Debreceni Egyetem

Informatika Kar

Windows Server 2008 újdonságai

Témavezető:

Dr. Krausz Tamás

Egyetemi adjunktus

Készítette:

Kántor András

Mérnök Informatikus

Debrecen

2010

Tartalomjegyzék

I. Bevezetés

A Windows Server 2008 napjaink legjobb olyan Microsoft terméke, amely elsősorban szervergépekre lett tervezve. Az új verzió a megbízhatóságával és az energiatakarékosságával fogja belopni magát a szívünkbe. Rengeteg újdonsággal rendelkezik, amelyeket elsőként ebbe az operációs rendszerbe implementáltak. A Windows Server 2008 a kis és nagyvállalatok igényeit egyaránt kielégíti, mégpedig úgy, hogy a termékcsalád tagjai a vállalatok nagyságának függvényében változnak.

A szakdolgozatom célja ennek a terméknek a bemutatása, egy-két helyen részletesebben, máshol kevésbé belemélyülten taglalva a téma terjedelme miatt. Az operációs rendszer telepítése és használata egyaránt egyszerű és könnyen átlátható, felhasználóbarát a környezet.

De talán nem is ez a legfontosabb szempont egy operációs rendszer kiválasztásánál, hanem inkább a megbízhatóság. Manapság már nagyon elterjedt a hackerkedés és mivel a nagyvállalatoknak fontos, hogy az üzlettel kapcsolatos információk biztonságban legyenek, a legfontosabb, hogy a telepített operációs rendszer a lehető legmegbízhatóbb és legbiztonságosabb legyen. Ezt a megbízhatóságot úgy tudjuk elérni, hogyha először is a megfelelően van megtervezve a hálózat, másodszor a hálózathoz hozzáférő számítógépek a biztonsági előírásoknak megfeleljenek, ezen kívül a támadható pontokat is minimalizálni kell.

A Windows Server 2008ban ez mind benne van. A felhasználók számítógépeinek „egészségi” ellenőrzése, jogosultságok meghatározása, a Server Core telepítési lehetőségnek köszönhetően csak a létfontosságú szolgáltatások lesznek telepítve.

A felhasználók kiszolgálásának minősége sem utolsó szempont. Lehetővé teszi, hogy akár otthonról is biztonságosan bejelentkezzünk a cég belső hálózatára, persze nem kapunk korlátlan hozzáférést. Az erőforrásokat jól osztja meg a kiszolgálandó felek között, a beépített virtualizációs eszköz segítségével pedig előre tesztelhetjük a rendszert.

A Windows Server 2008 első verziója a 6.0-ás Kernelre épült, de a Windows 7-tel együtt megjelent a Windows Server 2008 R2-es változata, amely már a 6.1es verzióra épül, további újdonságokat hozva magával, ezzel együtt növelve megbízhatóságát, hatékonyságát, hardverkihasználását, energiatakarékosságát.

A Windows Server 2008 bármely vállalati környezetben megállja a helyét ezért is ajánlom minden rendszergazdának a használatát.

II. A Windows Server 2008 termékcsalád tagjai:

II.1 Windows Server 2008 Standard

A Windows Server 2008 értékes új funkciókkal és hatékony fejlesztésekkel egészíti ki a központi Windows Server operációs rendszert, így tetszőleges méretű szervezet a változó üzleti igényeknek megfelelően fokozhatja a rendszer ellenőrzését, rendelkezésre állását és rugalmasságát. Az új webes eszközök, virtualizációs technológiák, biztonsági fejlesztések és felügyeleti segédprogramok révén idő és pénz takarítható meg, és szilárd alap biztosítható a vállalat informatikai infrastruktúrája számára.

II.2 Windows Server 2008 Enterprise

Korszerű kiszolgálói platform, amely gazdaságosabb és megbízhatóbb támogatást nyújt az üzletmenet szempontjából létfontosságú feladatok ellátásához. Innovatív szolgáltatásokat kínál a virtualizáció, az energiatakarékosság és a felügyelet terén, és egyszerűbbé teszi a mobil munkatársak számára a vállalati erőforrások elérését.

II.3 Windows Server 2008 Datacenter

A nagyarányú virtualizációhoz és a vertikálisan méretezhető munkaterhelésekhez ideális operációs rendszer. A Windows Server® 2008 Datacenter rendszer ideális kis- és nagyméretű kiszolgálói rendszerek nagyarányú virtualizálására, valamint a méretezhetőség, a megbízhatóság és a rendelkezésre állás legmagasabb szintjét igénylő, üzleti szempontból kulcsfontosságú alkalmazásokat ellátó munkaterhelések működtetésére. A korlátlan virtualizációs használati jogoknak és a hipervizor-alapú virtualizációs technológiának köszönhetően a Windows Server 2008 Datacenter rendszer biztosítja a szükséges rugalmasságot és gazdaságosságot nagyszámú virtualizált Windows Server® példány egyszerű üzemeltetéséhez. Eleget tesz a nagyszabású, üzleti szempontból kulcsfontosságú munkaterhelések – például a vállalati erőforrás-tervezés, az adatbázis-kezelés, a kiszolgálók összevonása, valamint az egyéni és az üzleti célú alkalmazások – memória- és teljesítményigényének.

II.4 Windows Web Server 2008

A Windows Server korábbi verzióinál robusztusabb képességekkel rendelkezik. Azt nyújtja, amire a felhasználónak egy nagyszabású, nagy rendelkezésre állású, egy pontban hosztolt környezetekre dedikált webes környezet támogatásához szüksége van, mindezt egyazon Windows Server-verzión belül. A kifejezetten egy feladatra tervezett Windows Web Server 2008 ideális webes alkalmazások és szolgáltatások biztosítására. A frissen áttervezett Internet Information Services 7.0 (IIS 7.0), ASP.NET és a Microsoft® .NET Framework környezettel integrálva, valamint a Microsoft® SQL Server™ helyi telepítésének támogatásával a Windows Web Server 2008 lehetővé teszi, hogy a vállalatok gyorsan hozhassanak létre weblapokat, webes alkalmazásokat és szolgáltatásokat.

II.5 Windows Server 2008 for Itanium-Based Systems

Az Itanium-alapú rendszerekhez készült változat nagyvállalati kategóriájú platformot biztosít az üzletmenet szempontjából létfontosságú alkalmazások rendszerbe állításához. Méretezési adatbázis, üzleti és egyéni alkalmazások szolgálják a növekvő üzleti igények kielégítését. A magas rendelkezésre állást segítik a feladatátvételi fürtszolgáltatások (failover clustering) és a dinamikus hardverparticionálási lehetőségek. A Windows Server korlátlan számú virtuális példányának futtatására feljogosító licenceknek köszönhetően a rendszerek virtualizáltan is üzembe helyezhetők. Az Itanium-alapú rendszerekhez készült Windows Server 2008 R2 biztosítja az alapokat a kiemelkedően dinamikus informatikai infrastruktúrák számára.

II.6 Windows HPC Server 2008

A nagy teljesítményű számítástechnika (HPC) következő generációja. Nagyvállalati kategóriájú eszközöket kínál a kiemelkedően hatékony HPC-környezetek megvalósításához. A Windows HPC Server 2008 akár több ezer processzormagra is hatékonyan méretezhető, és a rendszer állapotának és stabilitásának proaktív megfigyelésére és fenntartására szolgáló felügyeleti konzolokat is tartalmaz. A feladatütemezés terén megvalósított együttműködő-képesség és rugalmasság lehetővé teszi a Windows és a Linux rendszerű HPC-platformok integrációját, továbbá biztosítja a kötegelt és a szolgáltatásorientált alkalmazási (SOA) jellegű munkaterhelések támogatását.

III. A Windows Server 2008 újdonságai

A Windows Server 2008 rengeteg újdonsággal rendelkezik elődjéhez képest. A következőket fogom bővebben kifejteni:

- Server Core,
- Hyper-V,
- Active Directory,
- Read Only Domain Controllers,
- Network Access Protection,
- Terminal Services,
- Windows PowerShell,
- Bitlocker,
- Windows System Resource Manager,
- Secure Socket Tunneling Protocol,
- Windows Advanced Firewall,
- Policy Based Quality of Service,
- Windows Internet Name Service.

III.1 Server Core

A Server Core (kiszolgálómag) a Windows Server 2008 telepítési lehetősége, amely csak egy részhalmazát tartalmazza a végrehajtható fájloknak és a kiszolgálói szerepeknek. A Core változat csak a Standard, Enterprise és Datacenter termékekhez lett létrehozva. A minimalizált telepítés elérhető X86 és X64 architektúra esetén is. Természetesen nem kell külön megvásárolnunk a Core verziót, csak el kell döntenünk, hogy a teljes vagy a minimalizált változat kerüljön-e számítógépünkre. Telepítéskor figyelembe kell vennünk, hogy csak újratelepítés lehetséges, előző telepített termék frissítése nem. A kiszolgáló kezelését a parancssoron vagy egy önállóan futó beállító fájlon keresztül végezhetjük. A Microsoft azoknak a szervezeteknek szánják, akik vagy sok kiszolgálót üzemeltetnek, amelyeknek csak bizonyos kijelölt feladatokat kell végrehajtaniuk, de azokat kiemelkedő stabilitással, vagy olyan környezetet tartanak fenn, ahol magasak a biztonsági követelmények, és a kiszolgálónak csak minimális felületet szabad nyújtania a támadásoknak.
Ennek megfelelően a Core kiszolgálók csak bizonyos szerepeket tölthetnek be:

- DHCP kiszolgáló
- DNS kiszolgáló
- Fájlkiszolgáló, beleértve a fájltöbbszörözési szolgáltatásokat, az elosztott fájlrendszert (DFS), az elosztott fájlrendszeri többszörözést (DFSR), a hálózati fájlrendszert és az egypéldányos tárolást (SIS)
- Nyomtatási szolgáltatások
- Tartományvezérlő, beleértve az írásvédett tartományvezérlőket
- AD LDS kiszolgáló
- Windows Server Virtualization (virtuális Windows-kiszolgáló)
- IIS, bár a szokásos lehetőségeknek csak egy részével (statikus HTML-tárolás, a dinamikus webalkalmazások támogatása nélkül)
- Windows-médiaszolgáltatások (WMS, Windows Media Services)

A Server Core gépek ezen kívül részt vehetnek Microsoft-fürtökben, hálózati terheléselosztást alkalmazhatnak, helyet adhatnak Unix-alkalmazásoknak, titkosíthatják a meghajtóikat a Bitlocker segítségével, távolról kezelhetők a Windows PowerShell segítségével egy ügyfélgépről, és megfigyelhetők az SNMP-n keresztül.

Nagyszerűen alkalmazható fiókirodákban, ahol a számítógépeken tartományvezérlői feladatokat látnak el, és kitűnően hasznosíthatják a némileg régebbi hardvereszközöket, amelyeket másképp le kellene selejtezni. A Server Core kisebb mérete lehetővé teszi az operációs rendszernek, hogy kevesebb rendszererőforrást használjon fel, a támadásokra kevés alkalmat adó felülete és a stabilitása pedig nagyszerű választássá teszi az említett feladatokra. Ezenkívül egy fiókirodában könnyűsúlyú, biztonságos megoldást jelent, mert a Server Core-ral a kiszolgáló írásvédett tartományvezérlőként is működhet, amelyen mindent titkosíthatunk a BitLocker segítségével.

