepítve azok a komponensek amelyekre nincsen szüksége, így egy esetleges támadás során sem képesek aktiválni azokat, hogy később visszaéljenek egy komponens esetleges biztonsági résével. Ennek következtében jelentősen lecsökken a szerveren lévő biztonsági rések száma, és csökken a karbantartási idő is, mivel az olyan komponenseket, amelyek nincsenek feltelepítve nem is kell frissíteni nő a rendelkezésre állás ideje, nem kell még pár percre sem leállítani a kiszolgálót egy nem is használt modul frissítése után történő újraindítás miatt.
Az Internet Infomation Services 7 alapértelmezett telepítése csak 11 komponenst installál fel, amelyek csak alapszintű eszközöket biztosítanak, azokat a komponenseket amelyekre még szükségünk van például a Server Manager segítségével egyszerűen feltelepíthetjük.

Az IIS7 telepítése:

- Először indítsuk el Server Manager-t
- A *Roles Summary* csoportból válasszuk ki az *Add Roles* opciót
- Ekkor elindul az *Add Roles Wizard* varázsló, ahol válasszuk ki a *Web Server (IIS)* -t a szerepkörök közül
- Amikor varázsló megerősítést kér, hogy a szerepkörhöz szükséges funkciókat telepítse-e, kattintsunk az *Add Required Features* azután pedig

a tovább gombra.

- A következő ablakon kiválaszthatjuk, hogy milyen modulokat szeretnénk telepíteni a webszerverre, majd lépjünk tovább.
- Klikkeljünk az *Install* gombra.

Az IIS7 konfigurációja

Az előző verzióhoz képest a konfigurációs rendszer is teljesen megváltozott, nem csak a futtatható komponensek lettek modularizálva, hanem a konfigurációkezelés is. Az IIS7 szorosan összefonódik a .NET platformmal, a webszerver beállításai a .NET-es alkalmazások beállításaival azonos helyen tárolódnak. A különböző konfigurációs fájlok hierarchiába rendeződnek, melynek csúcsán a *machine.config* fájl áll, amely az összes .NET-es alkalmazásra tartalmaz beállításokat. A hierarchia következő eleme a *web.config* fájl, amely az ASP.NET alkalmazások közös beállításait tartalmazza. Ezután az *applicationHost.config* állomány következik, amely az Internet Infomation Services 7 központi konfigurációs állománya, amit az egyes webhelyek és alkalmazások saját helyi *web.config* állományai követnek. Így már külön állományokban, elosztottan lehet konfigurálni az egyes weboldalak és webalkalmazások jellemzőit, és nem kell adminisztrátori joggal rendelkezni az adott gépen, hogy egy felhasználó módosíthassa a saját oldalához tartozó *web.config* fájlt.

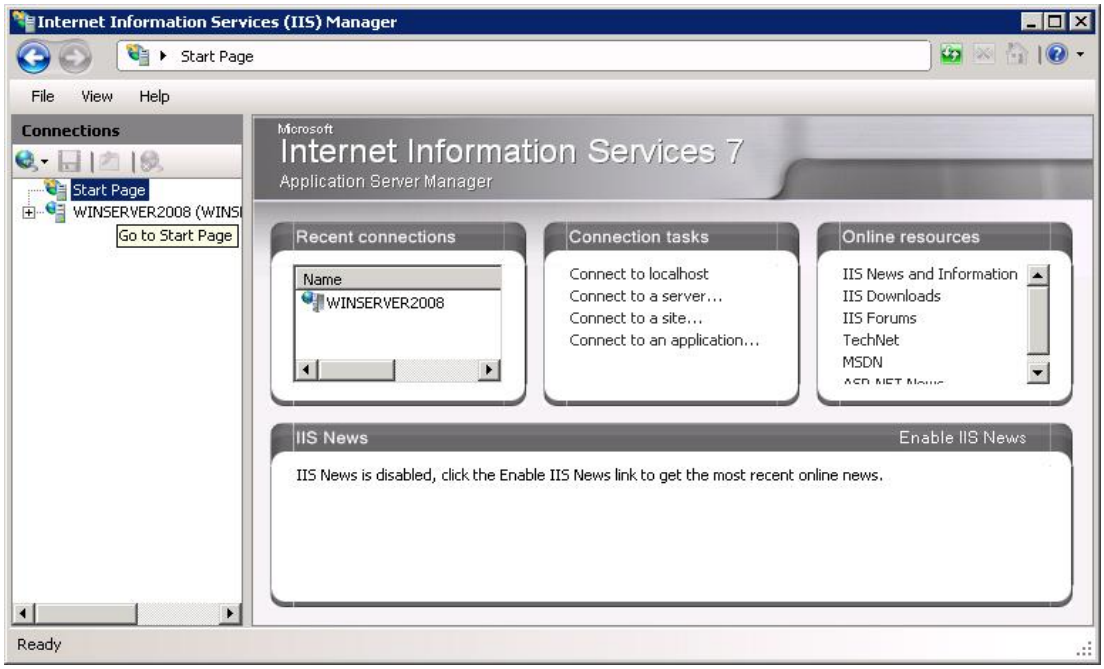
A hierarchián belül a beállítások öröklődnek, de van lehetőség az alsóbb szinteken a beállítások felüldefiniálására, illetve felső szinteken a felüldefiniálás tiltására is.

A fentieken kívül még létezik kettő konfigurációs fájl ami nem vesz részt a hierarchiában, a *redirection.config* amelyre akkor van szükségünk, ha igénybevesszük a Shared Configuration szolgáltatást, ugyanis ebben az esetben a *redirection.config* állomány határozza meg, hogy milyen megosztott mappában találhatóak a konfigurációs állományok. A másik különálló fájl az *administration.config* amely az ISS Manager beállításait tartalmazza.

