Debreceni Egyetem

Informatikai Kar

A WINDOWS SERVER 2003 HÁLÓZATI MEGOLDÁSAI

Témavezető:

Dr. Krausz Tamás

Egyetemi adjunktus

Készítette:

Bíró Zoltán

Programtervező informatikus

Debrecen

2008

Tartalomjegyzék

1. Bevezetés

A számítógépes hálózatok megjelenésének kezdetén, azokat elsősorban egyetemi kutatók használták elektronikus levelek elküldésére, valamint hivatali alkalmazottak nyomtatók megosztására. A biztonsági kérdésekre ekkor még nem sok figyelmet fordítottak.

Aztán néhány évvel ezelőtt, amikor kifejlődött a világméretű hálózat, az Internet, egyre több, nem csak hozzáértő ember kezdte el azt használni, elsősorban a sokféle új szolgáltatása miatt. Így a hálózatra kapcsolt gépek száma exponenciálisan növekedett.

Manapság, amikor már a hétköznapi emberek milliói használják a hálózat nyújtotta szolgáltatásokat, például banki műveletek közben, vásárláshoz, elektronikus levelezéshez, a hálózati biztonság kérdése komoly problémaként fogalmazódik meg. A legtöbb biztonsági problémát szándékosan okozzák a rosszindulatú emberek azzal a céllal, hogy előnyhöz juthassanak, vagy kárt okozzanak másoknak.

Ezért is döntöttem úgy, hogy dolgozatomban a Windows Server 2003 hálózati szolgáltatásait bemutatva különösen nagy figyelmet fordítok a biztonságra, és megpróbáltam a különböző szolgáltatások közül azokra fókuszálni, amelyek segítségével nagymértékben növelhető a rendszer és a hálózat biztonsága.

A Windows 2000 szerver operációs rendszer jelentős szerepet kapott a legmagasabb követelményeket támasztó üzleti és kormányzati informatikai környezetekben, egyértelműen az első helyre lépett a kiszolgáló operációs rendszerek sorában. 2001-ben például már a világszerte eladott kiszolgálók több, mint 60 százalékát a Windows Server-család rendszereivel szállították. Ez egyértelmű növekedést jelentett a korábbi évek eredményeihez képest. Végül, a folyamatos fejlesztések után, 2003 tavaszán napvilágot látott a Windows Server 2003 is.

A Windows Server 2003 újdonságai révén rugalmasan kezelhető a biztonság: már a gyári kiépítésű rendszer is nagyobb védelmet biztosító alapokat nyújt, de a technológiák széles köre révén még biztonságosabb megoldások elkészítésére, üzembe helyezésére és üzemeltetésére

nyílik lehetőség. A Microsoft alapvető szerkezeti változtatásokat hajtott végre, módosította a beállításokat, hogy alapértelmezés szerint is biztonságosabb legyen a rendszer, valamint olyan új szolgáltatásokat és technológiákat készített el, amelyek növelik a Windows platform biztonságosságát.

A biztonságot a Windows Server 2003 tervezésekor és elkészítésekor is kiemelt prioritásként kezelték. Olyan új funkciókat építettek be, amelyek birtokában könnyebben lehet biztonságos infrastruktúrát kialakítani. A Windows Server 2003 olyan továbbfejlesztett összetevőkből épül fel, amelyek a biztonsági szempontú tervezés új gyakorlatán alapulnak. Ezek az összetevők olyan elemeket tartalmaznak, amelyek tervezésekor a biztonság volt az első számú alapelv.

A Windows Server 2003 már gyári kiépítésű változatában is biztonságosabb alapot nyújt, amelyre a vásárlók a kiszolgáló támadásnak kitett felületét csökkentő megoldásokat építhetnek. A Microsoft a Windows Server 2003 termékcsalád fejlesztése során messzemenően felhasználta az ügyfelek és külső partnerek visszajelzéseit, valamint több ezer független tesztelő eredményeit.

2. A Windows Server 2003 bemutatása

A Windows Server 2003 a kiszolgáló operációs rendszerek következő, a modern világ igényeinek kielégítésére alkalmas generációja. A Windows Server 2003 a Windows Server termékcsalád természetes fejlődésének következő lépcsőfokát képviseli. A Windows Server 2003 a Windows 2000 Server technológiáira épül, azokat tökéletesíti és korszerűsíti. Ezen kívül, a felhasználók és a változó világ igényeinek megfelelően a Windows Server 2003 temérdek új szolgáltatást és technológiát tartalmaz. A Windows Server 2003-at új szolgáltatásai és bővítései a Microsoft legmegbízhatóbb vállalati kiszolgáló operációs rendszerévé tették.

2.1 A Windows Server 2003 újdonságai

A Windows Server 2003 operációs rendszer megbízható informatikai környezet, amely a Windows 2000 Server használata során megszokott megbízhatóságot, rendelkezésre állást, méretezhetőséget és biztonságot még magasabb szintre emelő jelentős fejlesztéseket foglal magában.