III.2 Hyper-V

A Windows Server 2008 Hyper-V a Windows Server 2008 rendszer hypervisor-alapú virtualizációs technológiája, amely a gépi virtualizáció támogatásához szükséges összes szolgáltatást tartalmazza. A Hyper-V technológia segítségével az informatikai osztályok csökkenthetik költségeiket, javíthatják a kiszolgálók kihasználtságát, és a korábbinál dinamikusabb IT-infrastruktúrát építhetnek ki. A Hyper-V technológia fokozott rugalmasságot nyújt, mert a dinamikus, megbízható és méretezhető platform szolgáltatásait egyetlen integrált felügyeleti eszközkészlettel ötvözi. Immár lehetőség van olyan virtuális gépek létrehozására, amelyek teljesen kihasználják a rendelkezésre álló hardvert, több operációs rendszer futtatására alkalmasak, és ugyanazon iparági szabványt jelentő eszközök használatával képesek a virtuális és a fizikai erőforrások kezelésére.

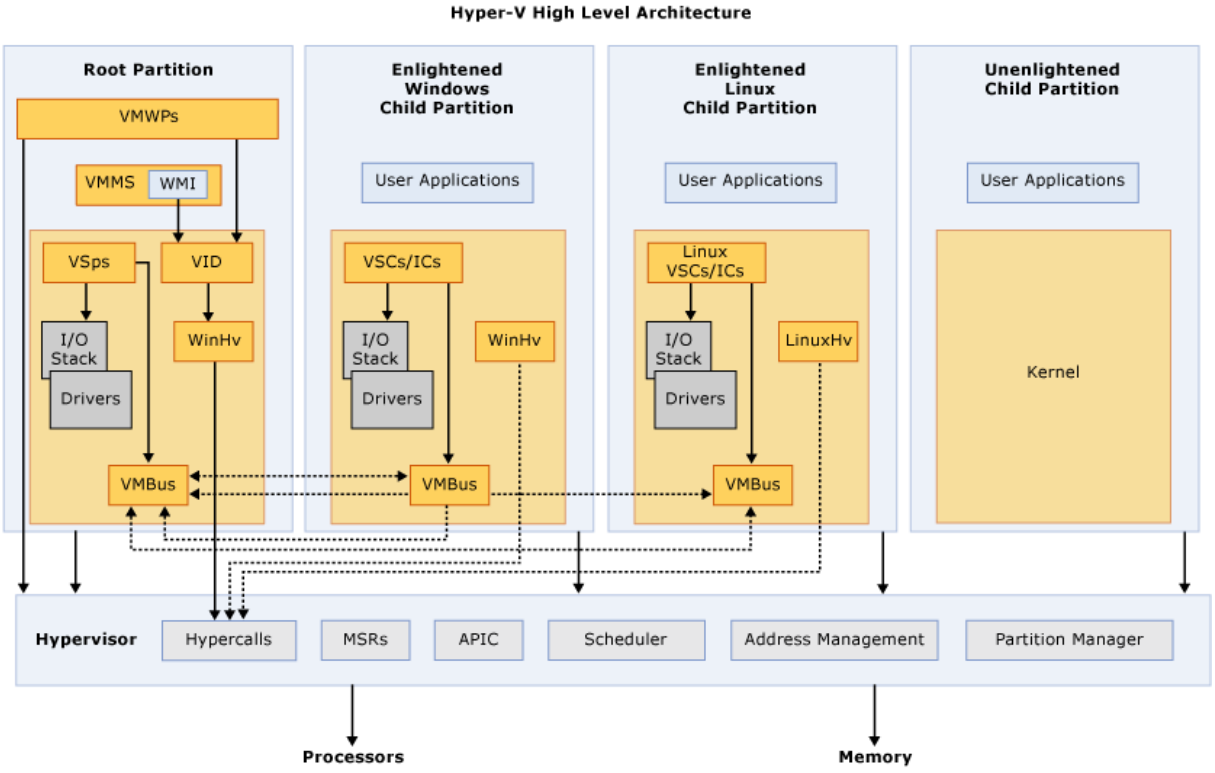
Az új 64 bites mikrokerneles hypervisor-architektúra révén a Hyper-V széles körű módszerekkel támogatja a különböző eszközöket, és a nagyobb teljesítmény mellett fokozott biztonságot is nyújt. Lehetőség van akár 4 processzort tartalmazó szimmetrikus multiprocesszoros (SMP) rendszerek támogatására a virtuális gépi környezetben a többszálas alkalmazások előnyeinek teljes kihasználásához. A virtuális gépek számára nagyméretű memória allokálható, így a feladatok legnagyobb többsége virtualizálható. A Hyper-V technológia ezáltal ideális platformot jelent mind a nagyvállalatok, mind a kis- és középvállalatok számára. A közvetlen lemezhozzáférés, valamint a tárolóhálózatok (SAN) és a belső lemezegységek elérésének kiterjedt támogatása révén nagyobb rugalmasságot nyújt a tárolási környezetek optimális konfigurálásához és kihasználásához. Új virtuális átkapcsolási lehetőségeket biztosít, így a virtuális gépek egyszerűen konfigurálhatók a Windows hálózati

terheléselosztási (NLB) szolgáltatásának futtatására, és a terhelés különböző kiszolgálón található virtuális gépek között is eloszthatóó. 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 elérését és kihasználását teszi lehetővé. Lehetővé teszi egy működő virtuális gép gyors, minimális leállási idő alatti áttelepítését egyik fizikai rendszerről a másikra a Windows Server és a System Center megszokott, magas rendelkezésre állást biztosító felügyeleti eszközeinek használatával. Használatával a működő virtuális gépről pillanatfelvételek készíthetők, így egyszerűen visszaállítható a gép korábbi állapota, és a biztonsági mentés és helyreállítás is hatékonyabban megoldható. A Hyper-V technológia szabványos WMI-illesztőfelületei és API-felületei segítségével a független szoftvergyártók és fejlesztők gyorsan készíthetnek egyéni megoldásokat, segédprogramokat és egyéb fejlesztéseket a virtualizációs platformra. A virtuális gépek kezelésére több eszköz is rendelkezésünkre áll. Egyik ezekből a Hyper-V Managerrel, ez egy kezdetleges, kevés funkcióval ellátott program ezért ajánlottabb a System Center Virtual Machine Manager 2007-et (SCVMM) használni. Az SCVMM segítségével kezelhetünk mind fizikai mind virtuális gépeket.

III.2.1 Hyper-V Architektúra

A partíció egy logikai része az izolációnak, amelyet támogat a hypervisor attól függően, hogy milyen operációs rendszert futtat. A Microsoft hypervisor tartalmaz, egy root vagy szülőpartíciót, amely a Windows Server 2008 64-bites változatát futtatja. A virtualizációs verem ezen a partíción fut, és direkt hozzáférése van a hardverekhez. A root partíció hozza létre a gyermekpartíciókat az Application Programming Interface (API) hyperhívásával.
A partícióknak nincs hozzáférése a fizikai processzorhoz, és nem is kezelik a processzor megszakításokat. E helyett virtuális képük van a processzorról, és minden egyes partíciónak van külön privát virtuális memória lefoglalva. A hypervisor kezeli a megszakításokat, és kezeli a kommunikációt vissza a megfelelő partíciókhoz. Hyper-V képes hardvergyorsításra a virtuális gépek között az Input Output Memory Management Unit (IOMMU) használatával, amely a memóriakezelőtől függetlenül működik a processzort használva. Az IOMMU újratérképezi a fizikai memóriát, majd hozzárendeli őket azokhoz a gyermekpartíciókhoz, amelyek használják. A kérések a szülőpartícióhoz kerül, vagy a hypervisorron vagy a

VMBuson keresztül, amelyek itt kiszolgálásra kerülnek. A VMBus egy logikai kommunikációs csatorna a partíciók között. A szülőpartíció Virtualization Service Providereket (VSP) használ, amelyek VMBuson keresztül kommunikálnak, hogy kiszolgálják a gyermekpartíciók virtuálishardver igényeit. A gyermek partíciók Virtualization Service Consumereket (VSC) használnak, amelyek irányítják a kéréseket a szülőpartíción lévő VSPhez a VMBuson keresztül. A virtuális eszközök használhatják a Windows Server Virtualization sajátosságát, amelynek neve Enlightened I/O (Enlightened = felvilágosult) adattárolásra, hálózati kommunikációra és alrendszerek elérésére. Az Enlightened I/O egy speciális virtualizációs implementáció, amely magába foglal magas szintű kommunikációs protokollokat (pl SCSI), amely a VMBus-t direktben irányítja, átugorva az emulációs rétegeket. Ez hatékonyabbá teszi a kommunikációt, de ehhez szükség van felvilágosult hypervisorra és VMBusra. Szükséges egy processzor, amely tartalmaz hardversegítő virtualizációt, például Intel VT vagy AMD Virtualization (AMD-V) technológia.



APIC: Advanced Programmable Interrupt Controller – Az eszköz, amely a megszakítások prioritását állítja be.
Child Partition: Gyermekpartíció
Hypercall: Interfész a hypervisorral való kommunikálásra.
Hypervisor: A réteg, amely a hardver és az operációs rendszerek között áll. Elsődleges feladat a partíciók elkülönítése. Irányítja a hozzáférést a hardverhez.
IC: lehetővé teszi a kommunikációt a hypervisorral és a többi partícióval
MSR: Memory Service Routine

Root Partition: Szülőpartíció, csak egy van belőle, és ő szolgálja ki a gyermekpartíciókat. Az egyetlen partíció, amelynek van hozzáférése a fizikai memóriához és eszközökhöz.
VID: Virtualization Infrastructure Driver. Gondoskodik a partíciók, a virtuális processzor és a virtuális memória kezeléséről.
VMBus: A partíciók közti kommunikációt teszi lehetővé.
VMMS: Virtual Machine Management Service. A gyermekpartíciók állapotát irányítja.
VMWP: Virtual Machine Worker Process. Feladati: létrehozás, configurálás, futtatás, megállítás, újraindítás, mentés, és tárolás, valamint pillanatkép készítése az adott virtuális gépről.
WinHv: Windows Hypervisor Interface Library. Összeköttetés a partíció operációs rendszerének driverei illetve a hypervisor között, amely lehetővé teszi a drivereknek a hypervisor hívását.
WMI: Windows Management Instrumentation. A partíciók kezelésében játszik szerepet.