IIS7 Manager

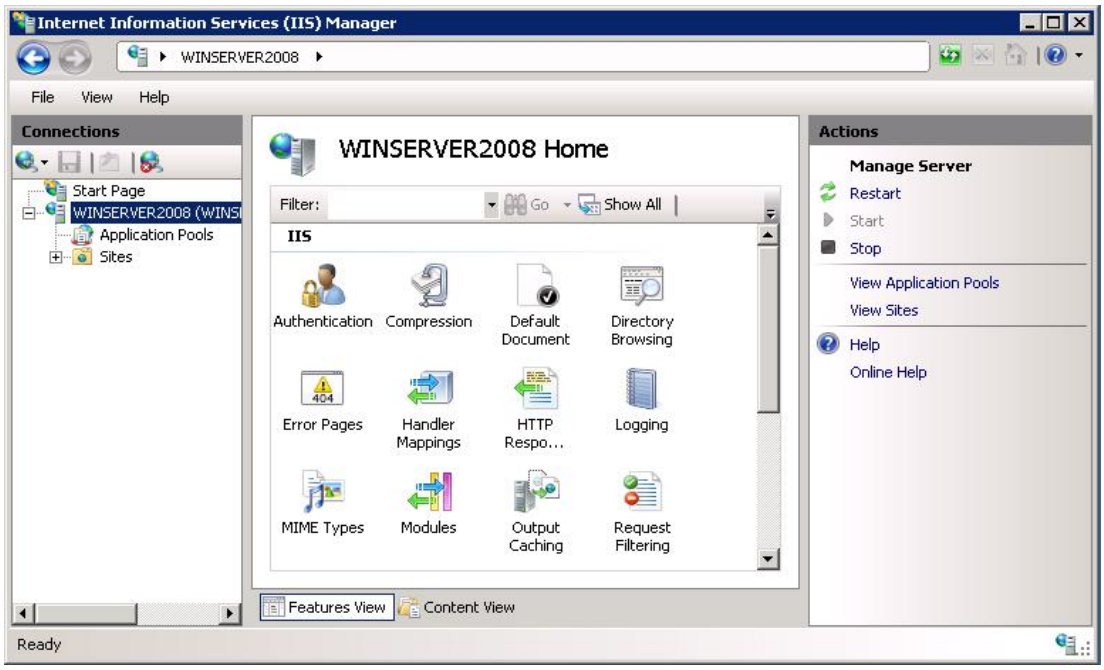
Az Internet Information Services 7 kiszolgáló oldali felügyeleti eszköze, ami szintén sok változtatáson esett át, egy teljesen új, könnyen átlátható MMC(Microsoft Management Console) alapú felügyeleti konzol. Automatikusan installálódik amikor a kiszolgáló felveszi a webkiszolgáló szerepkört. Lehetőséget nyújt a webkiszolgáló távoli felügyeletére is, amely a Web Management Service segítségével szabványos HTTPS protokoll használatával valósul meg.

Amikor elindítjuk az IIS Manager-t a következő képernyő fogad minket:



A kezdőképernyőn megtekinthetjük az előző kapcsolatainkat webszerverekhez, weboldalakhoz vagy webalkalmazásokhoz, a Conection Tasks hasábon csatlakozhatunk újabbakhoz, az Online Resources listán pedig hivatkozásokat találhatunk különböző webes erőforrásokhoz. A bal szélen lévő Connections panelen találhatóak a különböző IIS7-es szerverek, alapbeállításon csak a helyi szerver jelenik meg, de lehetőségünk van más szervereket is hozzáadni a Create New Connection gombal. Ahhoz hogy bővebb információkat kapjunk a saját szerverünkről, klikkeljünk a listában a nevére.

Ekkor a következő ablak jelenik meg:



A legördülő menüben a szerver neve alatt két almenüt láthatunk, *Application Pools* és *Sites*. Az Application Pool arra való, hogy elkülönítse egymástól a különböző webalkalmazásokat, mindegyik Application Pool külön szálon fut, ezért nem kell attól tartanunk, hogy egy alkalmazás által kiváltott hiba akadályozhat egy másik alkalmazást, amíg külön Application Pool-ban tároljuk őket. A rendszer létrehoz egy alapértelmezett Application Pool-t *DefaultAppPool* néven, és ha máshogy nem rendelkezünk az összes alkalmazásunk ebben fog futni. A Sites könyvtár a kiszolgálón található weboldalakat tartalmazza.

Az ablak közepén található Home panel részletes leírást ad a Connections listában kiválasztott elemről, itt a különböző tulajdonságok csoportosíthatóak a könnyebb átláthatóság érdekében. Ezen a panelen minden rendelkezésre áll ami ahhoz kell, hogy felügyelet alatt és karbantartsuk a webszerverünket.

A jobboldali panelen különböző utasításokat adhatunk ki, attól függően, hogy éppen milyen elemen állunk, például ha kiválasztjuk a szerverünket akkor meg tudjuk állítani vagy el tudjuk indítani a működését.

Az IIS Manager egy jól átlátható és könnyen kezelhető felületet nyújt a

webszerver kezelésére, de lehetőségünk van a parancssoros adminisztrációra is az AppCmd.exe segítségével. Szinte mindent el lehet végezni vele amit az IIS Manager tud, remekül paraméterezhető, jól használható batch-fájlokban és sok feladat automatizálható a segítségével. Hiba esetén nem csak hibakódot jelenít meg, hanem leírást ad a hibáról és javaslatot a megoldására. Az AppCmd utasítások eredménye lekérhető xml formátumban is a */xml* paraméter használatával, ez lehetővé teszi két parancs összekötését csővezeték segítségével a | operátor és a /in paraméter használatával.
Példa:

appcmd list apppool /state:Stopped /xmp | appcmd start apppool /in

A fenti példa elindítja az összes leállított Application Pool-t.

