Szakdolgozat

Bundik Sándor

Debrecen

2009

Debreceni Egyetem

Informatikai Kar

A Windows Server 2008 újdonságai

Témavezető:
Dr. Krausz Tamás
Egyetemi adjunktus

Készítette:
Bundik Sándor
Programtervező informatikus

Debrecen
2009

Tartalomjegyzék

1 BEVEZETÉS

A mai informatikában a biztonság jelenti a legnagyobb kihívást az informatikai rendszerekkel szemben. A hordozható számítógépek ellopása és a kártékony támadások ma már mindennapos eseménynek számítanak. A vállalati hordozhat számítógépek vírusokkal, biztonsági résekkel és lopásokkal szembeni védelme hatalmas számítástechnikai erőforrásokat igényel, nem beszélve azokról a felmérhetetlen károkról, amelyeket csupán az adatvesztések okozhatnak a vállalatok és azok ügyfeleinek számára. A virtualizáció és a megfelelő biztonsági eljárások együttes alkalmazásával úgy gondolom, hogy jelentősen növelhető az adatok és alkalmazások biztonsága. Ezért is döntöttem úgy, hogy dolgozatomban a Windows Server 2008 újdonságait bemutatva különösen nagy figyelmet fordítok a biztonság és virtualizáció témakörök megismerésére, és az ezekből eredő problémák bemutatására. A dolgozatom írása során megpróbáltam a különböző szolgáltatások közül azokat kiemelni, amelyek segítségével nagymértékben növelhető egy vállalat informatikai infrastruktúrájának biztonsága és teljesítménye.

Egy új szerver operációs rendszer megjelenése mindig egy új korszakot szokott kijelölni mind infrastrukturális, mind pedig fejlesztői szempontból. Minden a Windows NT-vel kezdődött, amellyel a Microsoft belépett a hálózati kiszolgálók piacára. A kezdetekben megjelent Windows NT 3.1-es és 3.5-ös változata nem hozta meg a várt sikereket, míg a továbbfejlesztett Windows NT 4.0 már sokak elismerését kivívta, nagyobb figyelmet kapott és szélesebb körben el is terjedt.

Az igazi előrelépés azonban a Windows 2000 Server megjelenésével történt, amelyhez teljesen átdolgozták az NT 4.0-t, és amelynek tervezésekor a stabilitás és a méretezhetőség volt az elsődleges szempont. A Windows Server 2000 esetén megtörtént az átverés, valódi nagyvállalati elosztott címtár született, a rendszerfelügyeleti platform és a skálázhatóság is új alapokra helyeződött, s pályára tette a következő generációs alkalmazás szervereket és felügyeleti alkalmazásokat.

Közben eltelt három év, és volt egy Windows Server 2003-as verzió, amely növelte rendszer biztonságát, javult a teljesítmény, nagy hangsúlyt fektettek az operációs rendszer

méretezhetőségére és a vállalati rendszerfelügyelet is hatékonyabbá vált. Ez a kiadás hozott néhány kényelmi funkciót és végre a .NET is a részévé vált, de funkcionális szempontból nem tatalmazott egetrengető újdonságokat.

A Windows Server 2008-as változattal nem ez volt a helyzet, hiszen eltelt további öt év és közben ismét sok minden változott az operációs rendszerek piacán. Az egyik, amit ezek közül ki lehet emelni az a virtualizáció, a Hyper-V technológia. A másik jelenség, amit érdemes kiemelni a Windows Server 2008-al kapcsolatban az a tendencia, ahogy egyre modularizálódik a rendszer, amelynek következtében egy szerver szerepkörrel kapcsolatban tényleg csak az odatartozó szolgáltatások települnek fel, például Server Core esetén.

A Windows 2000 Server és a Windows Server 2003 közötti átmenettől eltérően, ami inkább csak kisebb frissítés volt, a Windows Server 2008-ban radikálisan átírták a termék kódjának magját. A Windows Server 2008 alapkódjának jelentős része megegyezik a Windows Vistáéval, amelyet közvetlenül a biztonságos fejlesztési modell eljárásaira építve írtak. A Windows Server 2008 hatékony, sokoldalú kiszolgáló operációs rendszer, amely a Windows Server 2003 rendszerhez fejlesztett Service Pack 1 és Release 2 bővítéseire épül. A Windows Server és a Windows Vista számos közös szolgáltatással rendelkezik, hiszen egyetlen fejlesztési projekt részei. Ezek a szolgáltatások mindkét operációs rendszerben számos helyen felbukkannak, legyen szó akár felügyeletről, biztonságról, hálózatkezelésről vagy tárolásról. A Windows Server 2008 a Windows Server 2003-as változathoz képest jelentős mértékben továbbfejlesztett operációs rendszert tartalmaz. Az új funkciókon túlmenően érdemes megemlíteni továbbfejlesztett funkciókat, mint például a korszerű biztonsági és hálózatkezelési szolgáltatásokat, a kiszolgálói szerepkörök központi elérését, alkalmazások távelérését, a központi telepítést és fájlrendszert, valamint a továbbfejlesztett fürtkezelési technológiát. Ezeknek a továbbfejlesztett elemeknek köszönhetően a szervezetek könnyebben ki tudják használni a kiszolgálóik rugalmasságát, rendelkezésre állását és irányítását.

Összességében elmondható, hogy a Windows Server 2008 is egy korszakos lépés, a maga modularizált felépítésével, nyíltságával, a felügyelhetőségével, és mindenek felett az ASP .NET-el való mély integrációjával.

2 Windows Server 2008 termékcsalád bemutatása

A Windows Server 2008 a különböző méretű szervezetek eltérő igényeit figyelembe véve több termékváltozat formájában érhető el. A Windows Server 2008 kifejezés egy termékcsaládra utal, amelyben öt főbb kiadás áll rendelkezésre, ezek közül három a Windows Server Hyper-V technológia nélkül is elérhető, így a termékváltozatok száma összesen nyolc. A különböző kiszolgálók alapszolgáltatásai és felügyeleti eszközei azonban megegyeznek.

Windows Server 2008 Standard

Ez a kiadás a Windows Server 2003 közvetlen utódja, amely a hálózaton belüli további rendszerek számára biztosít szolgáltatásokat és erőforrásokat. A kiszolgálóba beépített webes és virtualizációs szolgáltatások révén fokozza a kiszolgálói infrastruktúra rugalmasságát és megbízhatóságát. Hatékony eszközeinek segítségével a kiszolgálók állandóan ellenőrizhetők, a konfigurációs feladatok pedig könnyen elvégezhetők. Megbízható és biztonságos vállalati operációs rendszer, amely számos funkcióval rendelkezik, és lehetővé teszi az egyidejű folyamatok két- vagy négyutas szimmetrikus feldolgozását (SMP – Symmetric Multi-Processing). A biztonsági funkciók biztosítják az adatok és a hálózat védelmét, továbbá egy megbízható alapot biztosít a vállalat működése számára.

Az operációs rendszer támogatja a többprocesszoros rendszereket maximum 4 darab processzormagig, továbbá lehetővé teszi 32 bites rendszereken legfeljebb 4 gigabájt, 64 bites rendszereken legfeljebb 32 gigabájt memória használatát.

Windows Server 2008 Enterprise

Nagyvállalati felhasználásra alkalmas platformot biztosít az üzleti szempontból kritikus fontosságú alkalmazások használatához. Ez a kiadás a Windows Server 2008 Standard szolgáltatásait egészíti ki, jobb skálázhatóságot és magas rendelkezésre állást biztosít, valamint támogatást biztosít további szolgáltatásokhoz, mint például a fürtöző szolgáltatás (Cluster Service) vagy az egyesített címtárszolgáltatás (Active Directory Federated Service). Az Enterprise kiadás kimagasló üzleti értéket kínál, és megfelelő alapot biztosít egy

dinamikus IT-infrastruktúra kiépítéséhez. Ez az operációs rendszer 32 bites rendszereken 64 gigabájt memóriát, 64 bites rendszereken 2 terrabájt memóriát tud kezelni, ami akár a kiszolgáló futása közben is bővíthető, és akár 8 processzort is képes támogatni az igények kielégítése érdekében.

Windows Server 2008 Datacenter

A három kiszolgáló közül a legnagyobb teljesítményű Windows kiszolgáló. Nagyarányú munkaterheléshez és virtualizációhoz ideális operációs rendszer. A korlátlan virtualizációs használati jogoknak és a Hyper-V virtualizációs technológiának köszönhetően a rendszer korlátlan virtualizációs jogosultságot biztosít a nagyszámú Windows Server 2008 példány működtetéséhez. Ez elősegíti a licencgazdálkodási problémák és költségek csökkenését. A magas rendelkezésre állást segítik a fürtszolgáltatások és a dinamikus hardverpartícionálási lehetőségek.

A Datacenter kiadás megfelelő alapot nyújt a nagyvállalati virtualizációs és vertikálisan méretezett megoldások kiépítéséhez. Támogatja a nagy memóriás konfigurációkat, 32 bites rendszereken akár 128 gigabájt memória, 64 bites rendszereken akár 2 terrabájt memória kezelésére is alkalmas. A rendszer legkevesebb 2 processzort igényel, de képes 64 processzort is kezelni.

Windows Web Server 2008

A Windows Server 2008 webes kiadása, amely ideális webes alkalmazások és szolgáltatások hosztolására. Feladata a weblapok és alkalmazások kiszolgálása, így ez a kiadás csak az ide tartozó szolgáltatásokat biztosítja. További érdekessége még, hogy az előző generációs Windows-kiszolgálókban lévő Web Edition most már sokkal hangsúlyosabb nevet kapott, ezentúl Windows Web Server névre hallgat.

Az elődtől eltérően a Windows Web Server 2008 jobb processzor és memória képességekkel rendelkezik. Ez a kiadás tartalmazza a frissen áttervezett Internet Information Services (IIS 7.0), ASP.NET, a Microsoft .NET Framework környezetet, valamint egy alkalmazás kiszolgáló és hálózati terheléselosztási (NLB – Network Load Balancing) szolgáltatást. A Windows Web Server 2008 összes alapszolgáltatása mind be van építve a Windows Server 2008 család többi tagjába is. A kiszolgáló számos további szolgáltatást

nélkülöz, így például a DNS, WINS, a DHCP és a címtár-szolgáltatási funkciókat. A Windows Web Server segítségével egyszerűen megvalósítható a webes környezet skálázhatósága és teljesítményének növelése. Ez az operációs rendszer 32 bites verzióban 4 gigabájt, 64 bites verzióban 32 gigabájt memória használatát támogatja, és legfeljebb 4 processzort támogat.

Windows Server 2008 for Itanium-Based System

Ez a kiadás nagyméretű adatbázisok, üzleti és egyéb alkalmazások kiszolgálására készült. A vállalatok működésének kiszolgálása érdekében a magas rendelkezésre állás mellett akár 64 processzorral is üzemeltethető.

Windows HPC Server 2008

A Windows HPC Server a nagyteljesítményű számítástechnika következő generációja, amely nagyvállalati eszközöket kínál a hatékony HPC-környezetek megvalósításához. A Windows Server 2008 rendszer alapjaira épül, 64 bites technológiával működik és akár több ezer processzormagra is méretezhető a rendszer. A feladatütemezés terén megvalósított együttműködő-képesség lehetővé teszi, a különböző rendszerű HPC folyamatok integrációját.

Ez a kiadás alkalmas a rendszer állapotának megfigyelésére és karbantartására, továbbá biztosítja a kötegelt és a szolgáltatásorientált alkalmazások (SOA) jellegű munkaterhelések támogatását.

3 Windows Server 2008 telepítése

A Windows Server 2008, ennek az igencsak terjedelmes rendszer megismerésének egyik legjobb módja ha megnézzük, hogy milyen komponenseket telepíthetünk fel vagyis, hogy milyen lehetőségek és eszközök állnak a rendelkezésünkre az új szerver operációs rendszerben.

A telepítés első lépései

Telepítés során egy grafikus felületen ki tudjuk választani, hogy milyen verziójú Windows Server 2008-at szeretnénk telepíteni. Továbbá itt tudjuk eldönteni, hogy Server Core vagy teljes Windows Server 2008-at telepítünk, azon belül is Standard, Enterprise, Datacenter Edition-t vagy Windows Web Server-t.

Telepítéskor a szerver csak a legfontosabb, a működéshez és elinduláshoz feltétlen szükséges komponensekkel települ, ekkor még semmilyen szerepkör és képesség nem aktív még rajta. A rendszer első indításakor megjelenik az Initial Configuration Tasks ablak, ami nem más, mint az új Server Manager egy nézete. A Server Manager lehetővé teszi, hogy a szerverünket kényelmesen konfiguráljuk. A Server Manager a szerverre történő belépéskor automatikusan elindul, valamint hasznos adatokat és funkciókat tesz elérhetővé számunkra.

A korábbi verziókhoz képest változás történt a szerepkörök (Roles) és képességek (Features) hozzáadása esetén is. Már a Windows Server 2003 esetén is volt mód szerepkörök telepítésére, az azonban csak egyszerű varázsló volt arra, hogy a számunkra fontos, összetartozó képességek csoportját egyszerre telepítsük a rendszerre. Korábbi verzióknál megtehettük, hogy ugyanazt az Add/Remove programs menüpontból manuálisan érjük el. Windows Server 2008 esetén ez megszűnt, ezt a funkciót szintén a Server Manager vette át, ahol szerepkörök és képességek listájából tudom kiválasztani, hogy melyiket telepítsem. A szerepkör egy olyan feladat együttes, amely lehetővé teszi, hogy a kiszolgáló egy meghatározott feladatot lásson el a hálózaton. A legtöbb szerepkörhöz azonban további szerepkör szolgáltatások (Role Service) tartoznak, amelyek nem feltétlenül szükségesek az adott szerepkör működéséhez, csupán csak további képességeket tesznek lehetővé.

A rendelkezésre álló szerepkörök:

- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- Active Directory Federation Services
- Active Directory Rights Management Services
- Active Directory Certificate Services
- File Server
- Print Services
- Fax Server
- DNS Server
- DHCP Server
- Network Access Services
- Web Services (IIS)
- Windows Sharepoint Services
- Universal Description, Discovery, and Integration (UDDI) Services
- Windows Deployment Services
- Terminal Services
- Windows Media Services

A képességek egyfajta támogató funkciót látnak el, tehát lehetővé teszik a további szerepkörök és szerepkör szolgáltatások működését, vagy pedig további extra, szerepkörhöz nem köthető szolgáltatásokat (funkciókat) tesznek elérhetővé. A Server Manager segít abban, hogy a szervert könnyebben tudjuk beállítani és ezen belül nemcsak szerepkörök telepítésére és eltávolítására alkalmas, hanem ezek napi szintű kezelésére is.

A Windows Server 2008 telepítésekor a rendszert a hálózaton neki szánt szerepkörnek megfelelően kell beállítani az alábbi irányelveket követve:

- A munkaállomások és a kiszolgálók általában egy munkacsoport vagy egy tartomány részei.
- A munkacsoport számítógépek laza rendszere, amelyben minden számítógépet egyedileg kezelünk.

- A tartomány számítógépek olyan csoportja, amelyet együttesen tartományvezérlők segítségével felügyelünk. A tartományvezérlők olyan Windows 2008 kiszolgálók, amelyek kezelik a hálózati elérést, a címtáradatbázist és a megosztott erőforrásokat.

Távoli telepítés

A Központi Windows-telepítési szolgáltatás (Windows Deployment Services, WDS) a korábbi Windows Server 2003-ban már jelen lévő RIS-t (Remote Installation Services) váltja fel. A WDS számos újdonságot tartalmaz, ezek közül talán a legjelentősebb a WIM (Windows Imaging Format), amely egy olyan formátum, amely az operációs rendszer lenyomatát tárolja. Egy WIM fájlon belül akár több rendszerindító lemezkép is lehet. Ugyancsak lehetőség van például az alkalmazásokat külön image-ben tárolni a WIM fájlon belül, tehát akár gépenként is eldönthetjük, hogy melyekre mely alkalmazások kerülnek. WDS segítségével lemezképekről tudunk telepíteni, de az igazi jelentősége abban rejlik, amikor különböző kiépítésű és felületű rendszerekre, különböző rendszerindítási és telepítési lemezképeket tartalmazó WIM fájlokat állítunk be. Rendszerindító operációs rendszerként, telepítéshez és hibaelhárításhoz is használható a Windows PE (Windows Pre Environment), amely egy grafikus felületű végrehajtási környezet, és minden olyan eszközt tartalmaz, ami szükséges lehet ahhoz, hogy telepítsük a Windows Server 2008 rendszert.

Távoli telepítés esetén, a PXE hálózati kapcsolaton keresztül felállítódik a Windows PE környezet, amely segítségével a távoli telepítés történik, majd ezt követően pedig a rendszerindító lemezképek letöltésre kerülnek. A WDS-t futtató gépen elérhető minden lemezkép, a felhasználó kiválasztja a célt és a telepítő pedig elhelyezi a WIM lemezképet a célszámítógép merevlemezén. Parancsfájlok és a WDS együttműködésével még inkább önműködővé tehető az operációs rendszerek telepítése. Parancsfájlokkal testre szabhatjuk a telepítendő programokat, termékkulcsokat, a telepítő kérdéseire adott válaszokat, így egy egységes rendszerünk lehet minden számítógépen. A WDS-ben kétféle felügyelet nélküli telepítő fájl létezik. Az egyik a WDS-ügyfél felügyelet nélküli telepítőfájlja, amelyet a WDS-kiszolgáló tárol. A másik a lemezképeknek a felügyeleti nélküli telepítőfájlja, amely a telepítésnek azt a részét automatizálja, amelyet a WDS-telepítőfájl nem tud kezelni.