III.3 Actice Directory Domain Services

Fő célja a Windowst futtató számítógépek részére autentikációs és autorizációs szolgáltatások nyújtása, lehetővé téve a hálózat minden publikált erőforrásának (fájlok, megosztások, perifériák, kapcsolatok, adatbázisok, felhasználók, csoportok stb.) központosított adminisztrálását – vagy éppen a rendszergazdai jogosultságok delegálásával a decentralizált felügyeletét. Számos különböző erőforráshoz (megosztott mappák, nyomtatók, levelezés stb.) egyetlen felhasználónév/jelszó páros megadásával biztosít hozzáférést. Lehetőséget nyújt a rendszergazdák számára házirendek kiosztására, szoftverek és szoftverfrissítések telepítésére a szervezeten belül. Az Active Directory az információkat és beállításokat egy központi adatbázisban tárolja, a tartományvezérlő számítógépe(ke)n. Ennek az adatbázisnak a mérete egy kisvállalat néhány száz objektumától egy több ezer szervert üzemeltető nemzetközi vállalat sok millió objektumáig terjedhet.

Egy Active Directory-címtár legmagasabb szintje az erdő, ami egy vagy több bizalmi kapcsolatokkal összekötött tartományt (domain) magába foglaló egy vagy több fa összessége. A tartományokat DNS-beli névterük azonosítja. A címtár objektumait a Directory Information Tree adatbázisa tárolja, ami három partícióra bomlik, ezek: az objektumok tulajdonságait leíró sémapartíció, az erdő szerkezetét (tartományokat, fákat, helyeket) leíró konfigurációs partíció és a tartomány objektumait tartalmazó tartományi partíció.

Az Active Directory objektumokból épül fel. Ezek három fő kategória egyikébe tartoznak: erőforrások (például nyomtatók), szolgáltatások (például e-mail) és felhasználók (felhasználói fiókok, csoportok). Az AD információkat tárol ezekről az objektumokról, rendszerezi őket, szabályozza a hozzáférést és biztonsági beállításokat tárol; ezzel egyben központosítva a hálózatot. Egy objektumot egyértelműen azonosít megkülönböztetett neve (dn, distinguished

name), ami tulajdonképpen az objektum neve és a fában elfoglalt helye együttesen. Egy objektum megkülönböztetett neve változhat az objektum áthelyezésével, átnevezésével. Egy másik azonosító, ami viszont az objektum teljes élettartama alatt változatlan marad, az *objectGUID* attribútuma. Ez egy 128 bites, erdő-szinten garantáltan egyedi azonosító. Azt, hogy milyen típusú objektumok lehetnek az AD-ben, és ezek az objektumok hogyan viselkedhetnek, milyen információkat (attribútumokat vagy tulajdonságokat) tartalmazhatnak, a *séma* határozza meg.

Az Active Directory objektumait a Directory Information Tree adatbázisa tárolja, ebben egy többszintű keretrendszer foglal helyet. A struktúra legmagasabb szintjén foglal helyet az erdő. Az AD minden objektumának, azok attribútumainak és szabályainak gyűjteménye. Az azonos erdőben található tartományvezérlőkről elmondható, hogy közös sémán és konfigurációs partíción osztoznak, és a globális katalógusokról azonos információkat érnek el. Az erdőt egy vagy több, kétirányú és tranzitív bizalmi kapcsolat által összekötött fa alkotja. Egy-egy fában egy vagy több, konfigurációs és sémapartíciójukban megegyező tartomány lehet, amik egy tartományhierarchiát alkothatnak, melyben a szülő- és a gyermektartományok között automatikusan létrejövő, tranzitív kétirányú bizalmi kapcsolat van. Az azonos szintű tartományok között explicit bizalmi kapcsolatokat lehet létrehozni, ha szükséges. A tartományokat DNS-beli névterük azonosítja, és ez a tartományi hierarchiát is tükrözi (például a child.parent.root.com tartomány szülője a parent.root.com). A tartományban lévő objektumok szervezeti egységekbe *(Organizational Unit, OU)* rendezhetők. Fizikailag az Active Directory adatai egy vagy több egyenrangú tartományvezérlőn *(domain controller, DC)* tárolódnak.

Az Active Directory adatbázisa az alábbi három tárterületre vagy partícióra bomlik:

- Sémapartíció: az egész erdő számára meghatározza az objektumosztályokat: az objektumok létrehozásának és módosításának a szabályait, az objektumok lehetséges tulajdonságait (attribútumait). Az erdő minden tartományvezérlőjére replikálódik, ezért ún. vállalati partíció.

- Konfigurációs partíció: az egész erdő fizikai szerkezetét (például topológiáját) és beállításait határozza meg, beleértve a fákat, tartományokat, tartományi bizalmi kapcsolatokat és helyeket (sites, TCP/IP alhálózatok). Az erdő minden tartományvezérlőjére replikálódik, ezért ez is ún. vállalati partíció.

- Tartományi partíció: minden információt tárol az adott tartomány objektumairól. Kizárólag az adott tartomány tartományvezérlőire replikálódik.

- Részleges tartományi partíció – minden tartományi objektumot tartalmaz, de az objektumok tulajdonságainak csak részleges listájával.

A Windows Server 2008ban ez a szolgáltatás át lett nevezve Active Directory Domain Servicesre, mely bővült pár újdonsággal, amelyek a következők:

- Active Directory Recycle Bin

  Az Active Directory lomtárral könnyebben megőrizhetők és visszaállíthatók a véletlenül törölt Active Directory-objektumok, és ehhez nincs szükség az Active Directory adatainak biztonsági másolatokból történő visszaállítására, az Active Directory tartományi szolgáltatások vagy a tartományvezérlők újraindítására. Ha engedélyezve van a lomtár, megmarad az objektumok összes csatolt és nem csatolt értékű attribútuma
- Active Directory modul a Windows PowerShellhez

  Az Active Directory module for Windows PowerShell egy parancssori felület, amely használatával a rendszergazdák konfigurálhatják és diagnosztizálhatják a környezetükben működő Active Directory tartományszolgáltatásokat (AD DS) és Active Directory Lightweight Directory-szolgáltatásokat.
- Active Directory Administrative Center

  Az Active Directory felügyeleti központ segítségével a felhasználók és a hálózati rendszergazdák könnyebben kezelhetik az adatokat, és egy funkciókban gazdag felhasználói felületen végezhetik el az Active Directory objektumkezelési műveleteit.
- Active Directory Best Practices Analyzer

  A Best Practice Analyzer (BPA) egy olyan szoftver, amely előre meghatározott szempontok alapján teszteli SQL Serveres adattárházainkat, üzleti intelligencia rendszereinket. Ellenőrzi, hogy a szerverek beállításai, használata megfelel e az iparágban használt normáknak, s ha nem akkor javaslatot tesz változtatásokra.
- Active Directory Web Services

  AD DS és AD LDS címtár-szolgáltatási példányokhoz és Active Directory-pillanatképekhez webes szolgáltatási felületet nyújtó Windows-szolgáltatás.
- Authentication mechanism assurance

  A hitelesítési mechanizmust biztosító funkció csomagolja a bejelentkezési módszer típusával kapcsolatos információkat. Ezek segítségével történik a tartomány felhasználóinak hitelesítése az egyes felhasználók Kerberos-jogkivonatában.

- Offline domain join

  A tartományhoz való offline csatlakozás új folyamat, amelynek használatával a Windows® 7 vagy Windows Server 2008 R2 rendszerű számítógépek tartományhoz csatlakozhatnak. A tartományhoz való offline csatlakozás folyamata hálózati kapcsolat nélkül is képes elvégezni a tartományhoz való csatlakozás műveletét.

- Managed Service Accounts

  Managed service accounts are used to run various services for applications that are operating in your domain environment. This section contains topics that explain how to use the Active Directory module to accomplish many of the common tasks that are associated with service account management.

III.4 Read Only Domain Controllers

Bevezetésre került egy új tartományvezérlői üzemmód, az írásvédett vagy csak olvasható tartományvezérlőké (RODC). Ezt elsősorban a külső telephelyekre szánja a Microsoft, ahol nem érhető el a központéval megegyező szintű fizikai biztonság. A RODC az AD-nak (pontosabban az objektumok a sémában meghatározott attribútumainak) egy csak olvasható másolatát tartalmazza, bármilyen írási kísérletet egy teljes értékű tartományvezérlőre irányít át. A jelszavakat alapértelmezésben nem gyorsítótárazza, tervezési döntést igényel, hogy pontosan mely felhasználói fiókok jelszavát tárolhatja, hogy esetleges hálózati kimaradás esetén is be tudjanak jelentkezni a tartományba a távoli telephelyen.

A RODC tartományvezérlőkön – a megszokottól eltérően – helyi rendszergazdai fiók is található, ezzel rutin adminisztrációs feladatokat lehet végezni (hálózati kártya telepítése, partícionálás, stb.) a tartományhoz való rendszergazdai jogosultság nélkül.

A RODC üzemmód működéséhez szükséges, hogy egy Windows Server 2008-at futtató tartományvezérlőről szinkronizálja a központ adatait és, hogy az erdő működési szintje legalább Windows Server 2003-as legyen.

Azok a telephelyek ahová érdemes RODC-t telepíteni:

- Aránylag kevés felhasználó
- Gyenge fizikai biztonság
- Aránylag kisebb hálózati sávszélesség a központi telephely felé

- IT-ismeretek hiánya
- A telephelyen, a tartományvezérlőn kiszolgálói alkalmazást szeretnének futtatni

A RODC új funkciói:

- Írásvédett AD adatbázis
- Egyirányú replikáció
- A hitelesítő adatok gyorsítótárazása (amit engedélyezünk)
- Rendszergazdai szerepkör elkülönítése (helyi rendszergazda fiók)

III.5 Network Access Protection (NAP)

Egy nagyvállalathoz jellemzően rengeteg munkaállomás kapcsolódik, melyek lehetnek irodákba telepített számítógépek, laptopok, kéziszámítógépek. Ezeket az alkalmazottak otthon és a vállalaton belül, valamint nyilvános helyen egyaránt használják (VPN-n keresztül).
A védelem érdekében tehetünk biztonsági lépéseket, korlátozhatjuk a hálózatra kapcsolódó számítógépek fizikai (MAC) címeit statikus DCHP szolgáltatás alkalmazásával, ISA szerver segítségével szűrni lehet a hálózati forgalmat, házirend segítségével telepíthetünk vírusirtókat, korlátozhatjuk a hálózati portokat. Így viszont egyetlen nagy probléma vetődik fel, mi van olyankor, ha egy számítógép mely számára már engedélyeztük a hozzáférést, később veszélyforrássá válik. Feltételezzük, hogy egy hordozható számítógépet használó alkalmazott tartományi tag és mikor visszatér a munkába egy vírust hoz magával. Telepíthetünk a hálózati kliensekre víruskeresőket, de ezt az alkalmazott kikapcsolhatja. Az operációs rendszer számára fontos frissítések meglétét sem tudjuk vizsgálni. A fizikai cím korlátozása csak megköti a rendszergazdák kezét. Ilyen helyzetekre nyújt megoldást a Network Access Protection (NAP) szolgáltatás, amely segítségével a kliensek hozzáférését tudjuk szabályozni.