Hitelesítés és hozzáférés szabályozás

Az Internet Information Services 7 számos újdonságot vezet be a hitelesítés és hozzáférés szabályozás területén is, amelyek megkönnyítik a webkiszolgálóval kapcsolatos adminisztrációs feladatokat.
Megjelenik az *IIS_IUSR* beépített felhasználói és az *IIS_IUSRS* beépített csoport fiók. Mindkettő rögzített SID(Security Identifier)-el rendelkezik, így a fájlokra adott jogosultságok gond nélkül átvihetőek másik számítógépre is. További jellemzője a beépített felhasználónak, hogy nem kell a jelszava kezelésével foglalkoznunk, ugyanis nincsen neki. Az *IIS_IUSR* fiók segítségével a webkiszolgáló névtelen hozzáférést biztosít a nyilvános weboldalakhoz az azonosítatlan felhasználónak anélkül, hogy az hozzáférhetne a levédett privát adatokhoz.
A különböző Application Pool-okhoz rendelt felhasználói fiókok, futási időben automatikusan az *IIS_IUSRS* csoport tagjává válnak, így elég ennek a csoportnak jogosultságot adnunk, nem kell csoporttagsággal foglalkoznunk.
A hozzáférés szabályozásban újdonság az *URL Authoriztion*, amely lehetővé teszi, hogy a fájlrendszerben található erőforrásoktól függetlenül, URL-ekre adjunk meg hozzáférési szabályokat, amelyek a *web.config* állományokban tárolódnak.

A *Request Filtering* modul pedig lehetővé teszi a beérkező kérésekre vonatkozóan bizonyos kényszerek meghatározását, például az URL-ek hossza, amelynek segítségével megvédhetjük alkalmazásainkat a kérés rossz szándékú formázásával elért, néhány tipikus támadási formájától.

FTP szolgáltatás

Az Internet Information Services 7-hez egy teljesen újraírt FTP kiszolgáló érhető el, amely teljes egészében integrálódik az új webkiszolgáló konfigurációs és felügyeleti sémájával. Ezt a komponenst külön kell letöltenünk és telepítenünk, a neve *FTP Publiching Services 7*.

Az új verzió már támogatja az SSL, UTF-8 és az IPv6 használatát is, egyetlen IP-címen több FTP helyet is üzemeltethetünk, a szerver host név alapján irányítja a kéréseket a megfelelő helyre. Az FTP szerverre történő bejelentkezés integrálható ASP.NET vagy IIS Manager alapú hitelesítési megoldásokkal, így olyan felhasználók is bejelentkezhetnek FTP szolgáltatásokra, akik nem rendelkeznek windows felhasználói fiókkal.

A legfontosabb újítása viszont, hogy támogatja az FTPS(FTP-SSL) szolgáltatást, aminek segítségével titkosított csatornákon keresztül továbbíthatóak az adatok.

Kétféleképpen használhatjuk az FTPS szervert:

- Csak a vezérlő csatornát titkosítjuk: ekkor a felhasználónevek és a jelszavak titkosítódnak, az adatfolyam nem.
- Az adat és a vezérlő csatornát is titkosítjuk: Ekkor az adatfolyam is titkosítva továbbítódik, bár ez nagyobb sávszélességnél nagyobb terhelést jelent a processzor számára.

Az Internet Information Services új verziója tehát még biztonságosabbá, rugalmasabbá és könnyebben kezelhetővé teszi, a weboldalak és webalkalmazások közzétételét és karbantartását.

Hyper-V

A vállalatok életében egyre jobban előtérbe kerülnek a virtualizációs technológiák, amelyek segítségével költséghatékonyabbá, energiatakarékosabbá és biztonságosabbá tehetik a hálózati infrastruktúrájukat, miközben magasabb rendelkezésre állást tudnak biztosítani a különböző kiszolgálók számára. A szerver virtualizáció segítségével több operációs rendszert futtathatunk egy fizikai számítógépen, virtuális gépek segítségével.

A szerver virtualizáció előnyei

A kiszolgálóhardverek erőforrásai ritkán vannak teljes mértékben kihasználva, az egyes szolgáltatások különböző időben különböző erőforrásokat használnak. Célszerű az ilyen szolgáltatásokat minél kevesebb számítógépre összpontosítani, hogy minél jobban ki tudjuk használni a szerverek fizikai teljesítményét, aminek következtében csökkenthetjük a szervergépek számát és ezáltal csökkenthetjük a fenntartási és felügyeleti költségeket.

Fontos szempont, a szolgáltatások folyamatos működésének a biztosítása is. A kiszolgálóvirtualizáció segítségével minimalizálni lehet a tervezett és a nem tervezett rendszerleállások idejét, például fürtöző szolgáltatások használatával átmozgathatóak a virtuális gépek a fizikai kiszolgálók között, így ha az egyik kiszolgáló leáll, a virtuális gép átkerülhet egy másik fizikai kiszolgálóra, amennyiben az képes befogadni.

A szoftverfejlesztő cégek egyszerűen tesztelhetik programjaikat több platformon is, akár egy már használatban lévő szerveren is. Mivel ezekre a virtuális gépekre csak a tesztelés idejére van szükség, így erőforrásigényük is ideiglenes. A különböző tesztkörnyezetek pedig izolálhatóak egymástól, így nem kell attól tartanunk, hogy a tesztesetek befolyásolják egymás teszteredményeit.

A Windows Server 2008 a kiszolgálóvirtualizációhoz az összes elemet beépítve tartalmazza a Hyper-V technológia formájában.