4 A Windows Server 2008 és a Windows Vista

A Windows Vista és a Windows Server 2008 fejlesztése eredetileg egyetlen projekt volt, így számos közös technológia található bennük a hálózatkezelés, a tárolás, a biztonság és a felügyelet területén. A két operációs rendszer fejlesztése, ugyan külön kiadásokra vált szét, a továbbfejlesztett elemek jelentős része mindkét verzióra érvényesek. A Windows Vista és a Windows Server 2008 közös kódbázisra épülő szolgáltatásai azonos kezelőfelületen keresztül érhetők el. Természetesen az alapértelmezett beállítások között is akadnak olyan kivételek, amelyek nem egyeznek meg mindkét operációs rendszerben. Így például a Windows Server 2008 nem tartalmazza Windows Aero bővítéseket, a Windows minialkalmazásokat és más egyéb grafikus kiegészítőket. Ennek az az oka, hogy a Windows Server 2008 elsődleges célja az, hogy a kiszolgálói feladatokhoz optimális teljesítményt nyújtson.

A Windows Vista és a Windows Server 2008 is új architektúrával rendelkezik, amelynek főbb jellemzői a következők:

Modularizáción és lemezképek használatán alapuló nyelv- és hardverfüggetlen felépítés

A modularizáció segítségével az operációs rendszer minden összetevőjét független modulként lehet kezelni, amelyet egyszerűen eltávolíthatunk vagy üzembe helyezhetünk. A Windows Server 2008 operációs rendszer WIM (Windows Imaging Format) formátumú lemezképet tartalmazó hordozókon került forgalomba, amelyek a tömörítés és egypéldányos tárolási eljárás révén jelentősen csökkentik a lemezkép állományok méretét.

Telepítés és rendszerindítás előtti környezet

A telepítés előtti környezet, azaz a Windows Preinstallation Environment 2.0 (Windows PE) az MS-DOS helyét veszi át, és rendszerindító környezetet biztosít a telepítéshez, helyreállításhoz és hibakereséshez. A rendszerindítás előtti környezet az operációs rendszer indítását teszi lehetővé egy rendszerbetöltő program segítségével.

Felhasználói fiókok beállításai és hozzáférési jogok módosítása

A felhasználói fiókok felügyeletére szolgáló UAC (User Account Control), az általános és rendszergazda jogosultságú felhasználók fiókjainak szétválasztásával növeli a számítógép

biztonságát. A UAC miatt egy alkalmazás vagy általános felhasználói, vagy rendszergazdai jogosultságokkal futhat. Ha egy rendszergazdai jogosultságot igénylő alkalmazást futtatunk, akkor megjelenik a jogosultságkérő biztonsági prompt, amelynek működési módja a csoportházirend beállításokon múlik.

5 A Windows Server 2008 fontosabb újdonságainak rövid áttekintése

A Windows Server 2008 alapkódja egy biztonságos fejlesztési modell (SDM, Secure Development Modell) eljárásaira építve született meg. Ez a modell nagy változást jelentett, mert mindent a kód biztonságossá tételének rendelt alá. A termékben található számos új és továbbfejlesztett szolgáltatás, egy biztonságosabb alapkódnak az eredménye. A Windows Server 2008-ban a legjelentősebb változások a Server Core és az Internet Information Services 7.0 megjelenése volt.

Server Core

A Server Core (kiszolgálómag) a Windows Server 2008 telepítési lehetősége, amely segítségével az operációs rendszer legalapvetőbb szolgáltatásai kerülnek telepítésre. Meghatározott szolgáltatásokat és korlátozott felügyeleti kezelőfelületet tartalmaz. A felügyeleti funkciók csak parancssoron keresztül érhetők el, és a futtatható szolgáltatások köre is korlátozott, ezáltal csökkentve a rendszer támadási felületét.

A Windows Server Core a következő szerepköröket támogatja:

- DHCP (Dynamic Host Configuration Protocol) kiszolgáló
- DNS (Domain Name System) kiszolgáló
- Fájlkezelés és nyomtatás
- Active Directory tartományi szolgáltatások (AD DS)
- Írásvédett tartományvezérlő (RODC)
- Active Directory Lightweight Directory – szolgáltatások (AD LDS)
- Windows Media Services (WMS)
- Internet Information Server 7.0 (IIS 7.0)

A Server Core kisebb mérete lehetővé teszi az operációs rendszernek, hogy kevesebb rendszererőforrást használjon fel, valamint a rendelkezésre álló minimális felület a támadások is hatékony védelmet nyújt. Ezen kívül biztonságos megoldást jelent még az, hogy Server Core-al a kiszolgáló írásvédett tartományvezérlőként is működhet, amelyen mindent titkosíthatunk a BitLocker segítségével. A Server Core gépek ezen kívül még távolról is kezelhetők PowerShell segítségével, hálózati terheléselosztást alkalmazhatnak, részt vehetnek Microsoft fürtökben és megfigyelhetők egyszerű hálózatkezelési protokollon (SNMP) keresztül.

Internet Information Services 7.0

A Windows Server 2008-ban az IIS 7.0 jelentős változásokon esett át. Az IIS terméket biztonsági szempontokat szem előtt tartva újratervezték. Teljes mértékben bővíthető és teljes egészében az összetevőkön alapul. Csak azokat a szolgáltatásokat telepítjük, amelyekre szükségünk van, ezáltal egy biztonságosabb és megbízhatóbb üzemeltetést lehet elérni.

A legfontosabb fejlesztések a következők:

- A modulok tetszőlegesen tölthetők be függőségek nélkül, ami lehetővé teszi, hogy a kiszolgálón csak az általunk meghatározott alkalmazások fussanak, és csak azt csinálja amivel megbíztuk.
- A webalkalmazások és szolgáltatások gyorsabban üzembe helyezhetők és konfigurálhatók a kiszolgálófarmon. Az IIS 7 szinte minden beállítását megadhatjuk egy szövegfájlon keresztül, a weblapok beállításait egy `web.config` fájlon keresztül szerkeszthetjük.
- A kiszolgálói és webes alkalmazások jobban felügyelhetők. Az IIs 7 kezelőfelületét teljesen újratervezték, így sokkal feladatközpontúbbá vált.
- A biztonság javítására nagy hangsúlyt fektetnek, ezáltal egy biztonságosabb webes platform alakult ki. Az IIS 7 esetében a .NET alkalmazások közvetlenül az IIS magjában futnak, nem pedig az ISAPI (Internet Services Application Programming Interface) futtatja azokat.
- Nagyobb teljesítményű és jobban méretezhető webalkalmazások és szolgáltatások.

- FastCGI támogatással dinamikus nyelven alapuló alkalmazásokat is lehet futatni Windows alapú kiszolgálókon.
- Részletesen ellenőrizhető, hogy hogyan és mikor használják az alkalmazások és a szolgáltatások az operációs rendszer erőforrásait
- Az IIS 7 eléréséhez használható a Windows PowerShell parancssor környezet is.

Active Directory : Írásvédett tartományvezérlők

A Windows Server 2008 operációs rendszerben egy újfajta tartományvezérlő-konfiguráció jelenik meg, ez az Írásvédett tartományvezérlő (Read-Only Domain Controller, RODC). Ennek köszönhetően olyan helyeken is lehet tartományvezérlőket működtetni, ahol nem garantálható a tartományvezérlő fizikai védelme. Az írásvédett tartományvezérlők csak egy, olvasható másolatot tartalmaznak az Active Directory-ról, ezáltal biztonságot nyújtanak az esetleges támadásoktól. Ezen tartományvezérlő segítségével az Active Directory egy írásvédett példánya közelebb kerülhet a más telephelyen dolgozókhoz, ezáltal gyorsabbá válik a bejelentkezés, hatékonyabban érhetők el a hálózati hitelesítési erőforrások, és a biztonságot is javítja.

Következő generációs TCP/IP

A Windows Server 2008 teljesen újratervezett TCP/IP protokollcsomagot tartalmaz. Az IP protokoll 4-es verzióját (IPv4), és 6-os verzióját (IPv6) egyaránt támogatja. Amíg a 32 bites címzést lehetővé tevő IPv4 a legelterjedtebb internetprotokoll, addig a 128 bites címzést lehetővé tevő IPv6-ot az internetprotokoll követező generációjának tartják. Az IPv6 128 bites címei nyolc, egyenként 16 bites blokkokból állnak, amelyeket kettőspont választ el egymástól. Minden 16 bites blokkot egy hexadecimális érték ír le. IPv6-címzés esetén az IP-cím első 64 bitje a hálózati azonosító, míg az utolsó 64 bitje a hálózati interfész. A következő generációs TCP/IP-megvalósítás tervezésénél fő cél az volt, hogy javítsanak a hálózatkezelés sebességén és hatékonyságán. A kommunikáció biztonságát az IPsec jobb beépülése biztosította a TCP/IP verembe.

TCP/IP-verem

A fejlesztések jelentős része a TCP/IP-vermet érinti. Az egyik ilyen fejlesztés a TCP ablakméretének automatikus hangolása. Ez a funkció a nagy mennyiségű adatok átvitelének hatékonyságát növeli ugyanazon hálózaton belül, mivel a Windows Server 2008 képes önmagától megváltoztatni a fogadási ablak méretét. A hálózat méretezési lehetőségeit is továbbfejlesztették. A korábbi verziók esetén egy hálózati kártya egyetlen processzorhoz társult. A Windows Server 2008 ezzel a funkcióval a hálózati kártyákat és a rajtuk áthaladó forgalmat több processzor között is képes elosztani, ami lehetővé teszi, hogy egy-egy hálózati kártya sokkal nagyobb adatmennyiséget fogadjon.

Terminálszolgáltatások

Három teljesen új terminálszolgáltatás jelent meg a Windows Server 2008-ban. Az egyik a Terminal Services RemoteApp, amely lehetővé teszi, hogy közvetlenül futtassunk programokat egy kiszolgálóról, tehát központi hozzáférést biztosít az alkalmazásokhoz anélkül, hogy ehhez a teljes távoli asztalt kellene szolgáltatni. A felhasználó számára úgy tűnik, mintha az alkalmazás a helyi számítógépen futna, miközben csupán csak a távoli számítógépen futó alkalmazás megjelenítését észleli.

A második új szolgáltatás a Terminal Services Gateway, amely lehetővé teszi a felhasználónak, hogy a terminálszolgáltatások által nyújtott alkalmazásokat bármilyen webes portálról biztonságosan elérhessék egy titkosított HTTPS-csatornán keresztül.

A harmadik újdonság a Terminal Services Web Access, amely segítségével a rendszergazda nyilvánosan közzéteheti a hozzáférhető terminálprogramokat egy weboldalon. Ez még szélesebb körű lehetőséget nyújt arra, hogy a felhasználók hozzáférjenek a távoli terminálon futó programokhoz és futtassák azokat. Terminálszolgáltatások segítségével a szervezetek virtuális magánhálózatok (VPN) használata és a tűzfalon felesleges portok megnyitása nélkül tudnak biztonságos hozzáférést biztosítani az alkalmazásokhoz. Ezen szolgáltatás segítségével lehet biztosítani az adatok és az alkalmazások biztonságos távelérését.

BitLocker

A BitLocker meghajtó titkosítás használatával az adathordozón található összes adat titkosítható. Olyan helyzetekre tervezték, amikor egy támadó fizikai hozzáférést próbál szerezni egy merevlemezes meghajtóhoz. A Windows Server 2000 és Windows Server 2003-ban alkalmazott titkosított fájlrendszer (EFS, Encrypting File System) már kísérletet tett a meghajtón lévő adatok védelmére azzal, hogy a biteket összekeverte a meghajtón, viszont a fájlok visszafejtéséhez szükséges kulcsok védelme nem volt megfelelő. Ezzel szemben a BitLocker a kulcsokat vagy egy TPM lapkában az alaplapon, vagy egy USB flash-meghajtón tárolja, amelyet rendszerindításkor kell csatlakoztatni. A BitLocker egyrészt titkosítja a Windows operációs rendszer teljes kötetét a merevlemezen, másrészt pedig ellenőrzi a rendszerindítás kezdeti szakaszában részt vevő összetevők sértetlenségét, és ha hibát talál, akkor megakadályozza a rendszerindítást.

Hálózatvédelem (Network Access Protection)

Ezen új keretrendszer segítségével a rendszergazda meghatározhatja a hálózattal szembeni alapkövetelményeket, és korlátozhatják azoknak a számítógépeknek a hálózattal való kommunikációját, amelyek nem teljesítik az előírt követelményeket. Ilyen alapkövetelményekkel előírható például, hogy milyen minimális szintű védelemmel kell ellátva lenniük azoknak a számítógépeknek, amelyek csatlakozhatnak a hálózathoz.

Windows-tűzfal

A Windows Server 2008 operációs rendszerben egy új, biztonságosabb tűzfal került bevezetésre, amely egyetlen beépülő MMC-modulban egyesíti a tűzfalszolgáltatások és az IPsec-kezelést. IPsec protokoll használatával ellenőrizhető a hálózati forgalom hitelessége, a felhasználó azonossága, a küldő és a címzett gép, valamint a nagyobb biztonság érdekében akár a hálózati forgalom is titkosítható. Ezáltal több szabályt lehet meghatározni, és egyszerűen adhatunk meg biztonsági követelményeket, mint például a hitelesítés vagy titkosítás. Ezen fokozott biztonságú Windows-tűzfal esetén nemcsak a bemenet, hanem a kimenet szűrésére is van lehetőség. További fejlesztések történtek a profilok támogatásában is, számítógépenként külön profilokat adhatunk a tartományhoz kapcsolódó gépek, a magánhálózati kapcsolatok és a nyilvános hálózati kapcsolatok számára.

Active Directory replikációja

A Windows Server 2008 verzióban ezen szolgáltatás a korábbinál hatékonyabban működik. Az Active Directory a változások replikálásához az elosztott fájlrendszeri replikáció (DFS-R) szolgáltatást használja. Ez a szolgáltatás csak az attribútumok változásait replikálja, így csökkenti a kommunikációs csatornán keresztül továbbítandó adatok mennyiségét.

Kiszolgálóvirtualizáció

A kiszolgáló virtualizálása révén egyetlen számítógépen több operációs rendszer is futhat virtuális gépként. A kiszolgálóvirtualizáció lehetővé teszi a nem megfelelő kihasználtságú kiszolgálói számítógépek munakterhelésének összevonását, kevesebb számú jól kihasznált kiszolgálókra. Ezen technológia segítségével kevesebb fizikai számítógépre van szükség, így csökkenthetők a kiadási költségek. A Windows Server 2008 rendszer a kiszolgálóvirtualizációhoz szükséges összes elemet beépítve tartalmazza a Windows Server Hyper-V technológia formájában. A Windows Server 2008 Hyper-V, a következő generációs hipervizor-alapú kiszolgálóvirtualizációs technológia. Több szerepkör egyetlen fizikai számítógépen, több virtuális gép formájában történő összevonásával lehetővé teszi a hardverberuházások legjobb kihasználását. A Hyper-V dinamikus, megbízható, és méretezhető virtualizációs platform, amely kiegészül a virtuális és fizikai erőforrások kezelésére alkalmas felügyeleti eszközökkel.

Kiszolgálókezelő (Server Manager)

A kiszolgálókezelőben (Server Manager) egy helyen tekinthetünk meg minden információt a kiszolgálóval kapcsolatba. Használatával egyszerűen adhatunk hozzá és konfigurálhatunk szerepköröket, szolgáltatásokat, valamint információkat kaphatunk azok állapotáról és elháríthatjuk az esetleges beállítási hibákat.

A Server Manager grafikus formában csak a helyi számítógép kezelésére alkalmas, míg a parancssoros változata a WinRM (távoli számítógép-kezelési protokoll) segítségével alkalmas távoli számítógépek felügyeletére. A Server Manager parancssoros változatának indítása a következő segítségével történik:

- `servermanagercmd.exe`

Ez a funkció Server Core változat alatt nem elérhető, viszont nagy jelentősége van az automatizálás és a távoli menedzsment alkalmazásában. A Server Manager a Configure Your Server, Manager Your Server és a Security Configuration Wizard felületeket váltja fel. Ennek segítségével az egyes elemeket egy helyről kezelhetjük.

Windows Deployment Services

Az előző generációs Windows-kiszolgálókban bővítményként elérhető távtelepítési szolgáltatás (Remote Installation Services, RIS) továbbfejlesztéseként jelent meg ez a szolgáltatás. A Központi Windows-telepítési szolgáltatások (Windows Deployment Services, WDS) segítségével automatizálható az operációs rendszer telepítése a hálózat távoli számítógépén is. Használatával gyorsan üzembe helyezhetők az új rendszerek, és telepítéséhez csak minimális felhasználói beavatkozás szükséges.