III.5.1 NAP főbb képességei

A Microsoft 5 kapcsolódási lehetőséget definiált, ahol a NAP képes vizsgálni a számítógépeket.
Ezek a területek a következők:
1. DHCP kiszolgálótól kért IP cím és további IP opciók
2. IEEE 802.1x - Vezetékes (Wired) és vezeték nélküli (Wireless) kapcsolódások
3. VPN alapú hálózati hozzáférés

4. RDP over HTTPS - Terminal Server Gateway szerepkörrel felépített terminál kapcsolat
5. HRA - IPSec alapú védett hálózati forgalom

NAP egy nagyon fontos rendszereleme az előírt egészségi állapot. Ez egy általunk sablonokból összeállítható szabálycsomag, melyben előírhatjuk például különböző programok jelenlétét a kapcsolódó gépen, programok speciális paramétereit, vagy akár a frissítések naprakészen tartását. A gyártó már a technológia korai stádiumától kezdődően azon dolgozott, hogy minél több hardver és szoftver gyártóval közösen kifejlesszen előre definiált szabály csomagokat (System Health Validators), melyeket az adott gyártó oldaláról letöltve és a rendszerbe importálva könnyedén használatba vehetünk. Jelenleg több mint 100 gyártó rendelkezik a NAP-hoz szükséges ellenőrző csomaggal (SHV), melyet a legtöbb esetben ingyenesen elérhetővé tettek. Ahhoz, hogy a kapcsolódó számítógép képes legyen fogadni az előírt egészségi állapot feltételéhez kötődő szabályokat, azokat saját magán le tudja ellenőrizni és az eredményt vissza tudja küldeni, szükséges egy kliens oldali ügynökalkalmazás.
A fent felsorolt 5 kapcsolódási területből négynél működik a karantén vezérlés (az RDP over HTTPS alapú kapcsolódásánál nincs karantén logika). Bár a karantén a kapcsolódó számítógép számára a belső hálózat védett erőforrásainak elérését nem engedélyezi, de biztosítja a szintre hozatalhoz szükséges szerverszerepek és erőforrások elérését. Korlátozhatjuk, hogy egy gép maximálisan mennyi időt tölthet el a karanténban, így ha záros határidőn belül nem képes magát megjavítani, akkor megszüntethetjük vele a kapcsolatot. Mindez persze akkor igazán érdekes, ha a javítási folyamat automatikusan történik.
És végül, de nem utolsó sorban, a rendszer képes folyamatosan figyelni a kapcsolódó gép egészségállapot változásait. Ez a gyakorlatban annyit jelent, ha a gép a számára előírt állapottól eltér, akkor automatizált folyamatok szerint azonnal kikerül a karantén hálózatba, ahonnan csak akkor kerülhet vissza a belső hálózatba, ha maximálisan teljesíti az előírt feltételeket.
A rendszer három fő kategóriára osztható:

- Áll egyrészt a kapcsolódó számítógépből, a rajta futó Network Access Protection Agent (napagent) szolgáltatásból, illetve az ehhez tartozó Enforcement Client (EC) komponensekből.

- Másrész a kliensek kapcsolódását fogadó komponensekből (5 különböző kapcsolódási terület).
- Harmadrészt pedig a háttér infrastruktúrából, ahol előírjuk az egészségi állapotot, azt publikáljuk az Active Directory-ba, és szükség esetén megjavíthatjuk a nem megfelelő szinten lévő számítógépet.

III.5.2 A kapcsolódó géppel szembeni elvárások

Fontos tudnunk, hogy nem minden operációs rendszer verzió támogatott a NAP-ban. Ez mindenképpen erősen lekorlátozza a lehetőségeinket. Meg kell oldanunk, hogy legyen *napagent* a gépen! Ha valaki Vista, vagy Windows 7 kliens operációs rendszerrel dolgozik, akkor nem lesz ezzel külön teendője, XP esetében azonban csak a Service Pack 3 csomag telepítésével kerül be ez a funkció. Szerver oldalon még korlátozottabbak a lehetőségek, mivel csak a Windows Server 2008 része az említett ügynök.

De hiába van fent az ügynök, mivel az alapértelmezett beállítás szerint az nem fut. Ennek viszonylag egyszerű az oka: a „Secure by Default" szemlélet szerint minden felesleges szolgáltatást ki kell kapcsolni. És mivel egyáltalán nem biztos, hogy be akarja mindenki alapértelmezettként vezetni a NAP-ot, ezért inkább kikapcsolták ezt a szolgáltatást. Ha azonban nem fut a szolgáltatás, akkor nem lesz semmilyen egészségállapot vizsgálat, így az ilyen gépek valószínűleg még a karanténba sem fognak bekerülni, a rendszer nem fog velük szóba állni.

Ahhoz, hogy az egészségállapot ellenőrzés folyamata rendkívül gyors legyen, minden ügynök a saját cache-ében tartja a gép aktuális állapotát, amit a kapcsolódáskor azonnal el is tud küldeni az ellenőrzést végző NPS kiszolgáló felé. Minden kapcsolódási területnek megvan a maga részterületi ügynöke, hiszen más-más formátumban kell küldeni az egészségi állapotot, illetve a karantén vezérlés logikája is máshogy működik. Itt csupán annyi a teendőnk, hogy bekapcsoljuk azt az EC komponenst, amelyen keresztül a kliensünk képes lesz kommunikálni az ellenőrzést végző szerverszereppel. Tehát, ha DHCP kiszolgálón keresztül kér a kliens IP címet, akkor a DHCP Quarantine Enforcement Client komponensre lesz szükségünk.

Természetesen Active Directoryval felügyelt rendszer esetében lehetőség van ezen beállítások házirenden keresztüli szabályozására is. Akár testreszabott üzenetek formájában tájékoztathatjuk a felhasználókat arról, hogy mit kell tenniük abban az esetben, ha az ellenőrzés szerint nem megfelelő a számítógépük. Ez főleg akkor igazán hasznos, ha egy

külsős felhasználó gépét kellene az előírt egészségi szintre hozni, de itt nem alkalmazható az automatikus javítás folyamata.

Talán a NAP platform legfőbb korlátját éppen az jelenti, hogy a külsősök gépére nem fog érvényre jutni az a házirend, ami bekapcsolná az említett komponenseket, és mivel a rendszernek nincs joga az automatikus javításhoz sem, ezért a felhasználó képességein múlik az, hogy megtud-e birkózni a különböző beállításokkal. Az is gondot okoz, ha a külsős felhasználó nem rendelkezik adminisztrációs jogokkal a gépén, mivel ebben az esetben nem állíthat szolgáltatásokat, nem telepíthet programokat. De ha esetleg ezek a jogosultságok adottak is, akkor hamar egy másik problémával találjuk szemben magunkat: előírtuk a Forefront Client Security programot, illetve annak definíciós frissítéseinek naprakészen tartását, de a kapcsolódó gépen nincs telepítve az alkalmazás. Ha ez egy vállalati számítógép, akkor egy központi szoftvertelepítési módszer alkalmazásával (pl.: SCCM) könnyedén orvosolhatjuk ezt a problémát. De mi a helyzet egy külsős gép esetén? Arra nem akarjuk feltelepíteni a vállalati alkalmazásainkat, hiszen ez licencelési problémákhoz vezetne. Így viszont nem tud kapcsolódni az ilyen számítógép a védett rendszerhez.

És ezzel el is érkeztünk a termék legfontosabb bevezetési korlátjához! Mivel ez a technológia nem képes kivételek kezelésére (de ennek nem is lenne túl sok értelme), ezért ha megfogalmazzuk az előírt egészségi állapot feltételrendszerét, illetve megadjuk, hogy mi legyen azokkal a gépekkel, melyek ezt nem teljesítik, akkor az minden a rendszerhez kapcsolódó gépre egységesen vonatkozni fog. A bevezetés előfeltételeként szükséges egy olyan felsővezetői szabályozás, hogy a külsős gépek nem érhetnek el védett, belső erőforrásokat. Tehát ki kell alakítani egy olyan hálózatot, ahol a külsős gépről csak például Internet hozzáférést biztosítunk.

III.5.3 A fogadó komponensek

A kliensek kapcsolódását fogadó komponensek nem közvetlenül döntenek arról, hogy a hozzáférést kérő gép állapota megfelelő-e vagy sem, ezt az információt az NPS kiszolgáló adja meg számukra. A fogadó komponensekkel kapcsolatos általános elvárás az, hogy mielőtt befogadnának egy hozzáférési kérést, továbbítsák a kliens egészségi állapotát az ellenőrzést végző NPS felé, aki azt visszaigazolva megmondja az adott kiszolgálónak, hogyan járjon el a kapcsolódó géppel szemben.

Az NPS három féle választ adhat:

- a kapcsolódó gépet fogadd be, helyezd őt a belső, védett hálózatba,
- a kapcsolódó gép nem teljesítette az előírt egészségi állapotot, ezért helyezd őt a karanténba,
- a kapcsolódó gép nem teljesítette az előírt egészségi állapotot, ezért utasítsd vissza a hozzáférési kérését.

Nézzük ezeket a komponenseket részletesebben:

III.5.4 DHCP szerver

A dhcp alapú kapcsolódáskor a kliens IP címet és további IP opciókat kér a DHCP kiszolgálótól. A Windows Server 2008 (és csak ez a verzió) felkészített a NAP technológia támogatására, így képes eltérő IP opciókat adni a nem megfelelő gépeknek. Ehhez szükség van a standard IP opciók mellé alternatív paramétereket is definiálni Scope, vagy akár szerver szinten.

Természetesen a kliensnek átadott IP cím nem változik a karanténból a belső hálózatba való bekerüléskor, vagy akár fordítva, mivel ez szakadást okozna a folyamatos kommunikációban, viszont a háttérben egy IPconfig /renew parancsnak megfelelő IP opciók megújításával járó folyamat zajlik le. Ennek eredményeképpen a kliens az állapotának megfelelő User Classhoz definiált opciókat fogja megkapni.

Bár látszólag bármilyen IP opciót definiálhatunk a NAP Classhoz is, de valójában korlátozott, hogy mit fog ténylegesen megkapni a kapcsolódó gép, például átadhatjuk a DNS szerver címét (006-os opció), vagy a DNS tartományi utótagot (015-ös paraméter), de az átjáró címét (003-as opció) nem fogja megkapni, ha nem teljesíti az előírt feltételeket. Tehát itt a karantén vezérlés az alternatív IP opciók kiadásával került megoldásra, ami csak akkor lesz igazán hasznos, ha a kliensek által elérhető hálózatot és a szerverinfrastruktúra hálózatát fizikailag is kettéválasztjuk egymástól. Ezzel el tudjuk rejteni a felhasználók elől a belső hálózatban használt névteret, a névfeloldásért felelős kiszolgálókat és egyéb fontosabb információkat.