A Hyper-V virtualizációs technológia

A Hyper-V egy szerepkör a Windows Server 2008-ban, ami eszközöket és szolgáltatásokat biztosít egy virtuális kiszolgálói környezet létrehozásához és felügyeletéhez.
A főbb jellemzői a következők:

- 64 bites mikrokerneles hypervisor alapú virtualizáció.
- Számos különböző operációs rendszer futtatható egyidejűleg, ezek lehetnek 32 vagy 64 bites rendszerek is.
- A virtuális gépek lehetnek egy vagy több processzorosak.
- A működő virtuális gépekről pillanatfelvételek készíthetőek, amelyek lementik az adott gép állapotát, adatait, hardver konfigurációját, így egyszerűen visszaállítható a virtuális gép egy korábbi állapotába.
- Támogatja a virtuális lokális hálózatokat(VLAN).
- A virtuális gépek egyszerűen beállíthatók a Windows hálózati terheléselosztási szolgáltatásának futtatására, a terhelés különböző kiszolgálón található virtuális gépek között is eloszthető.
- Szabványos WMI és API felület segítségével a független szoftvergyártók is készíthetnek egyéni megoldásokat a virtualizációs platformra.

A Hyper-V architektúrája

Mint ahogyan már említettem a Hyper-V egy 64 bites mikrokerneles hypervisor alapú virtualizációs technológia. A hypervisor az egy vékony réteg, amely a virtuális gépek és a fizikai hardver között húzódik, tulajdon képen egy mikrokernel ami közvetlenül a hardveren fut. Nincsen szüksége host-operációsrendszerre a működéséhez, ezért a hypervisor felel a virtuális gépek futtatásáért valamint teljesen elszigetelt partíciókat alakít ki, amelyekben a virtuális gépek egymástól függetlenül működhetnek. A különböző partíciókon működő virtuális gépek a hardver erőforrásokhoz csak a hypervisoron keresztül férhetnek hozzá, kivéve a szülő partíciót.
A partíciók olyan logikai egységek, amelyek elszeparálják egymástól a különböző virtuális gépeken futó operációs rendszereket. Van egy kitüntetett

partíció, az úgynevezett szülő vagy root partíció, amelyen csak Windows Server 2008 64-bites operációs rendszer futhat. Ez tulajdonképpen az a partíció, ahol a kiszolgáló felvette a Hyper-V szerepkört, és az egyetlen olyan, amelyiknek közvetlen hozzáférése van a hardver eszközökhöz. A szülő partíción helyezkednek el a perifériákhoz szükséges eszközmeghajtók is, és itt található a virtualizációs verem amely hardverrel kapcsolatos szolgáltatásokat nyújt a gyermek partíciók számára. A gyermek partíciókat a szülőpartíció segítségével hozhatunk létre, ezeken futnak az úgynevezett vendég(guest) operációs rendszerek. A szülő partíció létrehozható Server Core típusú kiszolgálón is, de ekkor a rendszer felügyelete kicsit körülményesebbé válik.

A Hyper-V egyik fontos újítása a hardver eszközök megosztására használt technológia, amely támogatja az emulált és a szintetikus eszközöket is a vendég operációs rendszeren. Az emulált eszközök valóságos eszközök virtuális reprezentációi, ha az operációs rendszer rendelkezik a szükséges eszközkezelőkkel, azonnal használatba vehetőek. Az emulált eszközök használata jelentősen leterheli a processzort, főleg több virtuális gép esetén, ezért lassíthatják a rendszer működését.

A szintetikus eszközöknek nincsen közvetlen fizikai megfelelőjük, nem egy valóban létező hardvereszköz képességeit emulálják, hanem egy csatornán keresztül kommunikálnak a szülőpartíción lévő szükséges eszközkezelőkkel. A szintetikus eszközök a három alábbi komponens együtteseként működnek:

Virtulization Service Provider(VSP): Ez a komponens a szülőpartíción fut, melynek feladata kommunikálni a driverekkel és megosztani azokat a gyermekpartíciók felé a Virtual Machine Bus-on keresztül. A VSP-k automatikusan telepítődnek a szülőpartícióra, amint felveszi a kiszolgáló a Hyper-V szerepkört.

Virtualization Service Client(VSC): Ezek a komponensek a gyermekpartíciókon futnak, és szintetikus eszközökként teszik elérhetővé azokat a hardvereket amelyeket a szülőpartícióra telepítettünk és megosztottunk az adott gyermekpartícióval.

A VSC-k telepítése nem automatikus, az Integration Components telepítésével együtt kerülnek fel a gépre, az Integration Components feladata, hogy a

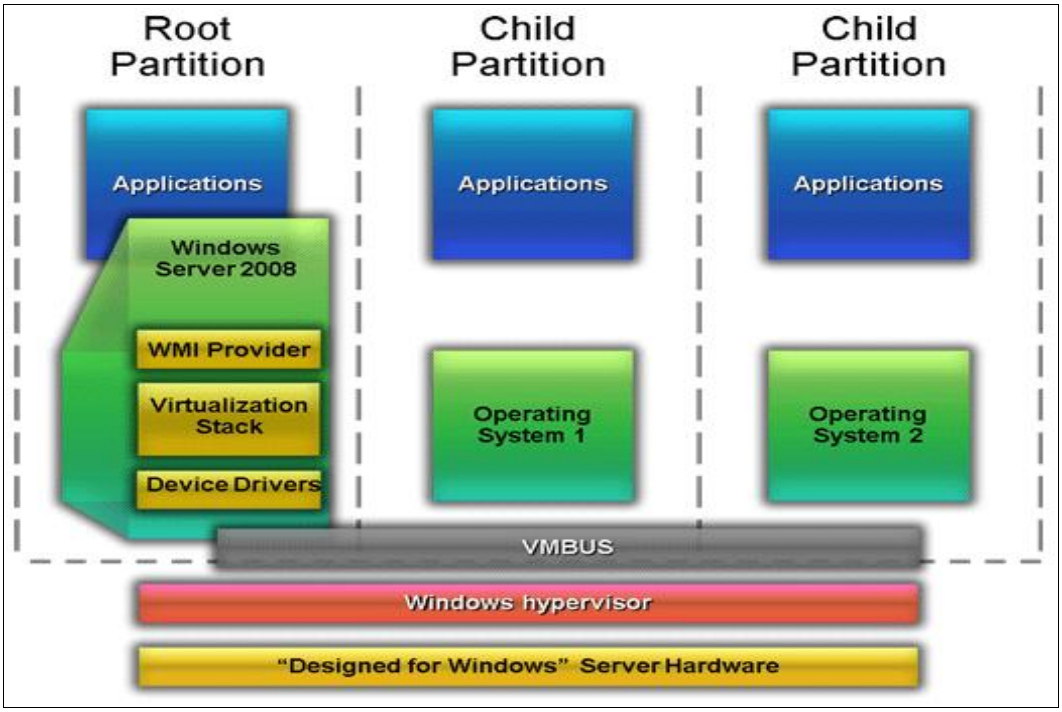
gyermekpartíció képes legyen kommunikálni más partícikkal és a hypervisorral.