Active Directory

A Windows Server 2008 fejlesztésekor több fontos változás került bevezetésre az Active Directory-szolgáltatásokban. Ezek alapja, hogy a Microsoft átszervezte a címtár működését és létrehozott egy szolgáltatás családot, amely számos rokon szolgáltatást tartalmaz. A számos továbbfejlesztések segítségével fokozták az Active Directory alapú hálózatok támogatását és biztonságát.

Az Active Directory a következő szolgáltatásokat biztosítja:

Active Directory tartományi szolgáltatások (*Active Directory Domain Services*)

Az AD DS az Active Directory lelke és nélkülözhetetlen a címtárat használó alkalmazások számára. Az Active Directory tartományi szolgáltatások a konfigurációs adatok, a hitelesítési kérelmek és az erdőn belül tárolt összes objektumra vonatkozó információk központi helye. Az AD DS biztosítja a tartományok létrehozásához szükséges címtárszolgáltatásokat többek között az adattárat, amely a hálózat objektumairól tárol és tesz elérhetővé információt. Az AD DS tartományvezérlőkön keresztül kezeli a hálózati erőforrásokhoz történő hozzáférést.

Active Directory egyszerű címtárszolgáltatás (*Active Directory Lightweight Directory Services*)

Az AD LDS segítségével a címtárhasználatra felkészített alkalmazások számára nyújtható címtárszolgáltatás. Az AD LDS adattárat biztosít az olyan, címtárat használó alkalmazások számára, amelyek nem igénylik az AD DS-t. Az AD LDS nem az operációs rendszer szolgáltatásaként fut, viszont együttesen használható az AD DS szolgáltatással, így egy központi helyen találhatók meg a biztonsági fiókok, és egy másik helyen pedig az alkalmazáskonfigurációs és címtári adatok. Az AD LDS használatával csökkenthető az Active Directory replikálásához kapcsolódó feladatok mennyisége.

Active Directory tanusítványszolgáltatások (*Active Directory Certificate Services*)

Az AD CS a digitális bizonyítványok kibocsátásához és visszavonásához szükséges funkciókat tartalmazza a felhasználók, a számítógépek és a kiszolgálók számára. Az AD CS ehhez tanusítványszolgáltatókat vesz igénybe, amelyek felelősek a felhasználók és számítógépek azonosságának ellenőrzéséért, valamint az azonosságot igénylő tanusítványok kibocsátásáért. Az Active Directory tanusítványszolgáltatások a fokozott biztonság érdekében a személyek, eszközök, szolgáltatások identitását saját titkos kulcsához kapcsolják. A tanusítvány és a titkos kulcs Active Directory rendszerben való tárolása elősegíti az identitás védelmét.

Active Directory összevonási szolgáltatások (*Active Directory Federation Services*)

Az AD FS az AD DS hitelesítési és hozzáférés-kezelési szolgáltatásait egészíti ki azzal, hogy kiterjeszti ezen szolgáltatásokat a világhálóra. Segítségével biztonságosan lehet külső felhasználók számára hozzáférést adni a szervezet tartományi erőforrásaihoz.

Az AD FS beállítást követően a felhasználók digitális személyazonosságukkal hitelesíthetik magukat a weben, és hozzáférhetnek belső webes alkalmazásokhoz egy webböngésző segítségével.

Active Directory tartalomvédelmi szolgáltatások (*Active Directory Rights Management Services*)

Az AD RMS az adatok védelmére szolgál, lehetővé teszi az adatok védelmét a jogosulatlan hozzáféréssel szemben. Felhasználható annak biztosítására, hogy csak azok a

személyek férhessenek hozzá egy adott fájlhoz, akik számára ez szükséges. Az AD RMS szolgáltatás azonosítja, hogy milyen jogokkal rendelkeznek a felhasználók és a jogaiknak megfelelően meghatározza, hogy mely felhasználók férhetnek hozzá az adott fájlhoz és milyen műveletet végezhetnek rajtuk.

Windows PowerShell

A Windows PowerShell új parancsértelmező és parancsfájlnyelv, amely segítségével a rendszergazdák nagyobb hatékonysággal és könnyebben végezhetik el a munkájukat. A PowerShell .NET keretrendszerre épül így .NET objektumok segítségével történik a kommunikáció. A környezetnek ez az alapvető fontosságú változása új eszközöket és módszereket valósít meg. A Windows PowerShell újdonsága, a `cmdlet`, amely egyszerű, egyetlen funkciójú parancssori eszköz.

A Windows PowerShell jól használható bizonyos szerepkörök, például IIS7.0 és a terminálkiszolgáló kezelésére.

6 A Windows Server 2008 rendszerkövetelményei

A rendszerkövetelmények a rendszer konfigurációjától, valamint a különböző telepített alkalmazásoktól és funkcióktól is változhatnak. Míg a fájlkiszolgálókon a lemezek sebessége a legfontosabb, addig az alkalmazás kiszolgálókon a memória és a processzor sebessége az, ami leginkább befolyásolja a teljesítményt. A processzor teljesítménye nemcsak a processzor órajelétől hanem a processzormagok számától és a processzor gyorsítótárának méretétől is függ.

A következő táblázat a Windows Server 2008 minimális és javasolt rendszerkövetelményit mutatja be:

Hardver	Minimális követelmény	Javasolt követelmény
Processzor	1 GHz (x86) vagy 1,4 GHz (x64)	2 GHz vagy gyorsabb
Memória	512 MB	2GB vagy több
Szabad lemezterület	10 GB	40 GB vagy több

7 A Windows Server 2008 maximális rendszerkövetelményei

A következő táblázat a Windows Server 2008 termékcsalád tagjainak összehasonlítását tartalmazza maximális rendszerkövetelmény szempontjából:

Komponens	Web	Standard	Enterprise	Datacenter
Processzor (x86)	4	4	8	32
Processzor (x64)	4	4	8	64
Memória 32-bites operációs rendszer esetén	4 GB	4GB	64GB	128GB
Memória 64-bites operációs rendszer esetén	32GB	32GB	2T	2T
Csomóponti Failover Clustering	-	-	16	16
Terminálkiszolgáló csatlakozások	250	250	65535	65535
Virtualizáció (Hyper-V)	nincs	van	van	van

8 BIZTONSÁG

A biztonság jelenti a legnagyobb kihívást a vállalatok informatikai részlegei számára. A Windows Server 2008 egy alapjaiban újjáépített szerver operációs rendszer, amely minden kis komponensét részében és egészében is úgy tervezték, hogy a lehető legnagyobb biztonságot adja az üzemeltetők és a felhasználók számára.

8.1 Windows Server 2008 Server Core

A kiszolgálónak nagyon gyakran csak egy vagy maximum néhány feladatkört kell ellátnia, ezért ilyen esetekben sok szolgáltatás feleslegesen kerül telepítésre, ezzel növelve a biztonsági kockázatot, bonyolítva a karbantartást és a hibaelhárítást. A Windows Server 2008 telepítése közben választhatjuk ezt az új opciót, amely segítségével csak a legalapvetőbb állományok kerülnek a számítógépre.

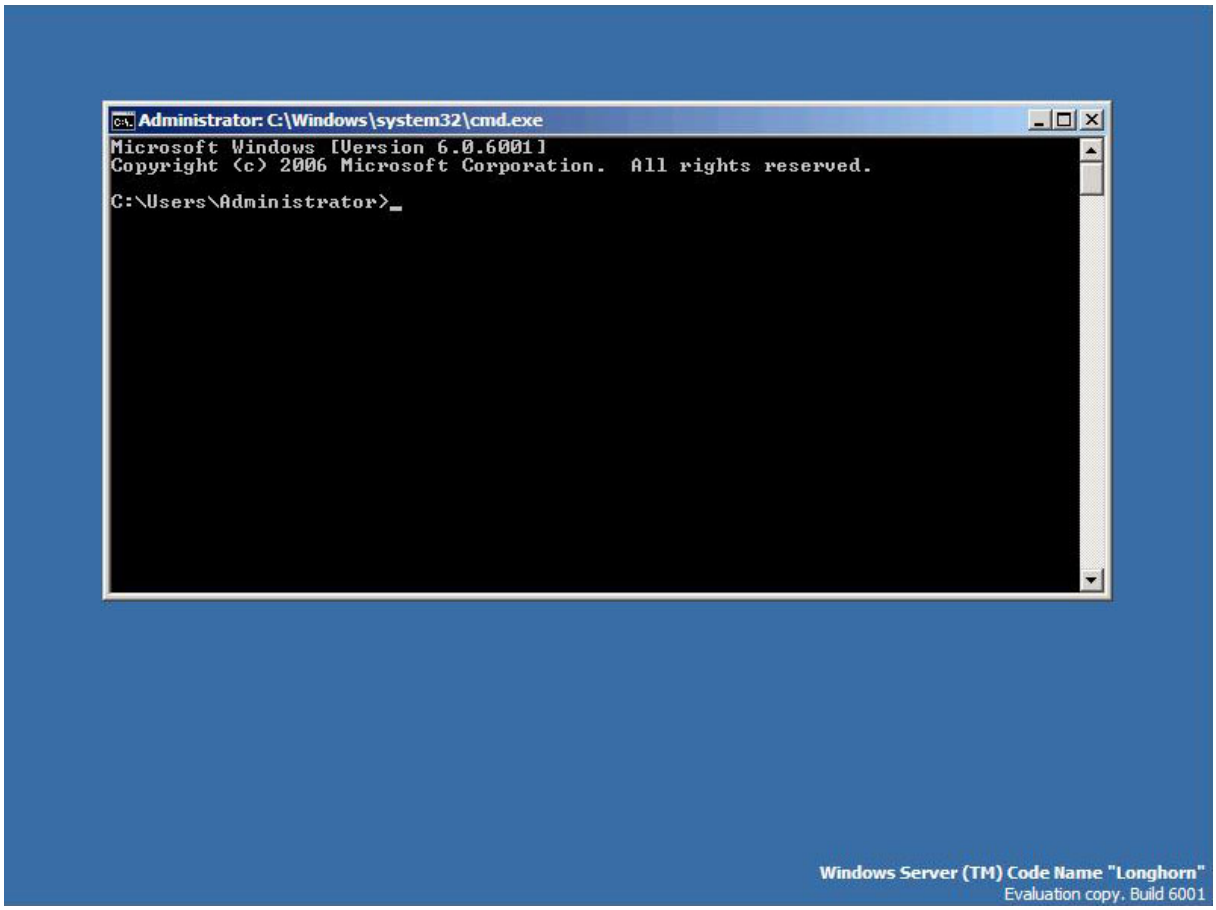
A Server Core egy olyan verziótól független telepítési mód, amelynek segítségével az operációs rendszer legalapvetőbb szolgáltatásai kerülnek telepítésre, ezáltal biztosítva a könnyebb menedzselhetőséget és a kisebb támadási felületet.

Különbsége elsősorban abból áll, hogy 95 százalékban parancssorból működik, azaz nincs grafikus interfész.
Több szempontból is előnyös a Server Core használata:

- Kisebb biztonsági kockázat
- Könnyebb menedzselhetőség
- Könnyebb hibaelhárítás
- Kisebb erőforrásigény
- Kisebb lemezterület igény
- Nagyobb megbízhatóság

Mind 32 és 64 bites rendszerek esetén is telepíthető ez a változat. Az operációs rendszer komponenseinek egy részét eltávolították és csak a legfontosabbak maradtak a rendszerben, csökkentve ezzel a támadási felületet.

Így például nem található meg ebben a változatban: grafikus felület, .NET Framework, MMC, CLR, Vezérlőpult, IE, grafikus help.



A Server Core kezelőfelülete

Server Core kiszolgálóverzió tulajdonságai:

- Kisebb hardveres erőforrást igényel, azaz lényegesen gyengébb számítógépen is jól működik. Ezen Windows-kiszolgálónak a teljes funkcionalitás biztosításához nem kevesebb mint 400 megahertzes CPU, 128 MB RAM és 6 GB szabad lemezterület szükséges.
- Számos kiszolgálói szerepkört képes ellátni, viszont ezek száma korlátozott.
- Kevesebbet kell biztonsági és egyéb javításokkal törődni, mivel nincs grafikus interfész és minimális alkalmazás fut.
- Megtalálható mind az Enterprise, a Standard és a Datacenter verziókban és egyformán használható x86 vagy x64 környezetben is.

A Windows Server 2008 Server Core változatban a következő szerepkörök és szolgáltatások használatára van lehetőség:

Szerepkörök	Szolgáltatások
Active Directory Domain Services	BitLocker meghajtótitkosítás
Active Directory Lightweight Directory Services	Feladatátviteli fürtszolgáltatás
DHCP-kiszolgáló	Többutas I/O
DNS-kiszolgáló	Cserélhető tároló kezelése
Fájlszolgáltatások	SNMP-szolgáltatások
Nyomtatószolgáltatások	UNIX-alapú alkalmazások alrendszere
Windows Server Virtualization	Telnet-ügyfél
Multimédia-szolgáltatások	Windows kiszolgáló biztonsági mentése
	WINS-kiszolgáló

Server Core parancsok:

Az alábbiakban felsorolt parancsok segítségével egy frissen üzembe helyezett Windows Server 2008 Server Core rendszerű kiszolgáló beállításait adhatjuk meg.

Kezdeti beállítások

- `net user administrator*`

Ez a parancs a rendszergazda jelszavának beállítására szolgál. Telepítéskor alapértelmezés szerint a Server Core egy beépített rendszergazdai fiókot hoz létre üres jelszóval, amelyet első bejelentkezéskor meg kell változtatni.

- `hostname`

A Server Core gép jelenlegi nevének lekérdezése.

- `netdom renamecomputer régi_név /NewName: új_név`

A kiszolgáló nevének módosítása régi névről új névre.

- `netdom join gépnév /domain:domain_név /userdd:user_neve /passwordd:*`

A kiszolgálókat a domain_név nevű tartományhoz szeretnénk csatlakoztatni. A userdd és a passwordd kapcsolók jelzik, hogy az adott azonosítójú felhasználó a megfelelő engedélyekkel rendelkezik ahhoz, hogy a gépet a tartományhoz csatolhassa.

- `netsh interface ipv4`

Hálózati kapcsolatok beállítására szolgáló parancsok csoportja.

- `netsh interface ipv4 show interfaces`

Ezen parancs segítségével hívhatjuk elő a Server Core összes beállított hálózati felületét. A kapott eredményből több adatot is hasznosítani tudunk, például a hálózati kapcsolat nevét, valamint sorszámát.

- `netsh interface ipv4 set address name =”Local Area Connection” source=static address=x.x.x.x mask=x.x.x.x gateway=x.x.x.x`

A netsh parancs set address kapcsolójának segítségével, statikus IP címet tudunk hozzárendelni egy géphez, a megfelelő maszkkal és átjáróval kiegészítve. A name utáni `Local Area Connection` a hálózati kapcsolat nevét jelzi.

- `netsh interface ipv4 add dnsserver name=”Local Area Connection” address=x.x.x.x index=1`

A netsh parancs add dnsserver kapcsolójának használatával DNS-kiszolgálót tudok hozzárendelni. Mivel több DNS-szerver is felvehető, ezért az index adja meg a használandó DNS-szerverek sorrendjét.

- `pnputil`

Segítségével a hardver-illesztőprogramokat tudjuk telepíteni, illetve frissíteni. A Serer Core támogatja a Plug and Play illesztőprogramokat, ezért ilyen esetekben az illesztőprogram fájljait át kell másolni a Server Core-ban található mappába, majd pedig a pnputil programot kell futtatni, például: `pnputil –i –a mappa_neve\<driver>.inf`

- `slmgr.vbs`

Ez a parancsfájl a megfelelő kapcsolókkal alkalmazva, felügyeli a felhasználási engedélyekkel és az aktiválással kapcsolatos feladatokat.

- `cscript slmgr.vbs –xpr`

Ellenőrzi a gép aktiválásához szükséges, jelenleg érvényben lévő felhasználási engedély állapotát és a lejárati engedélyét.

- `cscript slmgr.vbs –ato`

Ez a parancs végrehajtja az aktiválást.

Ellenőrzés és felügyelet

A felügyelet ellátható távolról több különböző módszer segítségével. Ezek a következők lehetnek:

- `control timedate.cpl`

Az idő/dátum beállítása.

- `Control intl.cpl`

Területi beállítások.

- `cscript scregedit.wsf au 4`

Automatikus frissítés engedélyezése a Server Core gépen, amely automatikusan letölti és telepíti a frissítéseket.

- `cscript scregedit.wsf /ar 0`

Segítségével engedélyezhető a távoli asztal kapcsolat (RDP).

- `cscript scregedit.wsf /cs 0`

Ha régebbi RDP-kliensről (RDP 6.0) szeretnénk kapcsolódni, akkor ezzel a parancssorral állíthatjuk át a biztonsági beállításokat.

- `WinRS`

A Windows Remote Shell vagy WinRS a Server Core gépen futó figyelőrészből, és a másik gépen lévő ügyfélszoftverből áll. Az ügyfélszoftver parancsokat küld a figyelőnek, a WinRS pedig ezeket végrehajtja és a kimenetet visszaküldi a parancsot kiadó ügyfélgépre. Miután a figyelőt beállítottuk küldhetjük WinRS-el a Server Core gépnek szánt parancsokat.