III.5.5 IEEE 802.1x

Ebben a komponensben található a vezetékes és vezeték nélküli hálózati kapcsolódást fogadó eszközök halmaza. Ezeknek az eszközöknek képesnek kell lenniük a kliensektől érkező egészségi állapotot befogadni, és azt továbbítani az NPS kiszolgáló felé. Az NPS válaszának függvényében a kapcsolódó gépet vagy a rendes VLAN hálózatba, vagy egy izolált VLAN-ba kell helyezniük. Ez utóbbi a karantén vezérlés logikája. A kapcsolódó gép és az aktív eszköz között EAP (Extensible Authentication Protocol) vagy PEAP (Protected Extensible Authentication Protocol) alapú kommunikáció zajlik le. Ebből kiderül, hogy az eszközzel szemben is van elvárás: támogatnia kell a NAP technológiát. A Microsoft éppen emiatt kötött egy megállapodást a Ciscoval, hogy legalább egy gyártó legyen, aki az eszközeit felkészíti a NAP-pal való együttműködésre. Javasolt úgy konfigurálni az eszközt, hogy az izolált VLAN-ban legyen olyan szerverszerep, melyen keresztül a kliens képes magát megjavítani.

III.5.6 VPN

A VPN karantén vezérlés logikája nem új elem a Microsoft védelmi megoldásaiban, hiszen ennek az első verziója a Windows Server 2003 Routing and Remote Access szerverszerepben megtalálható volt. A működési folyamat gerince nem változott, viszont számos új képességgel bővült a kínálat. Ahhoz, hogy lássuk az új verzió előnyeit, meg kell ismernünk a korábbi megoldás képességeit.

Az előző verzióban nekünk kellett mindenféle ügyes ellenőrző scriptet és exe-t fejlesztetnünk, amiben leírtuk, hogy mit akarunk ellenőrizni. Bár a Microsoft készített ehhez néhány minta scriptet, de a valóságban igen komoly kihívást jelentett ilyen ellenőrző csomagokat készíteni. Az ellenőrzést végző scriptet közvetlenül a VPN kapcsolat felépítése után kellett lefuttatni, és záros határidőn belül (pl.: 1 perc) elküldeni a VPN gatewaynek. Ha ez nem történt meg, akkor a VPN Gateway a megadott idő elteltével bontotta a kapcsolatot a géppel. További probléma volt, ha a gép nem teljesítette az előírt feltételeket, mivel ilyenkor a felhasználónak kellett „megjavítania” a gépét. És végül a gép ellenőrzése csak a kapcsolat felépítésekor történt meg. Miután a gépet beengedtük a VPN hálózatba és a felhasználó úgy döntött, hogy kikapcsolja a gépén lévő tűzfalat, akkor már semmi nem vizsgálta a gépet, hogy még mindig teljesíti-e az előírt állapotot. Sajnos ezzel előállhatott az a helyzet, hogy egyik interfészével védtelenül és közvetlenül kint lógott az Interneten, míg a létrejött PPP adapterével pedig a belső hálózaton figyelt a gép.

A NAP-ban lévő VPN támogatás a fent leírt összes problémára megoldást ad. Könnyedén előírhatjuk az egészségi állapotot, amit a kapcsolódó kliensen lévő ügynök folyamatosan figyel. Ha tartományi gép kapcsolódik, akkor az automatikus javítás sem lehet probléma, és a kapcsolódás ideje alatt folyamatosan ellenőrzés alatt marad a kliens.

III.5.7 RDP over HTTPS

A terminál alapú kapcsolódás egy új megoldása a Windows Server 2008-ban megjelenő Terminal Server Gatewayen keresztül folytatott RDP over HTTPS kommunikáció. A megoldás lényege, hogy a felhasználó képes Interneten keresztül HTTPS-be ágyazott RDP protokollon keresztül elérni a vállalati szervereket. Ezzel a megközelítéssel a felhasználó ugyanazon a teljes értékű felületen dolgozhat vállalaton belül, mint bárhol máshol, hiszen a jól megszokott terminál kiszolgáló felületét éri el bárhonnan. A megoldás tovább kombinálható a szintén Windows Server 2008-al megjelenő RemoteApp alapú alkalmazások használatával is. Ilyenkor a felhasználó a terminál kiszolgálóra telepített alkalmazás paraméterezett RDP kapcsolati ikonját kapja meg a saját gépének asztalára, de amikor elindítja az alkalmazást, akkor a rendszer detektálja, hogy a vállalati hálózaton belül vagy kívül tartózkodik a számítógép. Ennek függvényében próbálkozik közvetlenül az RDP vagy a HTTPS-be ágyazott RDP hívással. Ahhoz, hogy ez a technológia használható legyen a kliens oldallal kapcsolatosan is van elvárás, mégpedig az RDP 6.1-es kliens program.
A NAP ebben az egy kapcsolódási területben nem képes karantén vezérlésre. Tehát megvizsgálhatjuk a kapcsolódó gép egészségi állapotát, azonban ha az nem teljesíti az előírt feltételeket, akkor itt nem létesül karantén hálózat, ahonnan képes megjavítani magát a gép.

III.5.8 HRA - IPSec védett hálózati kommunikáció

Talán a legbiztosabb védelmet ez a megoldás képes nyújtani a nem megfelelően konfigurált gépekkel szemben. A megfelelő rendszer felépítéséhez alkalmaznunk kell a domain izoláció fogalmát, melynek lényege, hogy a belső hálózatban futó szenzitív információkat tartalmazó kiszolgálónkhoz IPSec alapú szabályokat hozunk létre. Az IPSec alkalmazásával nem csupán a hálózati forgalom titkosítását és az adatintegritás védelmet nyerjük, de egyúttal azt is szabályozhatjuk, hogy csak azok a kliensek legyenek képesek kommunikálni a kiszolgálói rendszerrel, akik teljesítik az előírt egészségállapot feltételrendszert.
Az IPSec alapú kommunikációs csatorna kiépítésének első lépése a két fél kölcsönös hitelesítése. A hagyományos IPSec esetében a hitelesítéshez alkalmazható a megosztott titok

(preshared key), a Kerberos alapú jegyrendszer és a megbízható, CA által kibocsátott tanúsítvány. A NAP esetében viszont kicsit tekertek a fejlesztők az alap logikán. Itt mindkét félnek egy speciális OID (Object Identifier) mezővel ellátott tanúsítvány sablonból kiállított tanúsítványra van szüksége, amit nem igényelhetnek közvetlenül.
Ilyen tanúsítványt a Health Registration Authority (HRA) Windows Server 2008-as szerepkört ellátó kiszolgáló állít ki az előírt egészségi állapotot teljesítő gépek számára.
Ha egy gép nem teljesíti az előírt feltételeket, akkor nem kaphat ilyen tanúsítványt, ha pedig korábban teljesítette azt, de valamilyen oknál fogva menet közben attól elért, akkor a korábban kibocsátott tanúsítványt a kliensen futó NAP agent eldobja, ezzel megszakad a védett kiszolgálóval felépített IPSec csatorna.

III.6 Terminal Services

Hiába is keresünk a Windows Server 2008 R2-ben Terminal Services szolgáltatásokat. Nem tűntek el, csak átalakultak: a szolgáltatás új neve Remote Desktop Services (RDS). Nem azért lett átnevezve a termék, mert a régi név elkopott volna, hanem azért, mert a funkcionalitás lényegesen megváltozott, de a legfontosabb az, hogy számos új szolgáltatással is bővült. Már maga a névválasztás is utal a szolgáltatás új képességeire: olyan eszközök és funkciók kerültek bele, amelyek forradalmian értelmezik újra a munkaállomásokról távolról elérhető eszközöket, erőforrásokat.

Vegyük elő újra a felhasználói igényeket

A jó IT infrastruktúra és az általa nyújtott szolgáltatások elsősorban az üzleti igényeket elégítik ki, de ezzel összecsengő igény, vagyis szinte ugyanilyen fontos az is, hogy a felhasználói igényeket is a lehető legjobban ki tudjuk szolgálni. Melyek azok az igények, amelyek a leggyakrabban jelentkeznek akkor, amikor a felhasználók távolról is szeretnének dolgozni?

- Ugyanazt a funkcionalitású és minőségű munkakörnyezetet érhesse el, bármikor, bárhonnan is jelentkezik be.
- Bárhol jár is a vállalaton kívül, ugyanazokat az erőforrásokat érje el, mintha a saját asztalánál ülne.

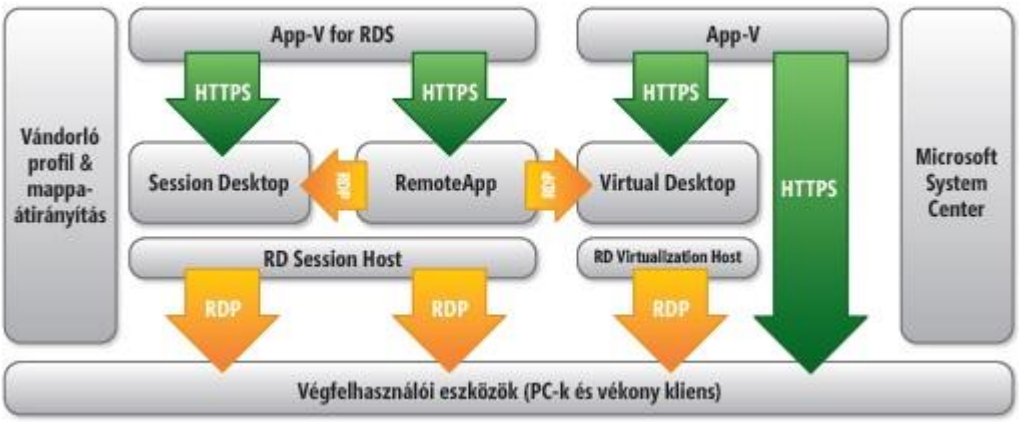
· A felhasználó eszközei meghibásodása miatt a lehető legkisebb kieséseket legyen kénytelen elviselni.

Ezeket az igényeket kielégíteni Terminal Server-rel nem igazán lehet. Ehhez ugyanis arra lenne szükség, hogy a felhasználó munkaállomásán és a Terminal Serveren is ugyanazok a környezeti beállítások, és ugyanolyan konfigurációjú alkalmazások legyenek elérhetők. Ez azért nem volt lehetséges, mert a Windows XP és Vista kliensek, illetve a Windows 2003 majd később annak R2-es változatának kernelverziói nem egyeztek meg. A Windows 7 és a Windows Server 2008 R2 változást, sőt szinergiát hoz ebbe a környezetbe: mivel kernelverzióik megegyeznek, ezért ugyanúgy kezelik a felhasználói környezet beállításait, egyformán telepítik és konfigurálják az alkalmazásokat.

Mire tudjuk felhasználni ezt a tulajdonságot? Mivel a Windows Server 2008 R2 át tudja venni a Windows 7 munkaállomástól a felhasználói munkakörnyezet megjelenítési és üzemeltetési feladatait, így a felhasználó függetleníthető a régi munkakörnyezetétől, így a munkaállomása állapotmentes lesz. Ez azt jelenti, hogy a felhasználó a munkája során létrehozott fájlok, környezeti beállítások nemcsak a munkaállomáson lesznek elérhetők, hanem valamilyen központi tárolón is, ahonnan bármikor elérhetők. Ezek az adatok rávehetők arra is, hogy nemcsak munkaállomáson, hanem RDS kiszolgálón is elérhetőek legyenek.