Virtual Machine Bus(VMBus): Egy olyan nagy teljesítményű sínrendszer, amelyen keresztül az egyes partíciók kommunikálni tudnak egymással. Ezen keresztül kommunikálnak egymással a VSP-k és a VSC-k, a hypervisor igénybevétele nélkül.

A szintetikus eszközök a gyermekpartíciókon csak akkor válnak láthatóvá, ha az Integration Services-t is telepítjük rájuk, ekkor telepítődik a Virtual Machine Bus is.

Az eszköz emulációhoz képest a szintetikus eszközök használata nagyságrendekkel gyorsabb megoldást képes nyújtani, és még a hypervisort is tehermentesíti, azzal a hátránnyal, hogy csak az Integration Services telepítése után működőképes.

A következő ábra nagy vonalakban szemlélteti a Hyper-V architektúra elemeit.



Processzor és memória kezelésére

A Hyper-V a megjelenésekor 16 logikai processzort volt képes kezelni, de a 6 magos processzorok(mint például az Intel Xeon 7400-as széria) megjelenését követően megjelent egy frissítés, amelynek segítségével már 24 processzormagot

is képes kezelni. Támogatja a processzortúljegyzést, ami akkor következik be, ha egy számítógépen több virtuális processzor van mint logikai processzor. A virtuális processzor a hypervisor által a virtuális gépekhez rendelt processzor. A logikai és virtuális processzorok maximális túljegyzési aránya 1:8. Ebből az következik, hogy a Hyper-V segítségével akár 192 darab virtuális gépet is futtathatunk egyetlen fizikai szerveren. De arra is van lehetőségünk hogy egy virtuális géphez több logikai processzort rendeljünk hozzá, virtuális gépenként 4 darab logikai processzor kezelése lehetséges.

A virtuális gépeknek kioszthatő maximális memóriaméret 61 gigabyte, és megjelenik egy új memóriakezelési technológia, a Page Sharing. A Page Sharing lehetővé teszi, a virtuális gépek közötti azonos memórialapok megosztását. Csak a teljesen azonos memórialapokat osztja meg a virtuális gépek között, minimális eltérés esetén is, a változás csak a saját memóriatartományán belül lesz elérhető. A megoldás előnye, hogy kevesebb memóriára lesz szükségünk, ha több hasonló virtuális gépünk van, hátránya viszont, hogy minimális teljesítménycsökkenést okoz. Egy másik újdonság a Memory Reserves funkció, amelynek segítségével lehetőség van arra, hogy a virtuális géphez rendelt memória egy bizonyos százalékát ne adjuk oda azonnal a virtuális géphez, hanem csak akkor ha már tényleg szüksége van rá, és ha van még szabad fizikai memória. Ha nincsen már rendelkezésre álló fizikai memória, akkor a Hyper-V virtuális memóriát hoz létre az adott virtuális gép számára.

Tárolóeszközök

A Virtual Service Provider és Virtual Service Client architektúrának köszönhetően a tárolóeszközökkel kapcsolatban is számos újdonság jelenik meg, amelyek kihasználják a szintetikus eszközök lehetőségeit.

A fizikai tárolóeszközök több fajtáját támogatja a Microsoft Hyper-V, ezek két csoportra bonthatóak:

- *Közvetlen csatlakoztatású tárolóeszközök(Directly Attached Storage):* Ezek a tárolóeszközök a Hyper-V-t futtató kiszolgálóra vannak közvetlenül csatlakoztatva. A támogatott típusok SATA, eSATA, PATA, SAS(Serial Attched SCSI), SCSI, USB és Firewire.

- *Tárolóhálózat eszközök(Storage Area Network):*A SAN egy nagy sebességű speciális célú hálózat vagy alhálózat, ami különböző adattároló eszközök összekapcsolásával jön létre. A támogatott technológiák Internet SCSI(iSCSI), Fibre Chanel, SAS.

A virtuális gépeken kétféle adattárolási technika közül választhatunk:

- *Virtuális IDE eszköz*: Minden virtuális gép 4 IDE eszközt használhat. A vendég operációs rendszer csak virtual IDE eszközről bootolhat be, amelynek emulált eszköznek kell lennie.
- *Virtuális SCSI eszköz:* A virtuális gépek 4 SCSI vezérlőt támogatnak, és minden vezérlőhöz 64 tárolóeszköz csatlakoztatható. Ezeknek az eszközöknek a használatához szükséges, hogy az Integration Services telepítve legyen a vendég operációs rendszerre.

A szintetikus IDE és SCSI eszközök egyaránt 2 terabyte tárolókapacitással rendelkeznek.

Hálózati csatlakozók

Emulált eszközökkel 4 míg szintetikus eszközökkel 8 darab hálózati csatlakozót lehet használni.