- `WinRM quickconfig`

A WinRS figyelő aktiválása a Server Core gépen.

Szerepkörök és szolgáltatások

A Windows Server 2008 Server Core által betölthető szerepkörök listáját az `oclist` nevű parancssori segédprogram segítségével tekinthetjük meg. Az oclist parancs kimenetéből nyert nevet felhasználva az `ocsetup` parancs kiadásával kezdhetünk neki a szerep telepítésének, például ha egy DHCP-kiszolgálót szeretnénk üzembe helyezni, akkor ezt a következő parancs segítségével érhetjük el: `ocsetup DHCPServerCore`

Az Active Directory telepítése azonban kívül esik az ocsetup hatáskörén. A tartományvezérlő Server Core gépre történő telepítésének egyetlen támogatott megoldása a `dcpromo` segédprogram használata, felügyelet nélküli módban.

Felügyelet nélküli módhoz össze kell állítani egy szövegfájlt, amely vezérelni fogja a telepítést, parancssori indítással.

Egy szövegfájlba legalább az alábbi beállításokra van szükség:

```
[DCInstall]
ReplicaOrNewDomain=Domain
NewDomain=Forest
NewDomainDNSName=xxx.yyy
AutoConfigDNS=Yes
DNSDelegation=Yes
DNSDelegationUserName=username
DNSDelegationPassword=password
RebootOnSuccess=NoAndNoPromptEither
SafeModeAdminPassword=
```

Futatása a következő paranccsal történik: `dcpromo /unattend:fájlnév.txt`

8.2 Hálózatvédelem (Network Access Protection)

Egy vállalati hálózathoz általában nagyon sokan csatlakoznak, ezért sok esetben az egyik legnagyobb problémát a hálózatok számítógépeinek védelme jelenti. Itt elsősorban a veszélyek elhárításáról, megelőzéséről van szó, amelyet a hálózatra csatlakozó munkaállomások jelentenek. A Windows Server 2008-ba beépítettek egy teljesen új technológiát, amely lehetővé teszi, hogy a számítógépek még a hálózatra csatlakozás előtt egy

ellenőrzésen essenek át, amelyet a rendszergazda határozhat meg. Ha a gép nem felel meg az ellenőrzésnek, akkor megtagadható tőle a hálózathoz való hozzáférés. Ekkor egy úgynevezett karanténba kerül a kliens egészen addig, amíg nincsenek pótolva a hálózat használatához szükséges elvárások és feltételek. Ezen szolgáltatás neve Network Access Protection (NAP).

A NAP biztosítja azt, hogy csak az egészséges kliensek férhessenek hozzá a hálózati erőforrásokhoz, valamit segít elérni ezt az egészséges állapotot. Az egészséges állapot az egy olyan állapot, amikor a számítógépek megfelelnek minden olyan feltételnek, amelyet a NAP házirendben meghatároztunk.

NAP elődjei

A NAP-hoz hasonló megoldások már a Windows Server 2003-ban is megjelentek. Ennek neve a Network Access Quarantine Control (NAQC), amely a karanténkezelésnek egy korlátozott változata volt. A NAQC csak távolról csatlakozó kliensek felügyeletére volt használható, tehát csak a saját gépét védte meg a távoli felhasználótól, amíg a távoli gép meg nem felelt a megadott hálózati alapkövetelményeknek. A NAQC felügyelete alatt, amikor egy számítógép megpróbál kapcsolódni egy távoli hálózati végponthoz, akkor megkapja az IP-címet, de az Internet Authentication Service hitelesítő szolgáltatás (IAS) karantén módba lép, és ez csak akkor kerül feloldásra, ha bizonyos ellenőrzések lezajlottak. Hátránya ennek, hogy az ellenőrző parancsfájlt nekünk kell elkészíteni, amely meglehetősen bonyolult és időigényes, valamint további hátrány, hogy ez a szolgáltatás nem biztosít védelmet a szervezeten belül működő többi számítógép ellen. Egy másik megoldás a NAC (Network Admission Control), amely már közelebb áll a NAP-hoz, sok közös tulajdonságot tartalmaz, valamint a NAC és a NAP képes közösen együttműködni egy hálózatban.

A NAP működése

A NAP a Windows Server 2008-ban három részből áll:

Rendszerállapot-érvényesítés

A csatlakozni kívánó számítógép átvizsgálásra kerül az előre meghatározott egészségügyi követelmények alapján. Ilyen követelmény lehet például a biztonsági frissítések, javítócsomagok megléte.

Állapotmegfelelés

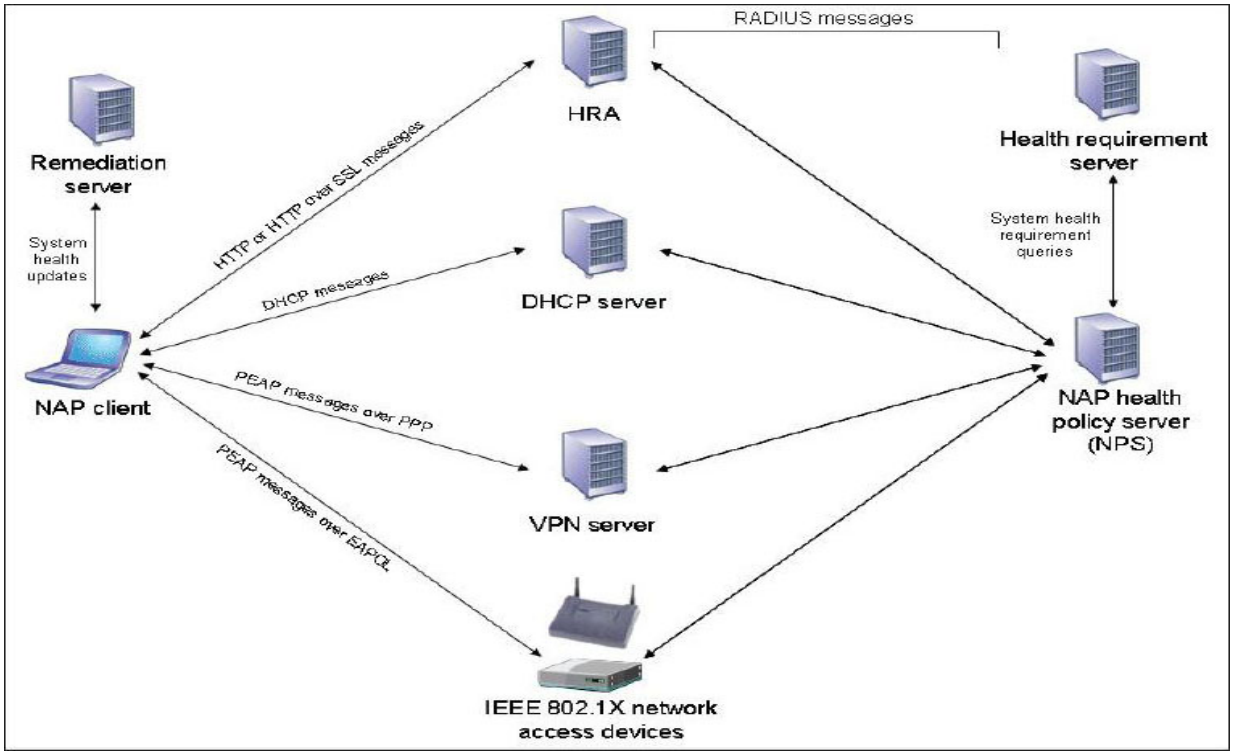
Állapotházirend segítségével lehetőség van arra, hogy a felügyeleti szoftveren keresztül sor kerüljön azoknak a felügyelt gépeknek az automatikus frissítésére vagy javítására, amelyek nem felelnek meg az állapotházirendnek. Lehetőség van továbbá olyan eljárások használatára is, amelyekkel biztosítható, hogy a hálózaton működő számítógépek betartsák az állapotházirendeket és egészségesek maradjanak

Korlátozott hozzáférés

A NAP működtethető figyelő vagy aktív módban is. A figyelő üzemmód esetén csak naplózza a hálózathoz kapcsolódó számítógépek állapotát, míg aktív módban futtatva azokat a számítógépeket, amelyek nem felelnek meg a házirendnek, azokat a hálózat egy korlátozott részére helyezi át. Ez a korlátozott rész szinte az összes hálózati kapcsolatot letiltja és a forgalmat olyan hálózati kiszolgálókra korlátozza, amelyek minden olyan eszközt tartalmaznak, amely segítségével a számítógép a hálózati feltételeknek megfelelő állapotra hozható.

A NAP rendszer ellenőrzése

A NAP rendszer ellenőrzése a következőképpen történik:



A NAP működése

1.) A számítógép hozzáférési kérelemmel fordul a DHCP- vagy a VPN-kiszolgálóhoz, vagy egy hálózati kapcsolóhoz, esetleg útválasztóhoz és a kérelemhez csatolja az állapotának leírását. Ezek mindegyike közös abban, hogy RADIUS-szal kommunikálnak az NPS felé.

2.) A hozzáférési kérelmet fogadó eszköz, a számítógép által adott állapotleírást továbbítja a Microsoft Policy Serverhez, amely egy RADIUS protokollt támogató számítógép. Ez a protokoll a Windows Server 2003-ban jelen lévő internethitelesítési szolgáltatást felváltó protokoll.

3.) A hálózati házirend-kiszolgáló ellenőrzi a kapott állapotleírást a megadott feltételek alapján, és ez alapján dönt a kapcsolódó ügyfélgép sorsáról. Ha az ügyfélgép nem felel meg a házirendbe leírtaknak, akkor egy virtuális hálózatra kerül, ahol teljesen elszigetelődik az egészséges gépektől. Ezek az elszigetelt gépek csak egy különlegesen megerősített kiszolgálót érhetnek el (Remediation Server), amelyek rendelkeznek a javításhoz szükséges eszközökkel. A csatlakozni kívánó ügyfélgép, mindaddig ebben a virtuális hálózatban marad, ameddig a házirendnek meg nem felel. A házirendnek megfelelő gépek teljes hálózati hozzáférést kapnak.

4.) Az ügyfél oldalán a rendszerállapot ügynökök (System Health Agents, SHA) és a rendszerállapot-érvényesítők (System Health Validator, SHV) biztosítják, hogy az ellenőrzések megtörténjenek minden ügyfélen. A NAP ügyféloldali ügynökei az SHA által készített állapotinformációkat továbbküldik a kényszerítő ügyfeleknek, amelyek végrehajtják a kényszerítést.

Kapcsolódási eljárások

A NAP többféle módon korlátozhatja az ügyfélgépek hálózati hozzáférését. A Windows Server 2008-ban öt különböző módszer áll rendelkezésre, amelyekkel biztosítani lehet a megfelelőséget:

DHCP

Ez a módszer a DHCP szolgáltatást használja fel a kliensek hozzáférésének szabályozására. A kliens megpróbál IP-címet kérni egy olyan Windows Server 2008 rendszerű DHCP-kiszolgálótól, amelyre telepítették a hálózati házirend-kiszolgálói (NPS)

szerepkört. Ez a kiszolgáló megvizsgálja a kliens állapotát, és ha az megfelelő akkor egy érvényes IP címet oszt ki. Ha viszont a klienst betegnek ítéli meg, akkor csak egy korlátozott hálózathoz kap hozzáférést, amelyben csak egy IP-cím, egy alhálózati maszk és néhány gyógyító kiszolgáló elérési útja szerepel, átjáró elérése nem. Ezek a gyógyító kiszolgálók biztosítják azokat az eszközöket, amelyek ahhoz szükségesek, hogy a kliens a megfelelő állapotba kerülhessen. Amint az ügyfélgép egészséges állapotba kerül egy teljes értékű IP-címet kap és csatlakozhat a hálózathoz.

VPN

A VPN alapú módszer hasonlít a NAQC-re. Ezen módszer használatakor a VPN kiszolgálónak Windows Server 2008 operációs rendszeren kell futnia, és az RRAS (Routing and Remote Access) szolgáltatásnak telepítve kell lennie. A folyamat azzal kezdődik, hogy a VPN kliens megpróbál csatlakozni a VPN-kiszolgálóhoz, amelyen fut a hálózati házirend kiszolgáló. A VPN szerver ellenőrzi a kliens állapotát, és ha az egészséges akkor korlátlan hozzáférést kap a hálózathoz. Ellenkező esetben a szerver csomagszűrőket alkalmaz, amelyek karanténba zárják a klienst és csak korlátozott hálózathoz engedik hozzáférni, ahhoz ahol általában a gyógyító szerver található. Ha a kliens már rendbejött a VPN-kiszolgáló a szűrőket eltávolítja és így a kliens szabadon hozzáférhet a hálózathoz.

802.1x

A 802.1x szabvány mind vezetékes, mind vezeték nélküli hálózaton lehetővé teszi, hogy csak az azonosított eszközök léphessenek fel a hálózatra. Ez állapottanusítvány vagy jelszó segítségével is történhet, az azonosítást pedig a központi címtárra lehet bízni. A NAP 802.1x alapú módszere, rögzített ügyfelek esetén jobb védelmet nyújt a DHCP alapú módszerrel szemben. A 802.1x az IEEE (Institute of Electrical and Electronics Engineers) szabványa, amely hálózati kapuk szintjén szabja meg a berendezések viselkedését. A fizikai infrastruktúrát használjuk a szabályozásra, tehát például ha egy switchez csatlakozó eszköz számára engedélyezzük a forgalmat, akkor a port nyitott, egyébként pedig tiltott. Ezen módszer segítségével védelmet lehet biztosítani, vagy korlátozást lehet kiszabni bármely csatlakozó eszközre.

A hátránya ennek a megoldásnak, hogy a csatlakozási pontok szintjén történő kényszerítésnek megfelelő hardver drága. A csomagkapcsolónak tudni kell kommunikálni a

Windows hálózati házirend-kiszolgálóval egy titkosított EAP kapcsolaton keresztül, így el tudja dönteni, hogy az adott kapun engedje-e az adatátvitelt, vagy sem.

IPsec

Ezen módszer segítségével csak azokat a gépeket engedjük csatlakozni a hálózathoz, amelyek megfelelő állapottanusítvánnyal rendelkeznek. A hálózat minden gépére IPsec-házirendet kell telepíteni, amely segítségével a NAP az egészséges gépeken állapottanusítványt tud létrehozni. A tanusítvánnyal rendelkező gépek ezt követően szabadon kommunikálhatnak egymással, ezzel szemben a beteg gépek, amelyek nem kapnak tanusítványt, ugyan érvényes IP címmel rendelkeznek, de nem tudnak kommunikálni az egészséges számítógépekkel. Az IPsec-házirend miatt az egészséges gépek egyszerűen figyelmen kívül hagyják a felőlük érkező információt.

TS Gateway

Ezt a módszert lehet alkalmazni a terminálszolgáltatásokat igénybe vevő távoli kliensekre. Ebben az esetben a kliensek elzárására van lehetőség, de ezek számára nem biztosítható az automatikus gyógyítás. A Terminal Services Gateway segítségével a hitelesített számítógép biztonságosan bejelentkezhet az interneten keresztül, biztonságos HTTPS-be ágyazott RDP-vel, anélkül hogy előtte VPN-kapcsolatot kellene létrehozni.

A hálózatvédelem megvalósítása

Az alábbiakban bemutatom egy vállalat számára a NAP bevezetésének szakaszait. Ezekre a fázisokra azért van szükség, mert a rendszerüzemeltető a hálózatban lévő kliensek állapotával nem biztos, hogy tisztában van, valamint a felhasználók is láthatják, hogy mi történik.

Első szakasz: (naplózás)

Ebben a fázisban csak jelentések készülnek az eseménynaplóba, tehát a NAP bármit is tesz, az eredmény csak a központi naplóba kerül be, és semmilyen valódi gyógyítás vagy karanténba helyezés nem történik meg. Ebben a szakaszban az a cél, hogy a hálózat gépeinek egészségügyi állapotáról egy átfogó képet kapjunk.

Második szakasz: (naplózás és gyógyítás)

Folyatódik a megfigyelés, azonban a naplózás mellett már engedélyezni lehet a gyógyítást. Megkezdődik a kliensek állapotának javítása, de a nem megfelelő gépeket a hálózattól még nem szigeteljük el.

Harmadik szakasz: (késleltetett kényszerítés)

Miután eltelt némi idő a NAP segítségével beállíthatjuk, hogy a beteg gépeket csak korlátozott ideig engedje fel a hálózatra. Ennek az időtartamnak a hossza tetszőleges lehet, de nem javasolt egy napnál rövidebbet, és egy hétnél hosszabbat megadni. Ezalatt az idő alatt a felhasználók pótolhatják a hiányosságaikat.

Negyedik szakasz: (azonnali kényszerítés)

Ebben a szakaszban, ha már mindenkinek sikerült megjavítani a gépet, és mindenkinek megvan a lehetőség az automatikus gyógyítás használatára, akkor szüntessük meg az előző szakaszban megadott türelmi időszakot és engedélyezzük a NAP számára, hogy a gyógyíthatatlan gépeket kizárja a hálózatból. A kizárás azonnal megtörténik, és nincs lehetőség a teljes hálózat elérésére a nem megfelelő állapotú kliensekről. A NAP a kisebb problémákat képes automatikusan megoldani, így csak azokat a gépeket fogja kizárni a hálózatból, amelyeknek súlyosabb problémájuk van.