III.6.1 Architektúra

A régi Terminal Services szolgáltatásokat nyújtó és akár az állapotmentes munkaállomás-környezetet is megvalósító RDS rendszer több komponensből áll, amelyek egymással való viszonyát az alábbi ábra mutatja be.



Az ábrán látható, hogy a régi terminal services szolgáltatás (Session desktop) köré épültek az új szolgáltatások. A vándorló profil és a mappaátirányítások valósítják meg azt, hogy ugyanazok az adatok legyenek elérhetők RDS-en, mint Windows 7-en. A Session Desktop nyújtja a klasszikus terminal services szolgáltatást, amely a Windows Server 2008 R2 felületén biztosítja a felhasználó számára a munkavégzést. Funkcionalitása kiegészül azzal, hogy nemcsak a Session Desktopra telepített alkalmazások érhetők el, hanem a felhasználónak publikált virtuális alkalmazások is. A Virtual Desktop (VDI) Hyper-V környezeten futtatott virtuális operációs rendszer (Windows 7) konzoljához való hozzáférést biztosít. A VDI-on elérhetővé tehetők a profiladatok, az átirányított mappák tartalmai és a felhasználó számára publikált virtuális alkalmazások is. A RemoteApp feladata, hogy egy közös felületről (akár weben keresztül is) elérhetővé tegye azokat a virtuális alkalmazásokat, Session Desktop és VDI hozzáféréseket, amelyekhez a felhasználónak joga van. A teljes környezet működését, a virtuális alkalmazások és munkaállomások életciklusának kezelését a Microsoft System Center termékei, az Application Virtualization, a Virtual Machine Manager, Configurations Manager és az Operations Manager (rendszerfelügyelet) támogatják. A környezet RDP 7 protokollon keresztül érhető el, amelyet egyelőre csak a Windows 7 és a Windows Server 2008 R2 támogat.

RemoteApp and Desktop Connection

A Windows Server 2008-ban elérhető RemoteApp egy ablakban megjelenítette a felhasználó számára, hogy milyen alkalmazások érhetők el számára a Terminal Services szolgáltatás felől. A Windows Server 2008 R2-ben a RemoteApp neve kiegészült a Desktop Connections résszel is, ami az új funkcionalitását is definiálja. A RemoteApp ezentúl nemcsak az alkalmazásokat, hanem a felhasználó által elérhető hagyományos RDS és VDI alapú Remote Desktop eléréseket is megjeleníti. Windows 7-en ez a funkció be is épül a Start menübe, és a publikált alkalmazásokat és más kapcsolatokat onnan is (vagy akár az asztalra kihúzva is) el lehet indítani (hasonlóan az XP mód vagy a MED-V funkcionalitásához).

Connection Broker

A Connection Broker nem más, mint egy olyan szolgáltatás, amely a RemoteApp mögött áll, és a tőle jövő kéréseket elégíti ki. A szolgáltatás biztosítja, hogy a megszakadt kapcsolatok ismét helyreállhassanak, és ugyanonnan folytatható legyen a munka, ahol azelőtt abbamaradt.

Biztosít továbbá egyfajta terheléseloszlást is: ha a VDI, Session host esetleg további RemoteApp erőforrásokból több is áll rendelkezésre, akkor Network Load-Balancing szolgáltatás felhasználása nélkül gondoskodik arról, hogy mindig legyen szabad hozzáférhető erőforrás, és a kiszolgálók egyenletesen (vagy inkább beállításaink szerint) legyenek terhelve.

Gateway

A Gateway biztosítja azt, hogy a RemoteApp-on keresztül publikált alkalmazások, session vagy VDI kapcsolatok elérésekor a felhasználó csak ahhoz a belső erőforráshoz férjen hozzá, amelyet a választott szolgáltatás igényel. Ehhez egy biztonságos csatornát épít fel, amint RDP over HTTPS protokollon keresztül bonyolítja a kommunikációt az internet felől érkező felhasználó és az RDS szolgáltatás között.

Web Access

A Remote Desktop Web Access egy webes felület, amelyen keresztül publikálhatók a felhasználó által elérhető RDS szolgáltatások.

III.7 Windows PowerShell

A Windows PowerShell egy új, elsősorban rendszergazdák számára fejlesztett, feladatközpontú parancssor-rendszerhéj és parancsnyelv. A Windows PowerShell a Microsoft .NET-keretrendszerre épülve segítséget nyújt a számítástechnikai szakembereknek a Windows operációs rendszerek és az azokon futó alkalmazások felügyeletének szabályozásában és automatizálásában.
A Windows PowerShell a .NET-keretrendszer osztályainak egy bővíthető készletét használja, ami lehetővé teszi a fejlesztők számára, hogy egyéni parancsmagokat, szolgáltatókat, gazdaalkalmazásokat és eszközöket hozzanak létre.
A beépített Windows PowerShell-parancsok (parancsmagok) lehetővé teszik, hogy a parancssorból kezelje a vállalat számítógépeit. A Windows PowerShell szolgáltatói a fájlrendszerben való navigáláshoz hasonlóan egyszerű hozzáférést biztosítanak az adattárolókhoz (például a beállításjegyzékhez és a tanúsítványtárolókhoz). A Windows

PowerShell ezenfelül gazdag kifejezéselemzővel és egy teljes körű parancsnyelvvel rendelkezik.

III.7.1 Új funkciók IT-szakemberek számára

A Windows PowerShell 2.0 jelentős teljesítménynövelő fejlesztésekkel és új funkciókkal bővült.

- Több mint 200 parancsmag segíti a leggyakoribb rendszerfelügyeleti feladatok elvégzését.
- A Windows PowerShell távfelügyelete. Távoli parancsokat küldhet egy vagy több számítógépnek, vagy kapcsolatot létesíthet egy vagy több kiszolgálóval annak érdekében, hogy távoli parancsokat fogadhasson több számítógéptől a WS-Management protokoll használatával.
- A Windows PowerShell integrált parancsfájlkezelési környezet (ISE) egy gazdaalkalmazás, amely parancsok futtatásához és parancsfájlok tervezéséhez, írásához, teszteléséhez és hibakereséséhez biztosít Unicode-alapú környezetet. A Windows PowerShell ISE színkódolt szintaxist használ.
- A háttérfeladatok támogatása.
- Parancsmagalapú hibakereső a parancsfájlok és függvények hibáinak keresésére.
- Windows PowerShell-modulok, amelyek lehetővé teszik a Windows PowerShell-parancsfájlok független, minden szükséges fájlt tartalmazó és szabadon terjeszthető egységekbe történő felosztását és rendszerezését.
- Tranzakciók támogatása, biztosítva a mindent-vagy-semmit típusú műveletsorozatok teljes mértékű visszavonhatóságát.
- Új esemény-infrastruktúra, amely lehetővé teszi a felügyeletre és a rendszereseményekre való feliratkozást, majd az események figyelését, továbbítását és a megfelelő művelet végrehajtását, szinkron és aszinkron módon egyaránt.
- Speciális függvények, amelyek segítségével a parancsmagokhoz hasonló függvények írhatók a Windows PowerShell parancsfájlnyelvén.
- Adatszakaszok használatával az adatokat tartalmazó részek elkülöníthetők a parancsfájllogikától.

- A parancsfájlok nemzetközivé tételére szolgáló funkciók, melyek lehetővé teszik, hogy a parancsfájlok és függvények üzenetei és súgószövege több nyelven is megjeleníthető legyenek.
- Teljes körű súgófunkciók, köztük az új online segítségkérési lehetőség.

III.7.2 Új szolgáltatások a fejlesztőknek

A Windows PowerShell 2.0 a következő új szolgáltatásokkal segíti a fejlesztők munkáját:

- Tranzakciókban használható parancsmagok és szolgáltatók írása. További információ a tranzakciók támogatásáról a parancsmagokban: a TransactionAvailable metódus. További információ a tranzakciók támogatásáról a szolgáltatókban: a ProviderCapabilities felsorolás.
- Az objektumok kibővíthetők a Windows PowerShell által kezelhető eseményekkel. További információ: a PSEvent osztály.
- Modulok és moduljegyzékfájlok írása, ami önálló, szabadon terjeszthető Windows PowerShell-megoldások létrehozását teszi lehetővé.
- Hatékonyabb gazdaalkalmazások írhatók a PowerShell osztály használatával. Ez az osztály lehetővé teszi a parancsfutószalag (command pipeline) létrehozását, a futószalag meghívására használt futtatótér meghívását, illetve a futószalag szinkron vagy aszinkron meghívását.
- Olyan gazdaalkalmazások írhatók, amelyek futtatótereket nyitnak meg távoli számítógépeken.
- Olyan gazdaalkalmazásokat írhat, amelyek közös konfigurációt használó futtatóterek készletét hozzák létre. További információ: az CreateRunspacePool metódus.
- Korlátozott futtatótereket hozhat létre a futtatótérben futtatható elemek korlátozására.

III.8 Bitlocker meghajtótitkosítás

Windows Server 2008 rendszerben elérhető adatvédelmi szolgáltatás. Az adatlopás és az elveszett, ellopott vagy a használatból nem megfelelően kivont számítógépek veszélyeire kínál megoldást. Az elveszett vagy ellopott számítógépeken található adatok esetében fennáll a jogosulatlan hozzáférés veszélye, akár szoftveres támadás, akár a számítógép merevlemezének más számítógépre való átmásolása útján. A BitLocker a fájl- és rendszervédelmének fokozásával mérsékli a jogosulatlan adathozzáférés kockázatát. Segíti az

adatok végleges megsemmisítését is a BitLocker-védelemmel ellátott számítógépek használatból való kivonásakor vagy újrahasznosításakor.
Két fő adatvédelmi eljárást alkalmaz:

- A merevlemezen található teljes Windows operációsrendszer-kötet titkosítása.
- A korai rendszerindítási összetevők és a rendszerindítási konfigurációs adatok sértetlenségének biztosítása.

Ezenkívül zárolható a normál indítási folyamat mindaddig, amíg a felhasználó meg nem ad egy személyes azonosítószámot (PIN), vagy be nem helyez egy indítókulcsot tartalmazó cserélhető USB-eszközt, például egy flash meghajtót. Ezek a kiegészítő biztonsági intézkedések többszörös hitelesítést biztosítanak, és garantálják, hogy a számítógép a helyes PIN-kód vagy indítókulcs nélkül nem indítható el, illetve hibernált állapotból nem oldható fel.
A BitLocker az alábbi módokon segíti az adatvédelmet a rendszer offline állapotában:

- A teljes Windows operációsrendszer-kötet titkosítása, beleértve a felhasználói adatokat és a rendszerfájlokat, továbbá a hibernálási fájlt, a lapozófájlt és az ideiglenes fájlokat.
- Átfogó védelem a nem a Microsofttól származó alkalmazások számára, melyek a titkosított kötetre való telepítés után automatikusan élvezhetik ennek előnyeit.