A virtuális gépek között virtuális hálózatokat hozhatunk létre:

- *Külső hálózat:* Ekkor lehetőségünk van két azonos fizikai szerveren lévő virtuális gép közötti kommunikációra, virtuális gép és a szülőpartíció közötti kommunikációra és virtuális gép és egy külső hálózaton található hálózati eszköz közötti kommunikációra.
- *Belső hálózat:* Ekkor csak azonos szerveren található virtuális gépek között és a szülőpartíció között történhet kommunikáció.
- *Privát hálózat:* Ekkor csak két virtuális gép között van kapcsolat.

A Hyper-V lehetőséget biztosít arra, hogy futás közben allokáljunk további memóriát, processzormagokat, tárolóeszközöket és hálózati csatlakozókat is. De ezt a funkciót a vendég operációs rendszernek is támogatnia kell. Menet közbeni eltávolítására csak tárolóeszközök és hálózati csatlakozók esetén van lehetőség.

Vendég operációs rendszerek

A gyermek partíciókon tulajdonképen az összes ma használatos Microsoft asztali és szerver operációs rendszer támogatott:

- Windows Server 2008 x64 és x86
- Windows Server 2003 x64 és x86
- Windows Server 2000
- Windows Vista x64 és x86
- Windows XP Professional x64 és x86

Egyéb gyártótól származó operációs rendszerek:

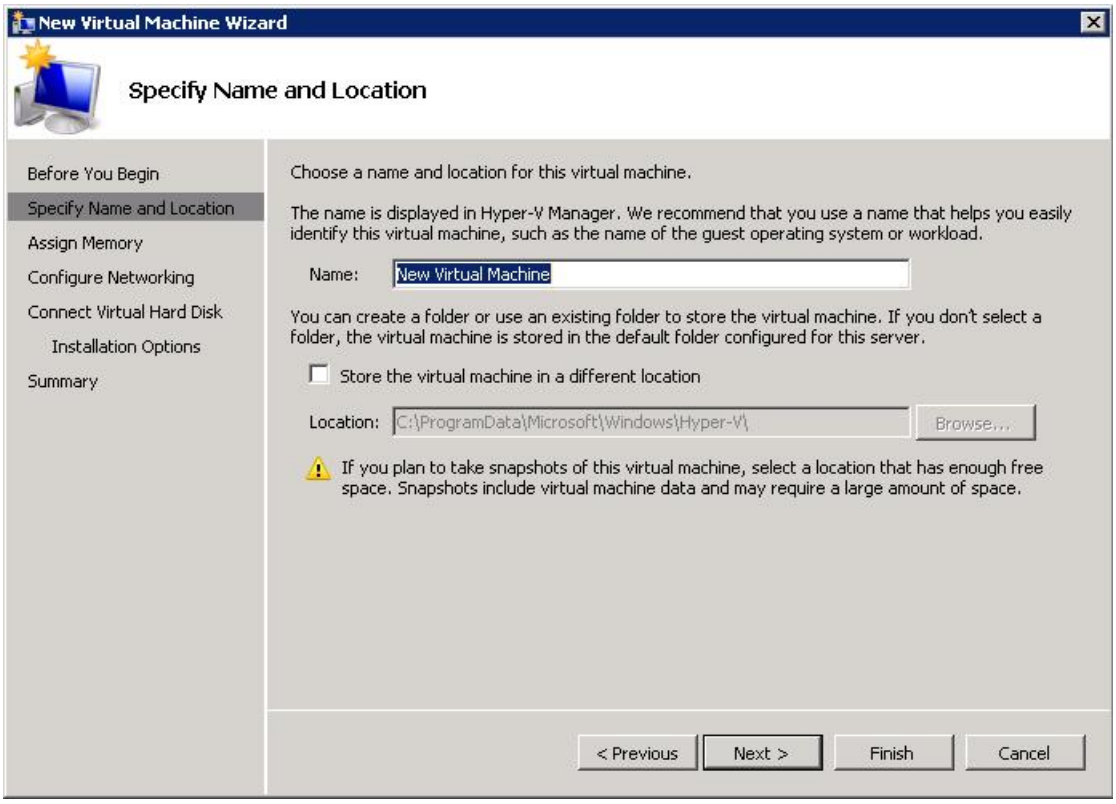
- SUSE Linux Enterprise Server 10 x64 és x86-os változatokban, a Service Pack 1 és Service Pack 2 is támogatott.

Természetesen más operációs rendszerek is működhetnek a Hyper-V technológia segítségével, de a Microsoft hivatalosan csak az utóbbiakat támogatja.

Hyper-V felügyelete

A virtuális gépekkel kapcsolatos feladatok elvégzését is egy MMC(Microsoft Mngement Console) grafikus felhasználói felület segíti, amelynek neve Hyper-V Manager. A Hyper-V Manager használatával egyszerűen létrehozhatunk, konfigurálhatunk és eltávolíthatunk virtuális gépeket, és minden virtuális gépről készíthetünk pillanatképeket. A pillanatképek(Virtual Machine Snapshot) segítségével lementhetjük az adott virtuális gép aktuális állapotát, ami úgy funkcionálhat mint egy ellenőrző pont, amivel visszaállíthatjuk a gép régebbi állapotát. Egy virtuális géphez több pillanatképet is készíthetünk, amelyeket hierarchiába rendezhetünk. Ez a funkcióhasznos lehet például alkalmazás tesztelésnél, ahol például egy operációs rendszer több verzióján is tesztelni szeretnénk a programot, például Windows XP SP1, Windows XP SP2 és Windows XP SP3 rendszereken, akkor nem kell állandóan telepíteni és eltávolítani a javítócsomagokat, elég csak betölteni azt a pillanatképet amelyre éppen szükségünk van.