A NAP nem csak egy szolgáltatás, hanem valójában egy platformról van szó, amely szerver és kliens oldali komponensekből áll, tehát egy kliens-szerver architektúrában működő szolgáltatás. Kliens oldali komponenseket saját magunk is készíthetünk egy API segítségével különböző platformokra. A NAP szolgáltatásit csak azok a számítógépek vehetik igénybe, amelyek futtatják a kliens oldali összetevőket. Ezt az összetevőt jelenleg a Windows Vista SP1-ben és a Windows Server 2008-ban találjuk meg, de korábbi verziójú operációs rendszerekhez is elérhető. A NAP a kliens állapotának folyamatos ellenőrzése mellett, segíti a klienseket az egészséges állapot elérésében, valamint a hálózati hozzáférést is korlátozza különböző eszközökkel. A NAP hatékony védelmet ad a rosszindulatú programok ellen még azelőtt, hogy azok beszivároghatnának a rendszerbe.

8.3 Active Directory

Windows Server 2008 biztonsági modell

A Windows Server 2008 biztonsági modell elemeivel vezérelhetjük a hálózati erőforrásokhoz való hozzáférést. Ezen belül a legfontosabb elemek a hitelesítés és a hozzáférés-vezérlés.

Hitelesítési protokoll

A Windows Server 2008 több különböző hitelesítési protokollt támogat. A Windows 2000 rendszertől kezdődően, az Active Directory a Kerberos 5-ös verzióját használja alapértelmezett hitelesített protokollként. Ezen kívül az Active Directory még ügyféltanusítványokat is használ a hitelesítéshez. Az NTLM-hitelesítést csak a korábbi verziókkal való kompatibilitás megőrzésére használja. A hitelesítési protokoll a Windows Server 2008-ban kétfázisú eljárásként valósul meg, amely egy bejelentkezésből és egy hálózati hitelesítésből áll. Amikor a felhasználó egy tartományi fiók használatával jelentkezik be egy számítógépre, akkor a bejelentkezési eljárás hitelesíti őt ezáltal hozzáférést biztosít az Active Directory-címtárszolgáltatáshoz. Ezt követően, ha a felhasználó hálózati erőforrásokat ér el mindig a hálózati-hitelesítési eljárás kerül alkalmazásra, amely meghatározza, hogy a felhasználónak van-e joga hozzá.

A Windows Server 2008 hitelesítési modell támogatja az egyszeri bejelentkezést, amely úgy történik, hogy:

- A felhasználó bejelentkezik nevének és jelszavának segítségével
- A bejelentkezési eljárás hitelesíti a felhasználót. Helyi számítógépre történő bejelentkezés esetén az adatok helyben kerülnek hitelesítésre, míg tartományi fiók esetén a bejelentkezési adatok az Active Directory hitelesíti. Ezt követően a felhasználó hozzáférhet a hálózat erőforrásaihoz.
- Tartományi fiókok esetén a hálózati hitelesítési eljárás automatikus, míg helyi fiókok esetén, mindig meg kell adni a felhasználónak a nevét és jelszavát amikor hálózati erőforrást érnek el.

A Windows Server 2008-ban az ADFS terjeszti ki az egyszeri bejelentkezést az internet megbízható erőforrásaira. Az ADFS segítségével a szervezetek az internet megbízható erőforrásaira. Az ADFS segítségével a szervezetek kiterjeszthetik az Active Directory-infrastruktúráját az internet megbízható erőforrásaihoz való hozzáférésére. A szervezet felhasználóinak csak a szervezet hálózatba kell bejelentkezniük, a partnerek megbízható webes alkalmazásaiba pedig már automatikusan jelentkezne be. Az összevont webes egyszeri bejelentkezés egyesített hitelesítést alkalmaz, amely a felhasználói azonosítókon és a fiókinformációkon kívül biztonsági jogkivonatok is szükségesek, amelyek a felhasználói hitelesítést részletezik.

Hozzáférés-vezérlők

Az Active Directory objektumalapú. Ezekre az objektumokra a hozzáférés-vezérlőket biztonsági leírókkal együtt alkalmazzuk, amelyek a következőket hajtják végre:

- Objektumok elérésére jogosult felhasználók és csoportok felsorolása.
- Felhasználókhoz és csoportokhoz rendelt engedélyek megadása.
- Az objektumok tulajdonságainak meghatározása.
- Azon események nyomon követése, amelyeket az objektumok esetén ellenőrizni kell.

A biztonsági leíró egyedi bejegyzéseit hozzáférés-vezérlő bejegyzéseknek (ACE – Access Control Entry) nevezzük. Az Active Directory objektumai örökölhetik a hozzáférés – vezérlő bejegyzéseket a szülőobjektumtól, tehát a szülőobjektumra vonatkozó engedélyek a gyermekobjektumra is érvényesek. A hozzáférés-vezérlő bejegyzések alapértelmezés szerint örökölhetők, valamint a hozzáférés-vezérlő módosítása után az öröklés azonnal megtörténik. Továbbá minden ilyen bejegyzés tartalmaz információt arra vonatkozóan, hogy az engedély örökölt vagy az objektumhoz lett hozzárendelve.

Active Directory alapjainak rövid áttekintése

A Windows 2000 bevezetése óta az Active Directory a windowsbeli tartományok központi eleme, mivel majdnem minden felügyeleti feladat érinti valamilyen módon az Active Directory címtárat. Alapját szabványos internetprotokollok képezik, felépítése pedig segít a hálózati struktúra maghatározásában. Az Active Directory szolgáltatást használó tartományokat Active Directory tartományoknak nevezik. Az Active Directory tartományok

kiterjeszthető és méretezhető címtárszolgáltatások, amelyek révén a hálózati erőforrások hatékonyan kezelhetők.

Az Active Directory tartományi szolgáltatások (AD DS) arra az elvre épülnek, hogy egy dinamikus, könnyen kezelhető szerkezetet hozzanak létre, amelyben a címtár- és felügyeleti információk központosítva találhatók, és ezen keresztül az információk az egész hálózaton elérhetők. Az AD DS összetevőit két csoportra oszthatjuk: fizikai és logikai összetevők. A logikai összetevők csoportjába a következők tartoznak:

Tartomány: A tartomány számítógépek egy csoportja, amely közös címtáradatbázissal rendelkezik. Egy erdőben több tartomány is létezhet, saját objektumokkal és szervezeti egységekkel. A tartományok elnevezése DNS-protokoll alapján történik.

Fák: A fa tartományok gyűjteménye, amelyek közös összefüggő névtérrel rendelkeznek.

Erdő: Egy vagy több tartományfa, amelyek közös címtárinformációval rendelkeznek. Az erdő a legnagyobb logikai tároló az AD DS-ben, amely a látókörébe tartozó összes tartományt átfogja. Ezeket a tartományokat egy biztonságos kommunikációs útvonal kapcsolja össze, így egy tartomány megbízhat az erdőben található összes többi tartományban. Az erdő a szervezet biztonsági határaként szolgál, és meghatározza a rendszergazdák hatáskörét. Alapértelmezett állapotban egy erdő egyetlen tartományt tartalmaz, ezt az erdő gyökértartományának nevezzük. Az erdőben további tartományokat is létre lehet hozni annak érdekében, hogy szétválassza az Active Directory tartományi szolgáltatások adatait, amelyek következtében a szervezetek csak a szükséges adatokat replikálják.

Szervezeti egység: A szervezeti egység (organizational unit) egy olyan tároló, amelyben objektumok találhatók. A szervezeti egységeket hierarchikus szerkezetbe rendezhetjük, amely megkönnyíti a felügyeleti feladatok elvégzését.

A fizikai struktúrák teszik lehetővé a hálózati kommunikációt. A fizikai összetevők, amelyek segítségével leképezhetjük a fizikai hálózat struktúráját, a következők:

Tartományvezérlő: A tartományvezérlő tárolja egy adott tartomány biztonsági adatait és címtárobjektum-adatbázisát, és ez felel a hatáskörükbe tartozó objektumok hitelesítéséért. Egy tartomány számára több tartományvezérlőt is létrehozhatunk, és ezen tartományon belül lévő tartományvezérlők erő szempontjából egyenlők.

Telephely: A telephely, az egy önálló földrajzi helyen található, vagy állandó hálózati kapcsolaton összekötött számítógépek csoportját jelenti. A telephelyeket arra használják, hogy meghatározzák hogyan kell frissíteni a tartományvezérlőket.

Alhálózatok: Egy jellegzetes IP címtartománnyal és hálózati maszkkal rendelkező hálózati csoport.

A rendszergazdák az Active Directory tartományi szolgáltatásokat hálózati elemek hierarchikus beágyazott struktúrába rendezésére használhatják. A hierarchikus beágyazott struktúra erdőből, az erdő tartományaiból, valamint a tartományokban található szervezeti egységekből áll.

Active Directory tartományi szolgáltatások új szolgáltatásai

Az Active Directory tartományi szolgáltatások számos új szolgáltatást tartalmaznak, amely a Windows Server Active Directory szolgáltatásának korábbi verzióiban nem volt elérhető. Az AD DS a következő új szolgáltatásokat tartalmazza:

Írásvédett tartományvezérlő

Az írásvédett tartományvezérlő a tartományvezérlők egy új fajtája, amely tartalmazza a címtár egy példányát, azaz képes az összes tartományvezérlő feladat ellátására, de a címtár tartalma nem változtatható meg helyben.

Írásvédett tartományvezérlő előkészített telepítése

Ezzel a szolgáltatással az írásvédett tartományvezérlő telepítése két lépésben végezhető el. Először a rendszergazda létrehoz egy fiókot az írásvédett tartományvezérlő számára, majd a delegált felhasználó csatlakoztat egy kiszolgálót az írásvédett tartományvezérlő fiókhoz.

Írásvédett tartományvezérlőről kiszűrt attribútumkészlet

Olyan attribútumok csoportja, amelyek nem replikálódnak az írásvédett tartományvezérlőre.

Rendszergazdai szerepkör szétválasztása

Ez a szolgáltatás lehetővé teszi a rendszergazdák számára, hogy delegálják az írásvédett tartományvezérlő telepítését és felügyeletét a nem rendszergazdai jogosultsággal rendelkező felhasználóknak.

Továbbfejlesztett telepítési varázsló

Az AD DS telepítési varázslója (`dcpromo.exe`) támogatja a felügyelet nélküli telepítést, az írásvédett tartományvezérlők telepítését és más speciális beállításokat.

Biztonságos telepítési adathordozó létrehozása

Az Ntdsutil.exe alkalmazás a Windows Server 2008 rendszerben történő futtatásával biztonságos telepítési adathordozókat hozhat létre az Active Directory tartományi szolgáltatások, és az Active Directory Lightweight Directory szolgáltatások későbbi telepítéseihez.

Újraindítható Active Directory tartományi szolgáltatások

Ezen szolgáltatás segítségével újraindítható az Active Directory tartományi szolgáltatások anélkül, hogy a tartományvezérlőt újra kellene indítani. Így az offline műveletek gyorsabban elvégezhetőek.

Active Directory tartományi szolgáltatások változásainak naplózása

A naplózó szolgáltatás esetén az Active Directory tartományi szolgáltatások objektumai és attribútumainak minden változásakor naplózás történik, ahol a régi és az új értékek is rögzítésre kerülnek.

Minden részletre kiterjedő jelszóházirend

A szolgáltatás segítségével megadható a tartomány felhasználóira és globális biztonsági csoportjaira vonatkozó jelszó- és fiókzárolási házirend.

Adatbányászat eszköz

Ezzel a szolgáltatással megtekinthető az AD DS és AD LDS azon adatai, amelyek a pillanatképekben vagy a biztonsági mentésekben tárolva vannak. Használatával különböző pillanatokban készített pillanatfelvételek adatai összehasonlíthatóak, így a kiszolgáló újraindítása nélkül is el lehet dönteni, hogy mely adatokat kell visszaállítani.

Írásvédett tartományvezérlő

A Windows NT 4.0 idején csak egyetlen elsődleges tartományvezérlő a PDC (Primary Domain Control) volt, amelynek tetszőleges számú alárendelt tartományvezérlője BDC (Backup Domain Control) lehetett. Az adatok áramlása könnyen követhető volt, mert a módosítások a PDC-n történtek és innen egyirányba terjedtek a BDC felé. Az AD DS megjelenésével, azonban minden tartományvezérlő egyenrangúvá vált, tehát megszűnt az elsődleges és a tartalék tartományvezérlő. Ez az új felépítés növeli a hibatűrést és az operációs rendszer tömeges telepítésének lehetőségét, viszont gondot okozhat az, ha a hálózat valamelyik tartományvezérlője sérült vagy helytelen adatokat tesz közzé a többi tartományvezérlő számára.

A Windows Server 2008 AD DS megvalósításánál a tartományvezérlők egyenrangúsága ugyanúgy érvényes, viszont ehhez kapcsolódóan bevezették az írásvédett tartományvezérlő fogalmát. Az írásvédett tartományvezérlő (Read-Only Domain Controller, RODC) egy olyan kiegészítő tartományvezérlő, amely csak olvasható másolatot tárol a tartomány Active Directory-adattáráról. Képes minden tartományvezérlői feladat ellátására, de a címtár tartalma nem változtatható meg helyben. Mivel nincs globális AD-módosítási lehetőség, ezért olyan környezetbe is használható, ahol fizikailag nem garantálható a biztonság, például telephelyek esetén, vagy olyan esetekben, amikor a tartományi jelszavak helyi tárolása nagy biztonsági kockázatot jelent. Ez igen hasznos, ennek segítségével nem kell teljes jogú tartományvezérlőket üzemeltetni a távoli helyeken.

Írásvédett tartományvezérlő funkciói

Írásvédett AD DS-adatbázis

A jelszavak kivételével az RODC-kiszolgálók ugyanazokat az objektumokat és attribútumokat tárolják, mint az írható tartományvezérlő társaik. Az objektumok és attribútumok egyirányú replikációval jönnek létre, egy írható tartományvezérlő segítségével. Az RODC-kiszolgálók saját számítógépfiókjuk és a Kerberos Target (krbtgt) fiók kivételével nem tárolnak jelszavakat vagy hitelesítési adatokat. Ezért a felhasználókat vagy számítógépeket hitelesítő adatokat a Windows Server 2008 operációs rendszert futtató, írható tartományvezérlőről tölti le. Ha az írható tartományvezérlő jelszó-replikációs házirendje ezt

engedélyezi, akkor az RODC kiolvassa, majd szükség szerint tárolja a hitelesítési adatokat, míg azok meg nem változnak. Az RODC-kiszolgáló a hitelesítési adatok csak egy részét tárolja, viszont arra van lehetőség, hogy bármely más fiók hitelesítési adatait gyorsítótárazzuk. Az írásvédett tartományvezérlő alatt működő címtár-adatbázispéldánynak ugyanúgy kell kinéznie, mint egy hagyományos tartományvezérlőnél, viszont változásokat nem tárolhat, és nem is replikálhat. Így az összes változtatási kérelemnek el kell jutnia egy írható tartományvezérlőig, hogy aztán az repikációval visszakerülhessen az RODC-címtár példányába. A helyi alkalmazások továbbra is kaphatnak egyszerű hozzáférést a címtár helyi példányához, de csak olvasási joggal. Ha ennél többre van szüksége, akkor LDAP-n keresztül továbbkerül a kérés a központi telephely felé, ahol egy írható DC van.

Hitelesítő adatok gyorsítótárazása

A hitelesítési adatok gyorsítótárazása a felhasználó vagy számítógép hitelesítő adatainak eltárolását jelenti. Alapértelmezés szerint az RODC két kivételtől eltekintve, amely az RODC gépfiókja és a krbtgt fiók, nem tartalmaz semmilyen felhasználói vagy számítógépfiók hitelesítő adatait. Minden más hitelesítő adatot érintő gyorsítótárazást külön engedélyezni kell az írásvédett tartományvezérlőn. A hitelesítési adatok tárolása azért előnyös, mert így nem kell kimenni a hálózatból, egy esetlegesen lassú kapcsolaton keresztül minden felhasználói belépés vagy hitelesítés esetén. Ez úgy lehetséges, hogy az RODC képes KDC-ként (Key Distribution Center) viselkedni, azaz képes érvényes Kerberos kulcsokat kiadni, amelyet a fiókok használhatnak a hitelesítési folyamatban a központi DC-k nélkül is.

Első alkalommal a hitelesítés csak a központi DC-n keresztül fog történni. A kliens szeretné használni az RODC-t, de először csak továbbítani tudja ezt a kérést, majd ha a közvetítés által sikerült a hitelesítés, akkor a RODC elkéri az adott fiók hitelesítési adatait. Az írható DC a PRP (Password Replication Policy) segítségével dönti el, hogy teljesítheti-e az RODC kérést. A PRP egy táblázat, amelybe manuálisan kell felvenni azokat a fiókokat, amelyeknek a hitelesítési adatait merjük gyorsítótárazni RODC-n. Ez a táblázat alapesetben üres. Ha viszont a kérdéses fiók számára engedélyezve van a gyorsítótárazás, tehát szerepel a táblázatban, akkor a központi DC átnyújtja a megfelelő adatokat az RODC-nek, amely elraktározza ezeket. A PRP tábla feltöltése a rendszergazda feladata ő dönti el, hogy mely fiókok vagy csoportok hitelesítési adatai kerülnek tárolásra az RODC-n belül. Ha a telephelyen használt minden fiók engedélyezve van, akkor a bejelentkezés gyors lesz ugyan,

de ha a gépet eltulajdonítják, akkor a jelszavakhoz hozzáférhetnek ugyanúgy, mint egy hagyományos tartományvezérlő esetén.