A BitLocker a TPM segítségével ellenőrzi a korai rendszerindítási összetevők sértetlenségét és a rendszerindítási konfigurációs adatokat. Ily módon csak abban az esetben teszi hozzáférhetővé a titkosított kötetet, ha ezeket az összetevőket nem manipulálták, és a titkosított meghajtó az eredeti számítógépben található.
A BitLocker az alábbi módokon segíti elő a rendszerindítási folyamat sértetlenségét:

- A korai rendszerindítási fájlok sértetlenségének megőrzésére alkalmas módszert kínál, és biztosítja, hogy ezeket a fájlokat ne módosítsák ártó szándékkal, például a rendszerindító szektorba beépülő vírusokkal vagy betörést álcázó programcsomagokkal (rootkitekkel).
- Hatékonyabbá teszi az offline szoftveralapú támadások elleni védelmet. A rendszerindításra alkalmas egyéb szoftverek nem férnek hozzá a Windows operációsrendszer-kötet visszafejtő kulcsaihoz.

- Manipuláció észlelése esetén zárolja a rendszert. Ha bármelyik megfigyelés alatt tartott fájlt módosítják, a rendszer nem indul el. Ez felhívja a felhasználó figyelmét a módosítás tényére, hiszen a rendszer nem a szokott módon indul el. A rendszer zárolása esetén egyszerű helyreállítási folyamatot kínál.

III.8.1 Biztonsági szempontok

Mivel a biztonsági folyamatok a kockázatkezelés témaköréhez tartoznak, fontos megjegyezni, hogy a BitLocker nem tudja megvédeni a számítógépet minden lehetséges támadástól. Ha rosszindulatú felhasználók vagy programok, például vírusok vagy betörést álcázó programcsomagok (rootkitek), hozzáférnek a számítógéphez annak elvesztése vagy ellopása előtt, olyan gyenge pontokat építhetnek a rendszerbe, melyek révén később titkosított adatokat is elérhetnek. A BitLocker-védelem akkor is kevésbé hatékony, ha az USB-indítókulcsot a számítógépben hagyják, illetve ha a PIN-kódot vagy a Windows bejelentkezési jelszót nem tartják megfelelően titokban.

A legcsekélyebb felhasználói beavatkozást igénylő módszer a kizárólag TPM útján megvalósuló hitelesítési mód (vagyis ha nincs indítókulcs és PIN-kód), ami olyan szervezetek számára ideális, amelyek biztonsági házirendjének teljesítéséhez alapszintű adatvédelem is elegendő. A csak TPM útján megvalósuló hitelesítést a legegyszerűbb telepíteni, kezelni és használni. Olyan számítógépek esetén is ideális megoldás, amelyek felügyelet nélkül működnek, vagy felügyelet nélküli használat során igényelnek újraindítást.

III.9 Windows System Resource Manager

A Windows rendszererőforrás-kezelő eszköz a kiszolgáló processzorát és memóriahasználatát a szokásos vagy egyéni erőforrás-házirendek alkalmazásával kezelheti. Az erőforrások kezelése biztosítja az erőforrások egyenlő elosztását az egyetlen kiszolgáló által nyújtott összes szolgáltatás között, illetve folyamatosan hozzáférhetővé teszi a magas prioritású alkalmazások, szolgáltatások vagy felhasználók számára a megfelelő erőforrásokat.

A Windows rendszererőforrás-kezelő csak akkor kezeli a processzor erőforrásait, ha a kombinált processzorterhelés nagyobb mint 70%. Ez azt jelenti, hogy az eszköz aktívan nem korlátozza az egyes ügyfelek részére rendelkezésre álló erőforrásokat, ha a processzor

terhelése alacsony. Ha a processzor-erőforrás iránti igény versengést okozna, az erőforrás-elosztási házirendek gondoskodnak a minimális erőforrás-elérhetőség biztosításáról a meghatározott kezelési profil alapján.

III.9.1 A Windows rendszererőforrás-kezelő szolgáltatásai

A Windows rendszererőforrás-kezelő az alábbi célokra használható:

- Rendszererőforrások kezelése (processzor és memória) előre meghatározott házirendek alapján, illetve egyéni házirendek létrehozása, amelyek folyamat, felhasználó, Remote Desktop Services munkamenet vagy IIS-alkalmazáskészlet szerint osztják el az erőforrásokat.
- Naptári szabályok alkalmazásával különböző időpontokban eltérő házirendek használhatók, manuális beavatkozás vagy újrakonfigurálás nélkül.
- Az erőforrás-házirend automatikus kiválasztása a kiszolgáló tulajdonságai és eseményei (például fürtesemények vagy állapotok), illetve a telepített fizikai memória vagy a processzorok száma alapján.
- Erőforrás-használati adatok gyűjtése helyben vagy egy egyéni SQL-adatbázisban. Több kiszolgáló erőforrásainak használati adatai is feldolgozhatók egyetlen Windows rendszererőforrás-kezelőt futtató számítógépen.
- Számítógépcsoportok létrehozásával a kezelni kívánt távoli asztali kiszolgálók rendszerezésének megkönnyítésére. A házirendek könnyen exportálhatók vagy módosíthatók egy teljes számítógépcsoport esetében is.

III.9.2 Az erőforrás-kezelés által kínált előnyök

Mivel a Windows Server 2008 rendszert úgy tervezték, hogy a nem operációs rendszerrel kapcsolatos feladatok számára a lehető legtöbb erőforrást biztosítsa, az egyetlen szerepkört betöltő kiszolgálók általában nem igényelnek erőforrás-kezelést. Ugyanakkor, ha egy kiszolgálón több alkalmazás és szolgáltatás is fut, azok nem kapnak információt a velük versengő folyamatokról. Egy rendszererőforrás-kezeléssel nem szabályozott alkalmazás vagy szolgáltatás tipikusan az összes rendelkezésre álló erőforrást felhasználja a feladat elvégzéséhez. Emiatt a többcélú kiszolgálókon igen fontos a Windows rendszererőforrás-kezelő vagy hasonló eszköz használata. A Windows rendszererőforrás-kezelő használata az alábbi kulcsfontosságú előnyöket biztosítja:

- Egy kiszolgálón több szolgáltatás futhat, mert a szolgáltatások rendelkezésre állása javítható az erőforrások dinamikus kezelésével.
- A magas prioritású felhasználók vagy rendszergazdák még maximális erőforrás-terhelés esetén is hozzáférhetnek a rendszerhez.

III.10 Secure Socket Tunelling Protocol

Az SSTP az alkalmazási rétegben működő protokoll, tipikusan két program közötti kommunikációra felkészítve – ugyanakkor egy hálózati kapcsolaton belül akár többre is (gyakorlatilag a teljes hálózatban), tehát jobban képes kihasználni a sávszélességet. A virtuális magánhálózati (VPN-) alagút egy új formája. Olyan szolgáltatásokat kínál, amelyek lehetővé teszik, hogy a forgalom áthaladjon tűzfalakon, amelyek blokkolják a PPTP- és L2TP/IPsec-forgalmat. Az SSTP a PPP-forgalom beágyazásához nyújt mechanizmust a HTTPS protokoll SSL-csatornáján keresztül. A PPP használata erős hitelesítési módszerek, például az EAP-TLS módszer használatát teszi lehetővé. A HTTPS használata azt jelenti, hogy a forgalom a 443-as TCP porton keresztül halad át, amely portot általánosan a web eléréséhez használják. A Secure Sockets Layer (SSL) a szállítási szinten nyújt biztonsági szolgáltatásokat kibővített kulcsegyeztetéssel, titkosítással és a sértetlenség ellenőrzéssel. Az SSTP nem támogatja a oldalról-oldalra kommunikációt, csakis a távoli hozzáférést. Támogatja az IPv6-ot .

III.11 Windows Advanced Firewall

A Windows Firewall az Advanced Security MMC beépülő modullal leváltja a korábbi IPsec beépülő modulokat, az IP-biztonsági házirendeket és az IP-biztonsági felügyeletet a Windows Vista és Windows Server 2008 rendszereket futtató számítógépeken. Ugyan ezek a számítógépek beállíthatók és felügyelhetők a korábbi IPSec beépülő modulokkal, a régebbi eszközökkel sok olyan új szolgáltatást és biztonsági beállítást nem lehet konfigurálni, amelyek a Windows Vista és Windows Server 2008 rendszerekben jelentek meg.

III.11.1 Mire szolgál a Fokozott biztonságú Windows tűzfal?

A Windows Advanced Firewall számos szolgáltatást biztosít a Windows Server 2008 rendszert futtató számítógépeken:

- Az összes, a számítógépbe belépő vagy azt elhagyó IPv4- és IPv6-forgalom szűrése. A tűzfal alapértelmezés szerint blokkolja a bejövő forgalmat, kivéve, ha az egy korábbi, az állomás kezdeményezte kérésre adott válasz (kért forgalom), vagy külön engedélyezve van egy olyan tűzfalszabály által, amely engedélyezi a forgalmat. Alapértelmezésben minden kimenő forgalom engedélyezett, leszámítva azokat a szolgáltatáskorlátozó szabályokat, amelyek megakadályozzák, hogy a szabványos szolgáltatások nem várt módon kommunikáljanak.
- Védhető a számítógépbe belépő és abból kilépő hálózati forgalom az IPsec protokoll révén, a hálózati forgalom sértetlenségének ellenőrzésével, a küldő és fogadó számítógépek vagy felhasználók azonosságának hitelesítésével, és a titkosság érdekében a forgalom választható titkosításával.

A Windows Advanced Firewall két olyan funkciót hangol össze, amelyek a Windows korábbi verzióiban külön voltak kezelve. Továbbá a tűzfal- és Ipsec-összetevőinek alapszolgáltatásai is jelentősen megváltoztak a Windows Vista és Windows Server 2008 rendszerekben.

III.12 Policy-based Quality of Service

A házirend alapú Quality of Service (QoS) komponens alapértelmezés szerint része a Windows Server 2008-nak. Segítségével egyszerűen megoldható a Windows Server 2008 vagy Vista-kliensek esetén az alkalmazások sávszélesség- szabályozása. Az összes beállítás és e beállítások terjesztése is a Csoportházirend segítségével történik. Ennek a módszernek számtalan előnye van, a központi üzemeltetéstől kezdve egészen a megfelelő gépek, gépcsoportok, telephelyek, tartományok, felhasználók és csoportjaik kiválasztásáig. Külön előnynek számít, hogy mivel a korlátozás az alkalmazási rétegben történik, a meglévő alkalmazásokat semmilyen módon nem kell megváltoztatni vagy frissíteni ahhoz, hogy ezt a technológiát igénybe vehessük. Képzeljük el, hogy egy telephelyes környezetben a telephelyi kliensek rendszeresen, időzítve mentik a rendszerállapotot a központi szerverre, ezzel szépen „eldugítják” a WANkapcsolatot, amely aztán rendszeresen fennakadásokat okoz az egyéb hálózati forgalomban, ezért aztán szükségesé válik egy QoS-házirend bevezetése. Szerencsére a közbülső hálózati eszközök ismerik a DSCP-t , azaz a prioritásszabályozást konfigurálhatjuk ezeken az eszközökön is. Ez azért fontos, mert ha elindítjuk a QoS-varázslót, akkor a legelső

panelen rögtön láthatjuk, hogy a konkrét sávszélességértéken kívül a DSCP értéket is szabályozhatjuk. Nos, mivel esetleg számtalan QoS-házirendünk is lehet, ezek között valahogyan fel kell állítanunk egy sorrendet, és ezt a hálózati eszközökkel is közölni kell. A DSCP alapján erre egy 0-tól 63-ig terjedő sávunk van, azaz minél magasabb értéket választunk, annál erősebb lesz az adott házirend. Miután ezzel végeztünk, sorban következik a korlátozandó alkalmazások megnevezése – de akár arra is van lehetőség, hogy az összes alkalmazásra nézve kötelezőnek állítsuk be a házirendet, a forrás és az esetleges cél IP-tartományok (IPv6 is lehet), illetve a protokollok és portok megadásával. Több teendőnk nem is lesz, a házirend a Csoportházirend frissítési ciklusának megfelelően érvényre jut.