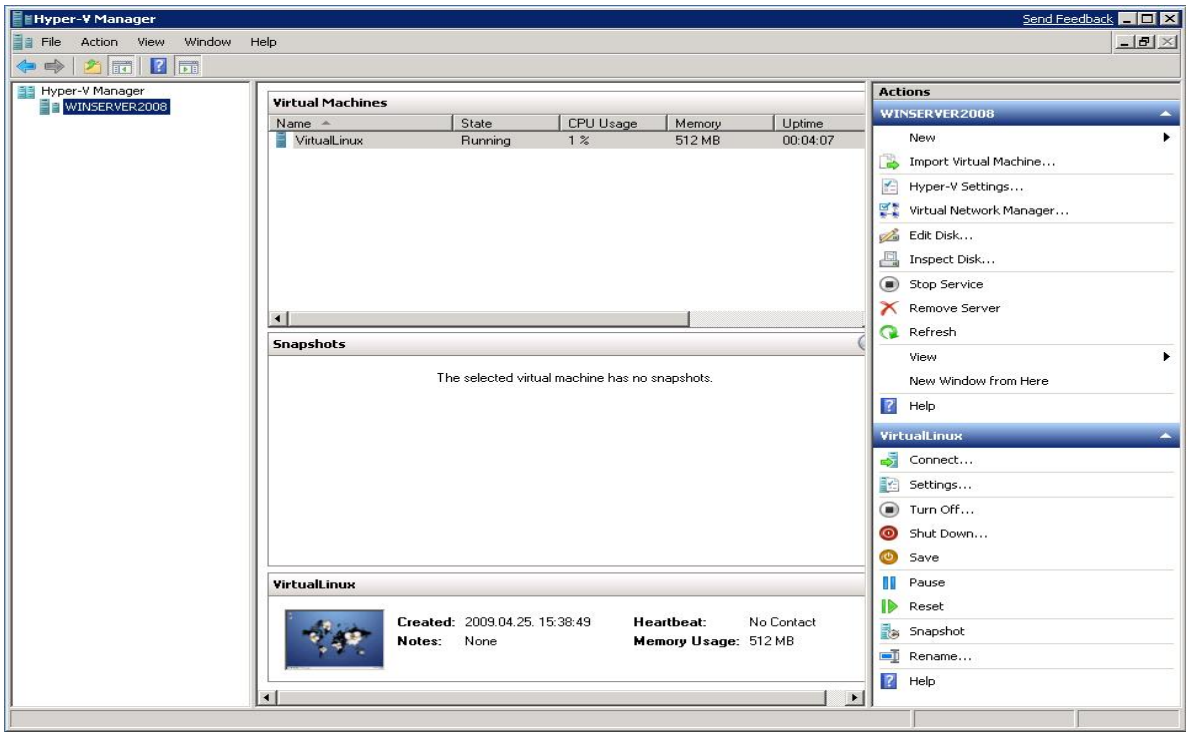
Egyszerűen létre tudunk hozni virtuális gépeket a Virtuális gép varázsló segítségével:



Megadhatjuk, hogy mennyi memóriát és tárhelyet használhat, hozzákapcsolhatjuk már létező virtuális hálózatokhoz, beállíthatjuk, hogy a Hyper-V kiszolgálón hol tárolódjanak a virtuális géphez tartozó állományok és lehetőségünk van közvetlenül létrehozáskor operációs rendszert telepíteni, akár hálózaton keresztül is, egy telepítőszerver segítségével.

Miután feltelepült az operációs rendszer a virtuális gépre, installálnunk kell az Integration Services funkciót is, amennyiben nem olyan rendszert használunk, amely alapból tartalmazza ezt a szolgáltatást(például Windows Vista). A telepítést egyszerűen elvégezhetjük, csak az adott virtuális gép *Action* menüjéből az *Insert Integration Services Setup Disk* opciót kell választanunk.

Ha végeztünk a konfigurációval, a virtuális gép már képes ellátni a neki szánt feladatkört. A Hyper-V Manager jobb oldali paneljein megtaláljuk a főbb vezérlési utasításokat mint például, indítás, leállítás és pillanatkép készítés.