Írásvédett tartományvezérlőkre nem replikált attribútumkészlet

Egyes alkalmazások, amelyek az Active Directory tartományi szolgáltatásokat adattárolásra használják, rendelkezhetnek olyan hitelesítési célú adatokkal, amelyeket nem szeretne tárolni az írásvédett tartományvezérlőn. Az ilyen alkalmazások esetében definiálni lehet olyan attribútumkészletet a tartományobjektumok sémáján, amelyek nem replikálódnak az írásvédett tartományvezérlőre. Ezt az attribútumkészletet az írásvédett tartományvezérlőről szűrt attribútumkészletnek nevezzük. Ebben az attribútumkészletben megadott attribútumok nem replikálódnak az erdő egyetlen írásvédett tartományvezérlőjére sem. Ha az írásvédett tartományvezérlő a nem replikált attribútumkészletben meghatározott attribútumokat olyan tartományvezérlőről próbálja meg repikálni, amelyen Windows Server 2008 rendszer működik, akkor a rendszer megtagadja a kérelmet. Míg ha ugyanezt Windows Server 2003 rendszert futtató tartományvezérlőről próbálja meg replikálni, akkor a replikációs kérés sikeresen lefut. Ennek elkerülése érdekében az erdő működési szintje csak Windows Server 2008 lehet, ha írásvédett tartományvezérlőkre nem replikált attribútumkészletet konfigurálunk.

Az írásvédett tartományvezérlőről kiszűrt attribútumkészletet, azon a tartományvezérlőn kell konfigurálni, amely a séma műveleti főkiszolgáló szerepkört tölti be. A nem replikált attribútumkészlethez a rendszer szempontjából kritikus fontosságú attribútumokat nem lehet hozzáadni. Egy attribútum akkor rendszerkritikus, ha szükséges az Active Directory tartományi szolgáltatások, a helyi biztonsági rendszer, vagy a biztonsági fiókkezelő helyes működéséhez. Ha mégis rendszerkritikus attribútumot adunk hozzá az írásvédett tartományvezérlőről kiszűrt attribútumkészlethez, és a főkiszolgáló a Windows Server 2008 rendszert futtatja, akkor az „`unwillingToPerform`” LDAP-hibával fog válaszolni.

Rendszergazdai jogok elkülönítése

Az írásvédett tartományvezérlő helyi, magas szintű jogosultságot biztosíthat bármely tartományi felhasználónak. Ez hozzávetőleg a lokális rendszergazda jogkörével egyenlő anélkül, hogy bármilyen felhasználói jogot biztosítana a tartományban vagy más tartományvezérlőkön. Ez a jogkör lehetővé teszi, hogy a telephely felhasználója

bejelentkezzen az írásvédett tartományvezérlőre, és karbantartási munkát végezzen a kiszolgálón. A felhasználó nem tud bejelentkezni másik tartományvezérlőre vagy rendszergazdai feladatot végezni a tartományban. Ezáltal a felhasználó kezelheti a telephely írásvédett tartományvezérlőjét anélkül, hogy a tartomány többi részének biztonsága sérülne. Egy tartományi felhasználó számára magas szintű jogosultság biztosítása kétféle módon történhet:

- parancssorból a Dsmgmt eszközzel
- az írásvédett tartományvezérlő telepítése során a varázsló egyik lépéseként.

Egyirányú replikáció

Az írásvédett tartományvezérlőre direkt módon semmilyen változás nem íródik, és innen semmilyen változás nem származtatható. Ezáltal az írható tartományvezérlőknek nem kell a változásokat bekérniük az írásvédett tartományvezérlőkről, így a rosszindulatú módosítások nem replikálódnak az írásvédett tartományvezérlőről az erdő többi részére. Az írásvédett tartományvezérlő egyirányú replikációja érvényes az Active Directory tartományi szolgáltatások és az elosztott fájlrendszer (DFS) replikációja esetén is.

Írásvédett tartománynévrendszer

Ha írásvédett tartományvezérlőre telepítünk DNS-kiszolgáló szolgáltatást, akkor az írásvédett tartományvezérlő írásvédett DNS-kiszolgálóként működik. Az RODC DNS-szerver teljes értékű, képes a DNS által használt alkalmazáspartíció replikálására, köztük a ForestDNSZones és a DomainDNSZones partíciók replikálására, vagy a kliensek névfeloldási kéréseinek kiszolgálására. Ha a DNS kiszolgáló telepítve van az írásvédett tartománykiszolgálón, akkor az ügyfelek ugyanúgy lekérdezéseket intézhetnek felé névfeloldás céljából, mint ahogy bármely más DNS-kiszolgáló esetén is tehették.

Az írásvédett DNS-kiszolgáló azonban nem támogatja a kliens-oldali frissítést. Egy fiókirodán belül több RODC-t is lehet üzemeltetni, és ezek mindegyikére lehet telepíteni DNS példányt. Mivel az RODC-k csak olvashatóak, ezért az ügyfelek dinamikus frissítési kérelmeit a központi iroda egyik írható tartományvezérlőjéhez kell irányítani. Az RODC-ben lévő DNS-példányok minden változtatási igényt a központi AD DS rendszerből kapnak meg. Amikor az ügyfélprogram megpróbálja frissíteni a DNS-rekordokat egy írásvédett tartományvezérlőn, akkor a kiszolgáló egy hivatkozást küld, amely segítségével az ügyfél ezt követően

megkísérelheti végrehajtani a frissítést a DNS kiszolgálón. Az írásvédett DNS-kiszolgáló ezután egy háttérben zajló replikációval megpróbálja kiolvasni a rekordot a frissítést végrehajtó DNS-kiszolgálóról. Ez a replikációs kérés csak a módosított DNS-rekordra vonatkozik, és nem replikálódik a módosított zónák és tartományadatok teljes listája.

Az írásvédett tartományvezérlő tulajdonságai

- Segítségével csökkenthető annak az esélye, hogy fertőzött adatok kerüljenek az AD DS adatbázisba.
- Az RODC alapértelmezés szerint nem gyorsítótárazza a tartományi rendszergazda azonosítóit.
- Az RODC csak azoknak a felhasználóknak és számítógépeknek az azonosítóit gyorsítótárazza, akik az RODC-re jelentkeztek be, és akiknek az azonosítóit a jelszótöbbszörözési házirend megengedi gyorsítótárazni.
- Az RODC által kiadott Kerberos hitelesítési jegyek csak az RODC hatáskörébe érvényesek, így az RODC nem tud hamis jegyeket kiadva hozzáférést biztosítani a teljes hálózathoz.
- Az RODC Server Core-szerepkör segítségével alig van szükség helyi felügyeletre, valamint a grafikus felület hiánya kevesebb támadási felületet eredményez.
- Gyors bejelentkezés és hatékonyabb hozzáférés a hálózati erőforrásokhoz.

Írásvédett tartományvezérlő telepítése

Az írásvédett tartományvezérlők telepítésének leggyakoribb oka a nem megfelelő fizikai biztonság. Ezen tartományvezérlő segítségével olyan helyekre is lehet telepíteni tartományvezérlőt, ahol nincsenek meg az írható tartományvezérlőkhöz szükséges fizikai biztonsági körülmények.

Az írásvédett tartományvezérlő úgy lett kialakítva, hogy elsődlegesen távoli vagy telephelyi környezetben legyen telepítve. Telepítéskor először létre kell hozni egy fiókot az írásvédett tartományvezérlő részére. A fiók létrehozásakor meg lehet adni, hogy ki telepíti és felügyeli az írásvédett tartományvezérlőt. Az írásvédett tartományvezérlő rendszergazdája befejezheti a telepítést úgy, hogy a kiszolgálót csatolja az írásvédett tartományvezérlő

fiókjához. Így nincs szükség a tartományi rendszergazda hitelesítő adatainak használatára az írásvédett tartományvezérlő felépítéséhez a telephelyen.

Az írásvédett tartományvezérlő telepítésének követelményei:

- Az első Windows Server 2008 tartományvezérlő, amely tartományerdőbe vagy tartományba lett telepítve, nem lehet írásvédett tartományvezérlő. Viszont a rákövetkező tartományvezérlők már írásvédettek lehetnek.
- A tartomány és az erdő működési szintjének Windows Server 2003 beállításúnak vagy magasabbnak kell lennie.
- Az írásvédett tartományvezérlőnek a hitelesítési kéréseket egy, a Windows Server 2008 rendszert futtató, írható tartományvezérlő felé kell továbbítani. Ezen a tartományvezérlőn be kell állítani a jelszó-replikációs házirendet azért, hogy a hitelesítő adatok replikálhatók-e a telephelyre az írásvédett tartományvezérlőtől kapott kérés alapján.
- Az írásvédett tartományvezérlő telepítéséhez a tartomány egy írható tartományvezérlőjén a Windows Server 2008 rendszernek kell futnia.
- Az erdőben egyszer futtatni kell az `adprep /rodcprep` parancsot az erdő összes DNS alkalmazásspecifikus címtárpartícióján található jogosultságának frissítéséhez. Így az olyan írásvédett tartományvezérlők, amelyek egyben DNS-kiszolgálók is, a jogosultságokat sikeresen képesek replikálni.

9 VIRTUALIZÁCIÓ

A virtualizáció az elmúlt évek igen jelentős technológiája. Sokan sokféleképpen határozzák meg, és a virtualizáció a növekvő vállalatok, felhasználók számára sok előnyt kínál. Ma az IT-ben egy állandó van, ez a változás. Ez a változás jól kiszolgálható a virtualizáció segítségével. Egyszerűbb, jobban skálázható, költséghatékonyabb IT infrastruktúra érhető el, amely rugalmasabban követheti a változásokat.

9.1 Bevezetés a virtualizációba

A hagyományos informatikai környezet minden rétege, tehát a hardver, az operációs rendszer, az alkalmazások és a tárhely egy megfelelő együttműködésre vannak beállítva. Ezek az összetevők csak meghatározott számítógépekbe helyezhetők el, és az ezek által létrejött rendszer nem képes rugalmasan alkalmazkodni a változásokhoz. Ezzel szemben a virtualizáció megszünteti a rendszer elemeinek egymástól való függését. A virtualizált infrastruktúrában a rendszer elemei logikailag elkülönülnek és függetlenek egymástól. A rendszer különböző rétegeinek szétválasztásával rugalmasabbá és egyszerűbbé válik a változtatáskezelés, tehát már nem kell minden egyes elemet beállítani ahhoz, hogy az elemek együttműködjenek. Az összetevők lényegében azonnal elérhetők, amely megkönnyíti az infrastruktúra elemeinek dinamikus hozzáadását, frissítését és támogatását.

A virtualizáció egyre fontosabb szerepet játszik az informatika valamennyi területén, a munkaállomásoktól egészen az adatközpontokig. Egyre több szervezet alkalmaz virtualizációs megoldásokat a munkaterhelések kezelésére, amely segítségével kihasználhatják a kiszolgálók összevonásával elérhető költségmegtakarítási lehetőségeket. A virtualizáció kiterjesztésével számos új funkció válhat elérhetővé egy szervezet számára, mint például a tesztelés és fejlesztés, vészhelyreállítás, üzletmenet folytonosság, valamint távoli irodák felügyeletének a támogatása. A virtualizált környezet segítségével egy informatikai szervezet képes hatékony és nagy teljesítményű feladatokat megvalósítani az igények gyors kielégítése érdekében. A virtualizáció kulcsfontosságú összetevője a dinamikus informatikának. A virtualizációs technológia elkülöníti egymástól a számítástechnikai erőforrásokat. A Microsoft szerint a

virtualizált környezet, a logikai műveletek és a fizikai hardver elválasztásával nagyobb működési rugalmasságot biztosít, és egyszerűbbé teszi a rendszerek megváltoztatását.

A következő összetevők alakulnak ki az elkülönítés során:

- Virtuális alkalmazás : alkalmazások elérése bármely számítógépen
- Virtuális megjelenítés : folyamattól elkülönült megjelenítési réteg
- Virtuális gép : az operációs rendszer tetszőleges munkaállomáshoz vagy kiszolgálóhoz hozzárendelhető.
- Virtuális tárolás : tárolás és biztonsági mentés a hálózaton belül
- Virtuális hálózat : elszórtan található erőforrások helybeli elérése

9.2 Biztonság és virtualizáció

A virtualizált rendszerek esetében nagyon sok olyan fenyegetéssel kell számolni, amelyek a hagyományos infrastruktúrák kapcsán is felmerülnek. A virtualizáció ezért biztonsági szempontból is odafigyelést követel. Azonban sokszor a védelmi intézkedések nem terjednek ki a virtuális világra. A vállalatok sokszor azt hiszik, hogy a virtualizációs megoldások implementálásával automatikusan biztonságba kerülnek, holott teljesen új fenyegetésekkel néznek szembe. A virtuális rendszerek ugyanis újfajta támadásokra is lehetőséget adnak, és több alkalmazást érintő károkozás következhet be, mint a hagyományos szerverek esetében. Sok szervezet úgy gondolja, hogy a virtuális gépek biztonságáról ugyanúgy kell gondoskodni, mint bármely más operációs rendszerről, ezért a meglévő konfigurációs beállításokat, szabványokat és eszközöket alkalmazzák. Ez kezdetnek megteszi, de a fizikai szerverek biztosítására használt eljárások nem nyújtanak elegendő védelmet a virtuális gépeknek.

A biztonsággal, a virtuális gépek telepítésétől fogva foglalkozni kell, de ideális esetben még előtte, már a szállítók és a platform kiválasztásánál is a biztonság legyen a fő szempont. Ennek során figyelembe kell venni, hogy a virtualizációs szoftverek egy új köztesrétegként épülnek be a szoftver verembe, ráadásul kiváltságokkal rendelkezik, ami nagy kísértés lehet a támadónak. [1]

[1] Gartner piackutató vállalat felmérése alapján

Az informatikai vezetőknek úgy kellene átalakítaniuk a biztonsági szabályzatokat, hogy azok a virtualizációval összefüggő kockázatok kezelésére is kitérjenek. Mindemellett a virtuális infrastruktúrákat biztonságos átjárókkal kell ellátni, miközben a rendszergazdai hozzáférések szabályozása is szükségessé válhat.[2]

Virtuális gépek esetén gondot okozhat még, hogy az operációs rendszer nem közvetlenül a hardverrel, hanem egy másik szoftverréteggel kommunikál, így konfigurációs hibák léphetnek fel. További problémát jelenthet még, hogy a behatolásvédelmi eszközök nem, vagy csak korlátozottan képesek figyelni a virtuális gépek és a virtualizációs szoftverréteg közötti kommunikációt. A virtualizált infrastruktúra biztonságához ellenőrizni kell, hogy a biztonsági folyamatok és eszközök megfelelőek-e. A virtuális gépeket megfelelően kell elhelyezni, például tűzfal mögött, valamint a kulcsfontosságú vagy támadásoknak kitett részeket el kell különíteni. Továbbá célszerű a kritikus fontosságú terheléseket több virtuális gép között elosztani, csökkentve ezzel a kockázatot és a leállások okozta hibákat. Az előbbiekben felsorolt problémákon kívül, azonban számos kérdésre ad megfelelő választ a virtualizáció.

A virtualizációval növelhető az adatok és az alkalmazások biztonsága. Az elemek elkülönítése biztosítja, hogy az adott virtuális gép, vagy a virtualizált alkalmazás vírusfertőzöttsége, vagy egyéb problémái ne legyenek hatással az infrastruktúra más részeire.

A virtualizáció továbbá egyszerűbbé és gyorsabbá teszi a biztonsági frissítéseket is, mivel ezeket nem különálló eszközök sokaságán kell telepíteni, hanem csak a forrásrendszerben. Ez csökkenti a munkaállomás karbantartásához szükséges munkamennyiséget és fokozza a biztonságot.

Virtualizált megjelenítési konfiguráció esetén, az adatok nem a munkaállomásokon szétszórva vannak tárolva, hanem a teljes adattárolást és feldolgozást egy központi helyen egyesíti, így a munkaállomás csak a felhasználói felület megjelenítésére szolgál.

Mivel egyre nagyobbak az informatikával szembeni elvárások és az adatközpontok kapacitása gyorsan kimerül, ezért újabb és újabb kiszolgálók beszerzésére volt eddig szükség, növelve ezzel a beruházási költségeket, ugyanakkor a kiszolgálók kihasználása nem volt megfelelő. Erre a kérdésre ad választ a virtualizáció, amely segítségével csökkenthető a

[2] Clavister

felesleges kiszolgálók száma és egyszerűsíthető az üzembe helyezésük. A virtualizáción alapuló kiszolgáló-összevonás számos előnye mellett a bonyolultságot is növelheti. A virtuális gépek túl nagy száma rosszabb helyzetet idézhet elő, mint a feleslegesen nagyszámú fizikai kiszolgálók, mert ezáltal nőhet a felügyelettel járó többletmunka és előfordulhat, hogy a rendelkezésre álló eszközök már nem elégségesek a virtuális gépek kezelésére.