III.13 Windows Internet Name Service (WINS)

A Windows Internet Name Service (WINS) a számítógépnevek regisztrációját és feloldását végző szolgáltatás, amely a számítógépek NetBIOS-nevét és IP-címét egymáshoz rendeli. Ha WINS-kiszolgálókat telepít a hálózatára, a végfelhasználók a hálózati erőforrásokat a nehezen megjegyezhető IP-címek helyett nevek megadásával is elérhetik. Emellett a számítógépeken és más eszközökön futó alkalmazások és egyéb szolgáltatások az IP-címek névfeloldására vonatkozó kéréseket küldhetnek a WINS-kiszolgáló felé.

III.13.1 A WINS-kiszolgálók által nyújtott szolgáltatások

A WINS használata a TCP/IP-alapú hálózatok felügyelete során az alábbi előnyökkel jár:

- A számítógépek névregisztrációjának és névfeloldásának támogatását biztosító dinamikus név-cím adatbázis.
- A név-cím adatbázis központi kezelése, mely megkönnyíti az Lmhosts fájlok kezelését.
- Csökkenti az alhálózatok NetBIOS-alapú szórásos forgalmát azáltal, hogy lehetővé teszi, hogy a távoli rendszerek közvetlen keresése érdekében az ügyfelek WINS-kiszolgálókat kérdezhessenek le.
- A hálózat korábbi Microsoft® Windows®- és NetBIOS-alapú ügyfeleit is támogatja, és lehetővé teszi, hogy az ilyen típusú ügyfelek távoli Windows-tartományok listáit

böngésszék anélkül, hogy minden alhálózaton szükség lenne helyi tartományvezérlők jelenlétére.

- A szolgáltatás támogatást nyújt a DNS-alapú ügyfeleknek, melynek köszönhetően azok megkereshetik a NetBIOS-erőforrásokat a WINS-alapú keresés integrálásának bevezetésekor.

III.13.2 A WINS-kiszolgáló összetevői

A WINS két fő összetevője a WINS-kiszolgálók és a WINS-ügyfelek. Néhány konfiguráció WINS-proxykat is alkalmaz.

A WINS-kiszolgálók kezelik a WINS-ügyfelek regisztrációs kéréseit, regisztrálják a neveket és az IP-címeket, és azzal válaszolnak az ügyfelek NetBIOS-névlekérdezéseire, hogy visszaküldik az ügyfélnek a lekérdezett név IP-címét, ha az megtalálható a kiszolgáló-adatbázisban. A WINS-kiszolgálókat úgy is konfigurálhatja, hogy az adatbázisainak (amelyek tartalmazzák a NetBIOS-számítógépnevek IP-címekre való leképezését) tartalmát más WINS-kiszolgálókra replikálja. Ha egy WINS-ügyfél (például egy munkaállomás) először indul el a hálózaton, a számítógépnévnek és az IP-címnek az elsődlegesként beállított WINS-kiszolgálóra regisztrációs kérésként történő küldése közvetlenül történik. Mivel a kiszolgáló regisztrálja ezeket az ügyfeleket, ezért az adatbázisban szereplő ügyfélrekordok tulajdonosának is tekinthető.

A WINS-adatbázis tárolja a hálózat NetBIOS nevek és IP-címek közötti leképezéseit. Ha a WINS-kiszolgálókat azon replikációs partnerekkel konfigurálja, melyekre az adatbázis tartalmát „áthelyezi”, a helyi kiszolgálón található adatbázis tartalma replikálódik a replikációs partner kiszolgálójára. Ha a replikációs partnerek „lehívásra” vannak konfigurálva, akkor a távoli WINS-kiszolgálón található rekordokat a rendszer a helyi adatbázisba másolja. A WINS Microsoft Management Console (MMC) segédprogramban a WINS beépülő modul, más néven WINS konzol használatával állítható be, hogy a replikációs események milyen időközönként következzenek be.

A WINS konzol emellett a WINS-adatbázis kezeléséhez, megtekintéséhez, biztonsági mentéséhez és visszaállításához szükséges eszközöket is biztosítja. Készítsen biztonsági másolatot az adatbázisról minden alkalommal, amikor a WINS-kiszolgálón a többi fájlról biztonsági másolatot készít.

Hálózat indításakor vagy ahhoz történő csatlakozáskor a WINS-ügyfelek megkísérlik regisztrálni nevüket a WINS-kiszolgálón. Az ügyfelek ezután – ha szükséges – távoli nevek feloldására vonatkozó kéréseket küldhetnek a WINS-kiszolgálónak.

A WINS működését engedélyező ügyfelek olyan számítógépek, melyeket a WINS-kiszolgálók közvetlen használatára konfiguráltak. A legtöbb WINS-ügyfél több NetBIOS-névvel rendelkezik, melyeket a hálózaton való használathoz regisztrálni kell. Ezek a nevek különféle típusú hálózati szolgáltatások közzétételéhez szükségesek, mint amilyenek például a Messenger vagy a Munkaállomás szolgáltatás, melyeket az egyes számítógépek a hálózaton belüli más számítógépekkel való kommunikáció során használhatnak.

A WINS-proxyk olyan WINS-ügyfélszámítógépek, melyek más, a WINS szolgáltatás közvetlen használatára nem képes számítógépek helyett végeznek műveleteket. A WINS-proxyk segítenek az útválasztásos, TCP/IP-alapú hálózatokon található számítógépekről érkező NetBIOS-névfeloldási kérelmek megválaszolásában.

A legtöbb számítógép alapértelmezés szerint a NetBIOS-névfeloldási kérelmek megválaszolására, valamint NetBIOS-nevük regisztrálására nem tudja a WINS-szórást használni. A WINS-proxyk beállíthatók úgy, hogy ezek helyett a számítógépek helyett figyeljen, és hogy a szórás által fel nem oldott neveket lekérdezze egy WINS-kiszolgálóról.

A WINS-proxyk csak az olyan hálózatok esetén hasznosak vagy szükségesek, melyek csak NetBIOS-szórású (vagy b-csomópontú) ügyfeleket is tartalmaznak. A legtöbb hálózaton a WINS használatát engedélyező ügyfelek fordulnak elő, így a WINS-proxykra általában nincs szükség.

A WINS-proxyk figyelik a b-csomópontú NetBIOS-névszolgáltatás funkcióit (név regisztrálása, feloldása és lekérdezése), és képesek válaszolni a távoli és a helyi hálózaton nem használt nevek esetén. A proxyk a helyi szórásokra való válaszadáshoz szükséges adatok megszerzése érdekében közvetlenül a WINS-kiszolgálókkal kommunikálnak.

IV. Összefoglalás

A Windows Server 2008, ahogy a fenti részekben taglaltam manapság a legkorszerűbb, megbízhatóbb és legjobb választás, ha szervergépekre akarunk operációs rendszert választani. Bár később napvilágra került néhány hiányossága, ahol támadható, de a fejlesztők az R2 érkezésére kijavították ezen hibák nagy részét, gondolok itt például az SMB támadhatóságára. Fontos tudnunk továbbá, hogy kliens oldalon nem támogat minden operációs rendszert, ha nem Microsoft termékről van szó már nehezebb egy Windows Server 2008at futtató szerverre felcsatlakoznunk, ráadásul néha az egyszerű felhasználónak meggyűlhet a baja a NAP-pal is, hiszen ha nem elég „egészséges" a számítógépe, nem biztos, hogy meg tudja oldani, hogy kikerüljön a karantén zónából. A Hyper-V nagy segítség a hálózat tervezésében a rendszergazdák számára, az Active Directory új hasznos kiegészítőkkel bővült a felhasználók könnyebb csoportosítása érdekében. A Server Core telepítési opció egy nagyon jó megoldás a szervergép támadhatatlanságának növelésére. Ezen kívül a megerősített tűzfal és a meghajtó titkosítás is segítségünkre van.

Remélem, hogy dolgozatom felkeltette pár érdeklődő figyelmét, és elég információhoz jutottak elolvasása után ahhoz, hogy e termék mellett döntsenek.

V. Irodalomjegyzék

Elektronikus könyvek:

Microsoft.Press.Windows.Server.2008.Networking.and.Network.Access.Protection.NAP.Jan.2008.pdf

Microsoft.Press.Windows.Server.2008.Security.Resource.Kit.Mar.2008.pdf

Sams.Windows.Server.2008.Unleashed.Feb.2008.pdf

Internet linkek:

http://www.microsoft.com/hun/windowsserver2008/prodinfo/editions/editions-overview.aspx

http://www.humansoft.hu/pages/template1.aspx?1=1&id=1661423&type=48

http://www.microsoft.com/hun/windowsserver2008/prodinfo/technologies/active-directory.aspx

https://www.hungassist.hungarnet.hu/mediawiki/index.php/%C3%8Dr%C3%A1sv%C3%A9dett_tartom%C3%A1nyvez%C3%A9rl%C5%91_%E2%80%93_RODC

http://technet.microsoft.com/en-us/library/cc753208(WS.10).aspx

http://www.brianmadden.com/blogs/gabeknuth/archive/2008/03/11/microsoft-windows-server-2008-hyper-v-solution-overview.aspx

http://technet.microsoft.com/en-us/network/bb545879.aspx

http://www.calsoftlabs.com/whitepapers/network-access-protection.html

http://www.interop.com/archive/pdfs/MSNAP.pdf

http://msdn.microsoft.com/en-us/library/cc768520.aspx

http://www.microsoft.com/hun/technet/article/?id=a2635af1-4bd9-412b-8240-18968b3771d3

http://technet.microsoft.com/en-us/windows/aa905065.aspx

http://technet.microsoft.com/en-us/library/cc771290%28WS.10%29.aspx

http://licenseport.helpserve.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=206

http://technet.microsoft.com/en-us/library/bb978526.aspx

http://technet.microsoft.com/en-us/library/bb978525.aspx

http://technet.microsoft.com/en-us/library/cc731400%28WS.10%29.aspx

http://technet.microsoft.com/en-us/library/cc772589(WS.10).aspx

VI. Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek Dr. Krausz Tamásnak a szakmai instrukciókért, valamint a könyvekért, amelyeket biztosított a számomra, hogy minden eszközöm meglegyen, egy tartalmas, lényegre törő szakdolgozat írásában.