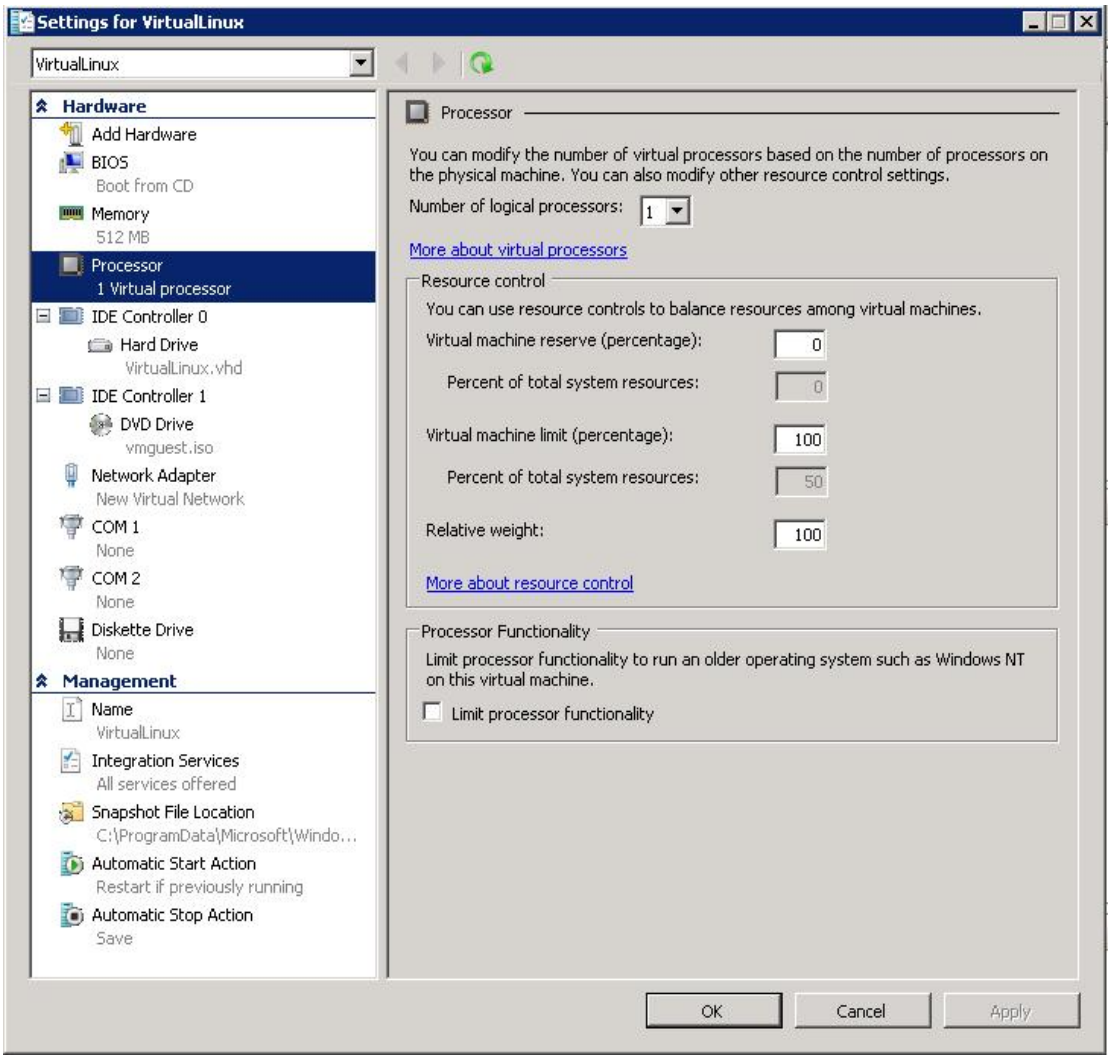


Hyper-V Manager

Amennyiben változtak a követelmények a virtuális géppel szemben, lehetőségünk van megváltoztatni annak paramétereit. Ehhez a Settings menüt kell megnyitnunk, ahol lehetőségünk nyílik további processzorok hozzárendelésére az adott géphez, növelni vagy csökkenteni a használatba vehető memória méretét, további tárolóeszközöket csatlakoztatni vagy eltávolítani és megváltoztatni a hálózati adapterek konfigurációit.

Továbbá a Settings menüben nyílik lehetőségünk az Integration Services egyes funkcióit engedélyezni vagy letiltani, például az idő szinkronizációt a szülő és a gyermek partíció között, valamint itt van lehetőségünk különböző automatizált feladatokat hozzárendelni eseményekhez, a virtuális géppel kapcsolatban, például automatikus leállás vagy indítás.

A következő képen a Settings menü látható:



Virtuális gép Settings menüje

Véleményem szerint ez a Hyper-V technológia ideális eszköz, hogy egy vállalat kihasználhassa a virtualizációval járó előnyöket, mint például költség megtakarítás, hardverkihasználtság optimalizációja vagy alkalmazás tesztelés.
Az általam ismertetett technológiákon kívül természetesen még számtalan lehetőséget hordoz magában, én csupán a rendszer alapjaiba szándékoztam betekintést nyújtani az olvasó számára.

Összefoglalás

Egy korszerű vállalat számára elengedhetetlen fontosságú tartani a lépést a megjelenő újabb és újabb technológiákkal szemben, hogy megőrizze piaci pozícióját és fejleszteni, bővíteni tudja a szervezet erőforrásait és szolgáltatásait.

A Microsoft szerver operációs rendszer családjának a legújabb tagja segítségével létrehozható egy olyan hálózati infrastruktúra, amely megfelel a mai korszerű technológiai elvárásoknak. A Windows Server 2008 számos forradalmi újítást vezet be, amelyek a lehető legnagyobb biztonságot, teljesítményt és rugalmasságot biztosítják az adott hálózatot felügyelő rendszergazdák és rendszer-adminisztrátorok számára.

Dolgozatom megírásának az volt a központi célja, hogy betekintést nyújtsak az Olvasó számára néhány általam fontosnak és érdekesnek tartott, a Windows Server 2008-ban megjelenő technológiába. Mivel ez a témakör hatalmas területet fed le, próbáltam azokra a fejlesztésekre rávilágítani, amelyek egy vállalat számára talán a legfontosabbak. Bízok benne, hogy az Olvasó hasznosnak találta a dolgozatban található információkat, és legalább annyira érdekesnek tartotta ezeket a technológiákat, amennyire én.

Irodalomjegyzék, források

Danielle Ruest, Nelson Ruest: Microsoft Windows Server 2008: The Complete Reference, McGraw-Hill 2008

Steve Seguis: Microsoft Windows Server 2008 Administration, McGraw-Hill 2008

Jonathan Hassell: Windows Server 2008: The Definitive Guide, O'Reilly 2008

William R. Stanek: Windows Server 2008: A rendszergazda zsebkönyve, SZAK kiadó 2008

http://www.microsoft.com/hun/windowsserver2008/home/default.aspx

http://msdn.microsoft.com/en-us/library/default.aspx

http://technet.microsoft.com/en-us/library/dd349801.aspx

http://technet.microsoft.com/hu-hu/library/cc706994.aspx

http://www.microsoft.com/hun/TechNet/archive/2008-07-08.mspx

Köszönetnyilvánítás

Köszönetet szeretnék mondani témavezetőmnek Dr. Krausz Tamásnak, a dolgozat megírásához szükséges források biztosításáért és a felmerülő kérdéseimre nyújtott válaszaiért.