9.3 Virtualizációs megoldások

Hardver virtualizáció

A hagyományos számítástechnikai környezetben, egy fizikai kiszolgálón egy operációs rendszer futhat, amely szorosan kapcsolódik a hardverhez. A hardver virtualizáció megszünteti a hardver és az operációs rendszer közötti szoros kapcsolatot és lehetővé teszi, hogy egy hardveren több operációs rendszer fusson. Ez a hardver jobb kihasználtsága mellett felgyorsítja az operációs rendszerek telepítését és felügyeletét.

Hardver virtualizáció során egy fizikai számítógépet egy virtuális gép szimbolizál, így egy operációs rendszerkörnyezet jön létre, amely logikailag különválik az őt futtató kiszolgálótól. Ez a technológia több virtuális gép azonos időben való elérésével lehetővé teszi, hogy egy fizikai gépen egyszerre több operációs rendszer fusson, egymástól elkülönített és védett módon. Kiszolgálóvirtualizáció segítségével az alacsony kihasználtságú kiszolgálók összevonhatók kevesebb számú, jobban kihasznált számítógépekre. A meghibásodott rendszerek visszaállítását is könnyebbé teszi, mert a virtuális gépek tárolása fájlként történik, így a meghibásodott rendszer visszaállításához elég lehet a fájl átmásolása egy másik számítógépre.

Alkalmazás virtualizáció

Az alkalmazás virtualizáció elválasztja az alkalmazás konfigurációs rétegét az operációs rendszertől. Ez nemcsak az alkalmazások telepítés nélküli futtatását teszi lehetővé, hanem azok központi felügyeletét is. Egy hagyományos számítástechnikai környezetben az alkalmazások közvetlenül az operációs rendszerre települnek. Az alkalmazás virtualizáció során a végfelhasználó rendelkezésére áll egy távoli központi szerverről egy alkalmazás, illetve tárolók anélkül, hogy a felhasználó lokális rendszerén teljesen installálni kellene azt.

Ekkor tehát a szerverek, az alkalmazások, a tárolók, az alkalmazási erőforrások dinamikusan el vannak választva. Mivel az alkalmazások közösen használt rendszerfájlokba írnak, ezért ezek az alkalmazások gyakran ütköznek egymással, amely a rendszer összeomlásához vezethet. Alkalmazás virtualizáció esetén minden egyes alkalmazás saját futtatókörnyezetben működik, a mögöttes operációs rendszertől elválasztva.

Az alkalmazás és operációs rendszer közötti kompatibilitási problémák a kiszolgáló virtualizáció vagy megjelenítési virtualizáció segítségével kezelhetők. Az operációs rendszer ugyanazon példányán telepített két alkalmazás közötti eltérést illetően, a megoldáshoz az alkalmazás virtualizáció szükséges. Az ugyanazon az eszközön telepített alkalmazások gyakran használnak közös konfigurációs elemeket, amelyek használata problémát okozhat. Ha például az egyik alkalmazás működéséhez egy dinamikus csatolású függvénytár (DLL) egy adott verziója szükséges, és a másik alkalmazás számára ugyanannak a DLL-nek egy másik verziója, akkor ha mindkét alkalmazást telepítjük az egyik felülírja a másik számára szükséges verziót. Mindez oda vezet, hogy valamelyik alkalmazás nem fog működni. Az alkalmazás virtualizáció ezt a problémát úgy oldja meg, hogy az összes megosztott erőforrásból alkalmazásspecifikus példányokat hoz létre. Azok a konfigurációs elemek, amelyeket az alkalmazások közösen használnak, minden egyes alkalmazással közös csomagba kerülnek, és a gép külön tárában futnak le, ezzel egy virtuális alkalmazást hozva létre. A virtuális alkalmazások a megosztott erőforrásokból mindig a saját példányukat használják. Az alkalmazás virtualizáció jelentősen megkönnyíti az alkalmazások bevezetését, valamint lehetővé teszi a virtuális alkalmazások és telepített alkalmazások közös felületen keresztül történő kezelését is.

Megjelenítési virtualizáció

A megjelenítési virtualizáció a feldolgozást különválasztja a grafikai és az I/O-műveletektől, így lehetőséget nyújt arra, hogy az alkalmazás egy adott helyen fusson, de máshonnan vezéreljék. A megjelenítési virtualizáció lehetővé teszi az alkalmazások, és az adatok központi helyen történő összevonását a fokozott biztonság érdekében, továbbá széles körű hozzáférési lehetőséget nyújt helyi és távoli felhasználók számára. Ezen folyamat során virtuális munkamenetek jönnek létre, amelyekben a futtatott alkalmazások a kezelőfelületüket távolra továbbítják. Egy munkamenetben futhat egyetlen alkalmazás, de lehetőség van arra is, hogy több alkalmazást kínáló asztal elérhető legyen a felhasználó számára. Mindkét esetben

több virtuális munkamenet is használhatja egy alkalmazásnak ugyanazt a telepítési példányát. A megjelenítési virtualizáció esetében a feldolgozás a kiszolgálón történik, míg a felhasználói I/O-műveleteket a végfelhasználói terminál kezeli. További előnye ennek a technológiának, hogy az alkalmazásokat nem kell külön frissíteni az egyes munkaállomásokon, hanem elég csak a kiszolgálón telepített példányt módosítani. Ezáltal jelentős mértékben csökkenthető az alkalmazások felügyeleti költsége.

A megjelenítési virtualizáció lehetőséget ad az alkalmazás egy központi kiszolgálón való futtatására, ahonnan bármilyen operációs rendszert futtató felhasználó számára elérhető, biztosítva ezáltal a rendszerek közötti kompatibilitási problémákat.

Munkaállomás virtualizáció

A munkaállomás virtualizáció külön operációs rendszerkörnyezetet hoz létre a munkaállomáson, így egy újabb verziójú operációs rendszeren a vele nem kompatibilis régi típusú alkalmazás is működhet. A munkaállomás virtualizáció a kiszolgáló virtualizációhoz hasonlóan, virtuális gépek létrehozását teszi lehetővé, amelyek mindegyike egy fizikai számítógépet virtualizál. Virtuális gépek segítségével operációs rendszerek futtathatók, és lehetőség van több operációs rendszer egyidejű futtatására is egyetlen fizikai munkaállomáson.

Ez a technológia olyan helyzetekhez készült, ahol több operációs rendszer támogatása szükséges, például a régi típusú alkalmazások támogatásához, technikai támogatási szolgáltatáshoz, vagy fizikai számítógépek összevonásához. A technológia segítségével egyszerűbb szoftvertesztelés valósítható meg többféle operációs rendszeren, megkönnyítve ezzel a bevezetést.

Tárolás virtualizáció

A tárolás virtualizáció a fizikai adattároló egyesítése, több hálózati tároló eszközből egy adattároló eszközzé, amelyet egy központi konzolról kezelnek. Ez lehetővé teszi, hogy a felhasználók vagy alkalmazások úgy férhessenek hozzá az adattárolóhoz, hogy közben ne kelljen törődnie azzal, hogy hol található fizikailag az adott tároló, és hogy hogyan kell kezelni. A virtuális tárolás egy logikai egyesítése az adatoknak, attól függetlenül, hogy az infrastruktúrán belül hol van a fizikai tároló. A fizikai adattárolót több alkalmazáskiszolgáló

közösen használhatja, és a virtuális réteg mögötti fizikai eszközök úgy látszanak, mintha egyetlen adattároló-készletet alkotnának.

Ez a technológia lehetőséget nyújt a kötetek elrejtésére olyan kiszolgálókkal szembe, amelyek nem jogosultak az adott kötet elérésére, továbbá lehetőséget ad a kötetek menet közbeni megváltoztatására is.

Hálózat virtualizáció

A hálózat virtualizáció kifejezés alatt leggyakrabban a virtuális magánhálózatokat (VPN) lehet érteni. A VPN-ek segítségével a távoli felhasználók úgy férhetnek hozzá a szervezet belső hálózatához, mintha fizikailag is az adott hálózathoz kapcsolódnának. A hálózat virtualizáció segít megvédeni az informatikai környezetet, valamint biztosítja az alkalmazások és az adatok gyors távelérését a felhasználók számára.

9.4 Microsoft virtualizációs megoldásai

A Microsoft különféle technológiák választékát kínálja a kiszolgálók, az alkalmazások és a munkaállomások virtualizálásához:

Server Virtualization

Munkaterhelések összevonása az erőforrások hatékonyabb kihasználása érdekében.

Termékek:

- Microsoft Virtual Server 2005 R2 / Windows Server 2008
- System Center Virtual Machine Manager

Desktop Virtualization

Elszigetelt operációs rendszer környezet létrehozása a munkaállomásokon.

Termékek:

- Microsoft Virtual PC

Application Virtualization

Alkalmazások központosítása és elválasztása a munkaállomás operációs rendszerétől.

Termékek:

- SoftGrid Application Virtualization

Presentation Virtualization

Adatok tárolásának és feldolgozásának központosítása, és a kezelőfelület helyi megjelenítése.

Termékek:

- Microsoft Terminal Services

System Management

Virtuális és fizikai eszközök kezelése egységes eszközkészlet segítségével.

Termékek:

- System Center

9.5 Windows Server 2008 Hyper-V

A virtualizáció már régóta jelen van, azonban eddig elsődleges célja a szoftverek visszafelé kompatibilitásának megőrzése volt. A rugalmasan változtatható informatikai rendszerek iránt egyre nagyobb az igény, ezért manapság már minden virtualizálható. A virtualizáció talán egyik legfontosabb célja az, hogy rendszerünk összetevőit minél inkább elszigeteljük egymástól, és lehetővé váljon ezeknek elemeknek a tetszés szerinti mozgatása, cseréje és frissítése. A Windows Server 2008 Hyper-V a Windows Server 2008 rendszer hypervizor alapú virtualizációs technológiája, amely a gépi virtualizáció támogatásához szükséges összes szolgáltatást tartalmazza.

Tervezés

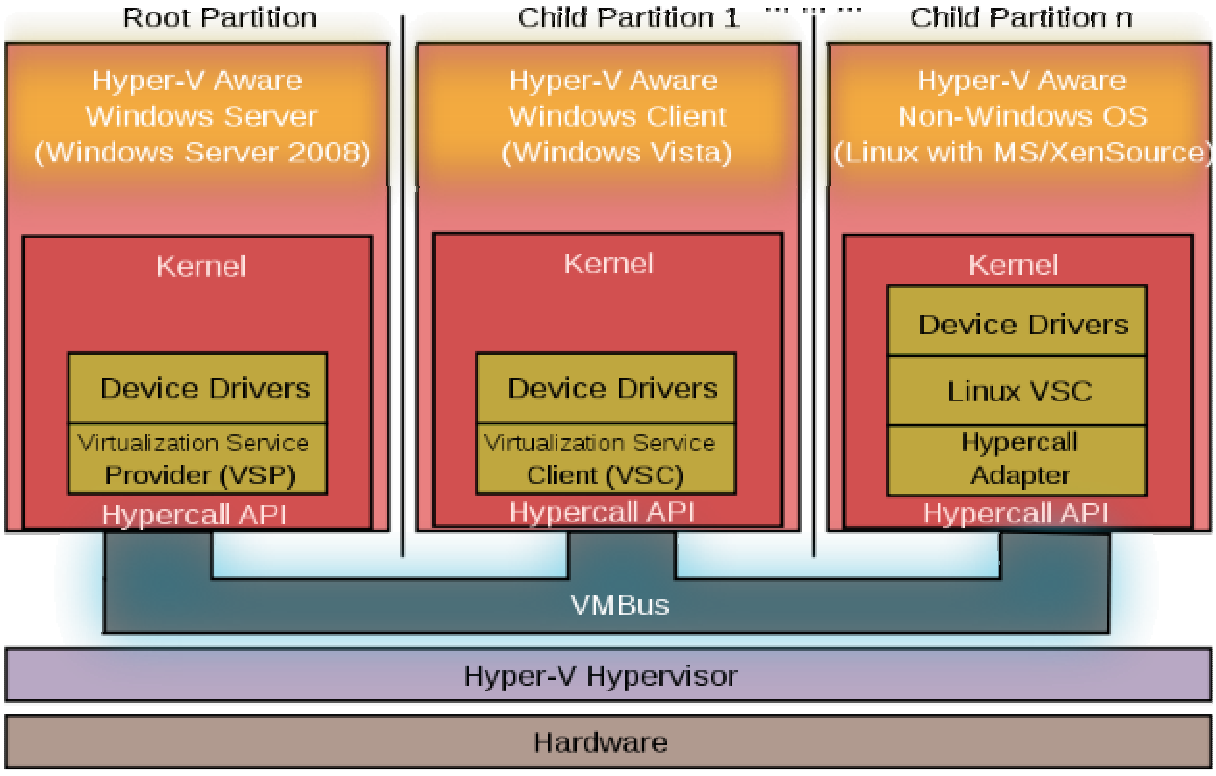
A Windows Server Hyper-V tervezésekor első szempont a biztonság volt. A biztonság elérése érdekében a fő cél az volt, hogy a virtuális rendszerek és a virtualizációt végző infrastruktúra egymástól teljesen elszigetelve legyenek, a virtualizált rendszerek ne érhessék el egymás adatait, és közöttük az erőforrás elosztását a virtualizált infrastruktúra végezze.

További szempont volt még, hogy ennek a virtualizációs rétegnek a kódja a lehető legkisebb legyen, ezzel is csökkentve a támadási felületet. A következő tervezési szempont a megbízhatóság volt, tehát annak az elkerülése, hogy a virtualizációs réteg hibája miatt leállás következzen be, hiszen az a rajta futó összes virtuális gép leállásával is együtt jár. A megbízhatóság érdekében a Windows Server Hyper-V szerkezete egymásra épülő rétegekből áll, amelyek között a kommunikációs kapcsolatok száma alacsony és működésük a lehető legegyszerűbb.

A harmadik tervezési szempont a skálázhatóság volt, tehát annak az elérése, hogy a Hyper-V akármekkora gépen tetszőleges számú virtuális gépet is képes legyen kezelni.

Architektúra

A Microsoft Server 2008 Hyper-V egy 64 bites, mikrokerneles hypervizor alapú virtualizációs technológia. A 64 bites technológia segítségével a virtualizációs réteg a 32 bites rendszerekkel szemben sokkal nagyobb memóriához fér hozzá, másrészt pedig lehetősége van mind 32 és 64 bites virtuális operációs rendszereket futtatni. A hardverhez legközelebb eső rétegek rendelkeznek a legnagyobb jogosultsággal, és ugyanakkor a lehető legkevesebb feladat elvégzésére képesek. Ezért a hypervisor egy apró mikrokernelként jött létre, amely csak azokat a funkciókat tartalmazza, amelyekre feltétlen szükség van. Minden funkció a hypervisor fölötti virtualizációs rétegben, vagy másnéven virtualizációs veremben fut. A hypervisor egy vékony réteg, amely a virtualizált gépek és a hardver között helyezkedik el, közvetlenül a hardveren fut és nincs szüksége host-operációs rendszerre a működéshez. A hypervisor felelős a virtualizált gépek futtatásáért, valamint azért, hogy az általunk megadott beállítások alapján olyan partíciót hozzon létre, amely a többi virtuális géptől teljesen elszigetelt. A hypervisor nem tartalmaz illesztőprogramot, ehelyett az illesztőprogramok a szülőpartíción helyezkednek el, és ez, valamint az új I/O-megosztási modell segítségével a Hyper-V biztonságos architektúrával rendelkezik.



A Hyper-V architektúrája

Az architektúrában van egy kiemelt jelentőségű virtuális gép, amelynek a neve szülőpartíció. Ez a szülőpartíció felelős a hardver kezelésért, valamint ez végzi a további partíciók létrehozásával, törlésével, felügyeletével kapcsolatos feladatokat. A szülőpartícióra kizárólag Windows Server 2008, vagy annak Server Core változat telepíthető. A szülőpartíció leállása esetén valamennyi virtuális gép is leáll. Ennek kikerülése érdekében fürtözni kell egy másik olyan géppel, amelyen szintén megtalálható ez a szülőpartíció, valamint minden virtuális gép másolata. A szülőpartíció amellett, hogy egy teljes értékű operációs rendszer, egyben a hypervisor-réteg kiterjesztése is. Azért előnyös, mert bármelyik driver amelyik itt megtalálható, az elérhető a többi virtuális gép számára is.

Ezekben a partíciókban három olyan technológia működik, amelyek a driverek megosztását segítik. Az első a Visualization Service Provider (VSP), amely a szülőpartícióban fut, kommunikál a driverekkel és megosztja azokat a virtuális gépekkel. A VSP-k telepítése automatikus a szülőpartícióra, amint engedélyeztük rajta a virtualizáció szerepkört. A Virtualization Service Client (VSC) a gyerekpartíciókon futnak és elérhetővé teszik azokat a hardvereket, amelyeket a szülőpartícióra telepítettünk. Minden gyerekpartíción megtalálhatók a VSC-komponensek, annak megfelelően, hogy milyen VSP-ket szeretnénk használni rajtuk. Telepítésük nem automatikus, az Integration Components telepítésével együtt kerül fel a virtuális gépekre. A harmadik a VMBus, amely a partíciók közötti adatkommunikációért felelős. Ezen keresztül kommunikálnak egymással a VSC-k és a VSP-k, de a hypervisor nem érhető el ezen keresztül.

Összességében elmondható, hogy ezek a technológiák növelik a virtualizált rendszerek teljesítményét, és lehetővé teszik olyan eszközök megosztását és virtualizálását, amelyre eddig nem volt lehetőség. Ezen technológiák nem váltják fel a hardveremulációt, mivel egyetlen operációs rendszer sem tartalmazza alapból a VSC-komponenseket, ezért legalább a virtuális gépek telepítésének ideje alatt szükség van hardveremulációra. A bootolás korai szakaszába is szükség van emulált eszközökre, mert a VSC-k csak később töltődnek be, de amint ez megtörténik, teljesen átveszik az irányítást az emulált eszközöktől.

Felügyeleti és eszközbeállítási funkciók

A hatékony folyamatkezelés mellett a virtualizált szolgáltatásokat nyújtó számítógép, üzem közben is bővíthető erőforrásokal. Virtuális gépekhez futás közben adhatunk processzormagokat, memóriát, tárolóeszközöket, hálózati kártyákat anélkül, hogy bármilyen szolgáltatást le kellene állítanunk.

A Hyper-V akár nyolc processzormag hozzárendelését is támogatja egy virtuális géphez. A memóriakezelés területén megjelent Page Sharing technológia lehetővé teszi az azonos memórialapok megosztását a virtuális gépek között. Ez azonos operációs rendszerek esetén nagyon hasznos, mert kevesebb memóriára lesz szüksége az azonos virtuális gépeknek. A memóriakezelést segíti a Memory Reserves funkció, amely lehetőséget ad arra, hogy a virtuális gépekhez rendelt memória egy adott százalékát csak akkor adjuk oda a virtuális gépeknek, ha tényleg szüksége van rá. Ennek a két memóriakezelési funkciónak tesztrendszerek kiépítése esetén van nagy jelentősége, valamint akkor, ha nem rendelkezünk korlátlan mennyiségű memóriával.

Hálózatkezelés területén virtuális gépenként akár nyolc hálózati csatoló használatára is lehetőség van, de ehhez a megfelelő VSC-k telepítése is szükséges. Az emulált eszközökkel pedig maximum négy hálózati kártya használata lehetséges. A virtuális gépek összekapcsolása virtuális hálózattal, egy virtuális switch segítségével történik, amely csak azokra a portokra küldi el a csomagokat, ahova tényleg szükséges. Lehetőség van VLAN-ok használatára, és virtuális hálózatok akár a NAP-al is képesek együttműködni.

A virtuális gépek felügyelete MMC segítségével történik, ami távolról is elérhető. A régebbi VMRC protokoll helyett minden RDP-vel érhető el, ezáltal lehetőség van olyan virtualizált operációs rendszerre is csatlakozni, ami nem támogatja a Terminal Services-t. A virtuális gépek felügyeleténél érdemes még megemlíteni a System Center Virtual Machine Manager és a Volume Shadow Copy szolgáltatásokat. A VSC szolgáltatás segítségével lehetőség van pillanatkép készítésére a virtuális gépről. A Virtual Machine Manager virtualizált adatközpontok felügyeltére készült, amely lehetővé teszi az infrastruktúra központi felügyeletét, a fizikai kiszolgálók jobb kihasználtságát, valamint az új virtuális gépek gyors üzembe állítását.

9.6 Windows Server Hyper-V technológia alkalmazási területei

A Hyper-V technológia segítségével több különböző operációs rendszer futhat, egymással párhuzamosan, egyetlen kiszolgálón az x64-alapú informatikai környezet teljesítményének kihasználása érdekében.

A Hyper-V technológia négy alapvető területen hasznosítható:

Kiszolgálók összevonása

A virtualizáció bevezetésének egyik legfőbb indoka a funkcionalitás átvitele sok kiszolgálóról kevesebb kiszolgálóra. A virtualizáció használatával nemcsak számos kiszolgáló vonható össze, hanem az ezek közötti izoláció is fenntartható, ezáltal egy rugalmasabb környezet alakul ki. Ezek segítségével javítható a kiszolgálók kihasználtsága, csökkenthető a felügyeleti költség valamint a terhelés is jól eloszthető az erőforrások között.

Folyamatos üzem és katasztrófa-helyreállítás

A folyamatos üzem biztosítása arra irányul, hogy a tervszerű és nem tervezett leállási idő minimális legyen, amelybe beletartoznak a rutinfeladatok, a karbantartás, a biztonsági mentés valamint a váratlan leállások miatt kiesett idő. A fürtszolgáltatás használatával a Hyper-V technológia támogatja az informatikai környezeten belüli, vagy a több adatközpontra is kiterjedő katasztrófa helyreállítást. A gyors vészhelyreállítás biztosítja azt, hogy az adattárolás legfeljebb minimális legyen.

Telepítés és tesztelés

Tesztelés és fejlesztés területén a virtuális gépek segítségével számos különböző használati környezet alakítható ki, amelyet tesztelhetnek egy biztonságos, független környezetben. Ezen folyamat által megfigyelhető a fizikai kiszolgálók és ügyfélgépek működése. Hyper-V technológia segítségével maximálisra növelhető a teszthardverek kihasználtsága, hatékonyabb életciklus kezelés valósítható meg és mivel több különböző operációs rendszerrel is használható, ezért jól alkalmazható tesztelői és fejlesztői környezetben.

Dinamikus adatközpont

A Hyper-V technológia és a megfelelő rendszerfelügyeleti eszközök használatával valóra váltható a dinamikus adatközpontok jövőképe. A virtuális gépek automatizált

újrakonfigurálása, a gyors áttelepítési lehetőség és az erőforrások rugalmas kezelése segítségével egy dinamikus informatikai környezet alakítható ki.

A virtualizáció célja nemcsak az, hogy kiszolgálókat vonjunk össze, hanem az is, hogy növeljék a szolgáltatások elérését a nem virtualizált kiszolgálókhoz képest. A Hyper-V támogatja több vendég fürtbe szervezését, továbbá Hyper-V-t futtató fizikai számítógépekből is fürtöt képezhetünk. Így a virtualizált példányok egy másik állomást használnak, ha valami történik az elsődleges gazdagéppel. A virtualizált vendégeket leállás nélkül át lehet telepíteni az egyik fizikai gépről a másikra, ami megkönnyíti a szolgáltatást és a tervezést.

9.7 A Hyper-V technológia tulajdonságainak összefoglalása

Követelmények és határok:

A Hyper-V a következők meglétét igényli:

- x64-es Windows Server 2008 Standard, Enterprise vagy Datacenter Edition akár teljes, akár Server Core változatban a szülőpartícióra.
- x64-es processzor, Intel VT vagy AMD-V technológiával

Ugyanakkor lehetőség van:

- 64 és 32 bites virtuális operációs rendszer kiszolgálására
- akár 8 processzormag hozzárendelése bármely virtuális géphez
- 2 terrabájt memóriát lehet szétosztani a virtuális gépek között
- tetszőleges számú virtuális gép futtatása

	Standard (x64)	Enterprise (x64)	Datacenter (x64)
A támogatott fizikai processzorok száma	1 – 4	1 – 8	1 – 64
Maximálisan támogatott memória	32 GB	2T	2T
Cluster– támogatás	nem	igen	igen

A Hyper-V technológia új és továbbfejlesztett funkciókat biztosít:

Operációs rendszerek széleskörű támogatása:

Számos különböző típusú operációs rendszer futtatható egyidejűleg, ezek lehetnek 32 bites és 64 bites rendszerek is, különböző kiszolgálói platformról.

Új és továbbfejlesztett architektúra:

Az új 64 bites mikrokerneles hipervisor-architektúra révén a Hyper-V széles körű módszerekkel támogatja a különböző eszközöket, és a nagyobb teljesítmény mellett fokozott biztonságot nyújt.

SMP támogatás:

Lehetőség van akár négy processzort tartalmazó szimmetrikus multiprocesszoros (SMP) rendszerek támogatására virtuális gépi környezetben, a többszálas alkalmazások előnyeinek kihasználásához.

Memóriahasználat:

A virtuális gépek számára nagyméretű memória allokálható, így a feladatok legnagyobb többsége virtualizálható.

Hatékonyabb hozzáférés az adattárolóhoz:

A közvetlen lemezhozzáférés, a tárolóhálózatok (SAN) valamint a belső lemezegységek elérésének támogatása révén, a Hyper-V technológia nagyobb rugalmasságot nyújt a tárolási környezetek konfigurálásához és kihasználtságához.

Hálózati terheléselosztás:

A Hyper-V technológia új virtuális átkapcsolási lehetőségeket biztosít, így a virtuális gépek egyszerűen konfigurálhatóak a Windows hálózati terheléselosztási (NLB) szolgáltatásának futtatására, és a terhelés, különböző kiszolgálón található virtuális gépek között is eloszthető.

Új hardvermegosztási architektúra:

Az új virtuális szolgáltatói és virtuális ügyfél architektúra (VSP/VSC) révén a Hyper-V technológia a központi erőforrások, például a lemezegységek, a hálózat, a megjelenítési eszközök stb. hatékonyabb elérést és kihasználását teszi lehetővé.

Gyors áttelepítés:

A Hyper-V technológia lehetővé teszi egy működő gép gyors áttelepítését egyik fizikai rendszerről a másikra, a Windows Server és System Center magas felügyeleti eszközeinek használatával.

Pillanatkép a virtuális gépről:

A Hyper-V technológia használatával a működő virtuális gépről pillanatfelvételek készíthetők, így egyszerűen visszaállítható a gép korábbi állapota, és a biztonsági mentés, valamint a helyreállítás hatékonyabban megoldható.

Méretezhetőség:

A gazdagép szintjén a több processzor és processzormag támogatása, valamint a virtuális gépeken belüli fejlettebb memória-hozzáférés révén a virtualizációs környezet már vertikálisan is méretezhető annak érdekében, hogy egy adott kiszolgálón nagyszámú virtuális gép legyen használható. A méretezhetőség érdekében lehetőség van a virtuális gépek más gazdagépre történő áttelepítésére.

Bővíthetőség:

A Hyper-V technológia szabványos WMI-illesztőfelületei és API-felületei segítségével a szoftvergyártók és fejlesztők gyorsan készíthetnek fejlesztéseket a virtualizációs platformra.

9.8 Hyper-V telepítése

Ahhoz, hogy használni tudjuk a Hyper-V-t szükség van a megfelelő hardverre, mégpedig konkrétan egy olyan számítógépre, amely képes 64 bites operációs rendszert futtatni. A Hyper-V szerepkör telepítését rendszergazdaként bejelentkezve kell végrehajtani, az alábbi lépések alapján:

1. Server Manager (Kiszolgálókezelő) program elindítása
2. A Roles Summary (Szerepkörök összegzése) / Add Roles (Szerepkörök hozzáadása) hivatkozás, majd pedig a Hyper-V lehetőség kiválasztása.
3. A varázsló lépéseinek követése. A virtuális számítógépeknek nem kell engedélyeznünk a hálózati erőforrások elérését, de egy hálózati kártyát ki kell választani azért, hogy egy virtuális kapcsolóhoz köthessük.

4. Újraindítás után töltsük be a Server Manager-t, azon belül bontsuk ki a Roles (Szerepkörök) ágát és válasszuk ki a Hyper-V elemet.
5. Ellenőrizzük a jobb oldali táblarészben, hogy fut-e a „vhdsvc” és a „vmms”. Ha igen, akkor a Hyper-V szerepkör telepítése sikeres volt.

A Hyper-V a Server Core lehetőséggel telepített Windows Server 2008-ra is telepíthető. Server Core verzióban a Hyper-V telepítése a következő parancs segítségével történik:

start /w ocsetup Microsoft-Hyper-V

9.9 Virtualizáció és fürtkezelés

A Hyper-V virtualizáció és fürtszolgáltatás egyre inkább előtérbe kerülő megoldást kínál a magas rendelkezésre állás tekintetében. A virtualizáció önmagában nem kínál magasabb rendelkezésre állást, ennek elérése érdekében a fürtkezeléssel kell együtt alkalmazni.

Quick Migration és Live Migration

Előfordulhat, hogy egy tervezett leállás miatt a cluster egyik node-ját le kell állítani, és át kell helyezni a virtuális gépet egy másik node-ra. A Quick Migration erre a problémára nyújt megoldást, segítségével nem kell leállítani a virtuális gépünket áthelyezés esetén. Mivel tud Hyper-V állapotot menteni, ezért a mozgatást megelőzi az állapot mentése a közös diszkre, ahonnan a másik node a mentett állapotot olvassa be. Ezáltal könnyedén és rövid idő alatt lehet áthelyezni virtuális gépünket egyik node-ról a másikra.

A Live Migration hasonló elven működik mint a Quick Migration annyi különbséggel, hogy ez a virtuális gép mozgatásakor keletkezett köztesidőt szünteti meg. Ami annyit jelent, hogy mozgatáskor, azaz a host tervezett leállásából adódóan a guest egy másik node-ra való átterhelése közben a kapcsolat a szolgáltatással kliensoldalról nézve nem, vagy csak nagyon rövid időre szakad meg.

A virtualizáció megjelenésével a fürt, amely maga is egyfajta virtualizációs technológia, nem alkalmazásokat biztosít, hanem azok magas rendelkezésre állását teszi lehetővé.

Összességében tehát elmondható, hogy a virtualizáció jelentősége és jövője megkérdőjelezhetetlennek látszik, főleg ha a magas rendelkezésre állással is párosul.

10 ÖSSZEFOGLALÁS

Dolgozatom témáját a Windows Server 2008 újdonságainak bemutatása adta. Így a dolgozat elkészülte után elmondhatom, hogy rendkívül hasznos információkkal és tudással gazdagodtam a kutatómunka és a dolgozat írása során, amiket minden bizonnyal hasznosítani tudok majd a további munkám során.

A szakdolgozat magírása egyaránt volt élvezet és munka is számomra. Amikor hozzáfogtam, mindenekelőtt azt szerettem volna kideríteni, hogy milyen újdonságokat hozott magával a Windows Server 2008 operációs rendszer az előző generációs Windows-kiszolgálókhoz képest. Egy operációs rendszer újdonságainak és az ezekkel járó belső működésének feltérképezése hatalmas kutatómunkát igényel, amelyről több száz oldalas dokumentációt is lehetne írni. Ezért esett választásom a biztonság és a virtualizáció témakörök bemutatására, mivel úgy gondolom, hogy napjaink informatikájában talán az egyik legfontosabb, és a legnagyobb tömeget megosztó kérdések közé tartozik.

A Windows Server 2008 használatakor azonnal feltűnik, hogy különbözik a korábbi Windows kiszolgálói kiadásoktól. Ami nem tűnik fel azonnal, az a különbség mértéke, hiszen az operációs rendszer legfontosabb változásai megbújnak a felszín alatt. Ezek a változások nemcsak a felhasználói felületet érintik, de a mögöttes architektúrát is, és pontosan ezeket a változásokat volt legnehezebb felkutatni.

A szakdolgozat készítése során próbáltam rávilágítani az elmúlt öt év legfontosabb újdonságaira, bár tudom, hogy ezen újdonságok részletes bemutatása nagyobb terjedelmet igényelne, akár több könyvet is lehetne írni erről, de én mégis úgy gondolom, hogy az olvasó számára egy megfelelő áttekintést nyújtott az elmúlt évek technológiai újdonságairól. Természetesen ezek csak dióhéjban tartalmazzák mindazt a rengeteg újdonságot, ami jelen van a Windows Server 2008 operációs rendszerben, amelynek részletesebb megismerése mélyebbre ható tanulmányozást igényel.

Dolgozatomban próbáltam bemutatni az olvasó számára, hogy miért is van ilyen nagy jelentősége ezeknek a technológiáknak, hiszen ezek a dolgok mind jelen vannak az informatikában, ugyanakkor láthatatlanok az emberek számára.

Úgy gondolom, hogy a bevezetésben tett célkitűzéseimet, ha nem is maradéktalanul de sikerült teljesítenem, és remélem, hogy az olvasó számára sikerült hasznos ismereteket bemutatnom.

11 Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőmnek, Dr. Krausz Tamásnak a szakdolgozatom elkészítésében nyújtott szakmai segítségéért és útmutató tanácsaiért.

12 Irodalomjegyzék

Jonathan Hassel:

Windows Server 2008 : The Definitive Guide

John Savill:

Complete Guide to Windows Server 2008

Jeffrey R. Shapiro:

Windows Server 2008 Bible

Joseph Davies and Tony Northrup:

Windows Server 2008 Networking and Network Access Protection

William R. Stanek:

A rendszergazda zsebkönyve

http://www.microsoft.com/hun/windowsserver2008

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

http://technet.microsoft.com/hu-hu/library/cc730957.aspx

http://winportal.net

http://www.microsoft.com/hun/technet

http://www.microsoft.com/hun/virtualization

http://www.microsoft.com/windowsserver2008/en/us/hyperv-main.aspx