Új, feladatorientált felépítés - A Microsoft a Windows Server 2003 rendszer készítése során a hatékonyságot és a könnyű használatot tartotta szem előtt. Az új, feladatközpontú felépítés révén egyszerűbb a mindennapos feladatok elvégzése. A felhasználóknak és a rendszergazdáknak kevesebb időt kell tölteniük a problémák megoldásával, és több idejük marad a hasznos feladatok ellátására.

Egyszerű telepítés és áttérés - A Windows Server 2003 bevezetéséhez hatékony telepítőeszközök állnak rendelkezésre, ilyen a távtelepítő szolgáltatás (RIS - Remote Installation Services), amelynek segítségével alacsonyan tarthatók a kezdeti költségek is. A felhasználók állapotát átvivő eszköz (USMT - User State Migration Tool) segítségével a felhasználói beállítások összegyűjtése és az új rendszerbe történő átvitele szintén egyszerű a rendszergazdák számára.

Háttérmásolat funkció - A háttérmásolat-helyreállítása funkcióval a rendszergazdák hozzáférhetnek a hálózati megosztások adott időpontban létrejött biztonsági másolataihoz. Az árnyékmásolatok beállítása, csakúgy, mint az erőforrások biztonsági másolatainak megkeresése, egyszerű.

Active Directory - A hálózat felhasználóiról és számítógépeiről központilag állnak rendelkezésre a hierarchikus információk, így az Active Directory jóvoltából egyszerűbb az asztali számítógépek felügyelete. Az Active Directory teljesítménye és menedzselhetősége lényegesen jobb lett a Windows Server 2003-ban. Az új metacímtár szolgáltatás (MMS - Microsoft Metadirectory Services) segítségével a vállalat több címtárának adatai egyesíthetők.

Csoportházirend - A csoportházirend biztosítja a hálózat központi beállítását és felügyeletét, így csökkenti az ezzel kapcsolatos felügyeleti költségeket. A Windows Server 2003-ban a csoportházirend-kezelés nagymértékben egyszerűsödött. Az eredő házirend eszköz segítségével a rendszergazdák hatékonyan kezelhetik az asztali számítógépeken alkalmazott házirendeket, a szoftverkorlátozási házirendek révén pedig beállíthatják, hogy milyen programok futhatnak a felhasználók gépein.

Tárolókezelés - A Windows Server 2003-ban a tárolókezelés új, jobban átgondolt kezelőfelülettel rendelkezik. A gyors és megbízható tárolókezelés a hatékonyság biztosításának elengedhetetlen eszköze. A Windows Server 2003 rugalmas, méretezhető módon tárolja a fontos adatokat. A DFS (Distributed File System) segítségével egy központi gépen, egy helyen tartható karban a hálózat összes gépének minden megosztott mappája. A SAN (Storage Area Network) egy nagysebességű, speciális célú hálózat, ami különböző fajta adattároló eszközök összekapcsolódását jelenti a hozzájuk kapcsolt adatkiszolgálóval, a nagyszámú felhasználók hálózata helyett. A DFS, a SAN, a tárolókezelés gyorsaságának és kapacitásának javítása mind a rugalmasságot és méretezhetőséget szolgálja.

Továbbfejlesztett terminálszolgáltatások - A Microsoft terminálszolgáltatási technológiájával a virtuális Windows-asztal összes funkciója elérhető szinte minden eszközről. Az új verziójú távoliasztal-protokoll (RDP - Remote Desktop Protocol) megnöveli a terminálszolgáltatások teljesítményét, és új funkciókkal ruházza fel a szolgáltatást.

Fájl- és nyomtatószolgáltatások - A Windows Server 2003 kiválóan alkalmas arra, hogy a felhasználóknak kiszolgálóoldali, például fájl- és nyomtatószolgáltatásokat nyújtson. A nyomtatószolgáltatást is továbbfejlesztették, amely így már a nyomtatófürtözést is támogatja.

Webszolgáltatások - A webszolgáltatások egy olyan alkalmazásgyűjteményt alkotnak, amelyekből teljes üzleti megoldás állítható össze. A Windows Server 2003 a legalkalmasabb platform az XML alapú webszolgáltatások igény szerinti, gyors elkészítésére, terjesztésére és közzétételére.

Internet Information Services 6.0 - A Windows Server 2003 a webkiszolgáló legújabb verzióját, az IIS 6.0-t tartalmazza. Az IIS weblapok, alkalmazások és webszolgáltatások közzétételének megbízható, méretezhető platformja, amelynek segítségével a web lehetőségeit a lehető legjobban kihasználhatjuk.

Windows Media szolgáltatások - A Windows Server 2003 médiafolyam-szolgáltatásai teljesen megújultak, és nagyszerű minőségű hálózati multimédia-sugárzást tesznek lehetővé. A médiaszolgáltatások gyorsabbak, robusztusabbak lettek, és a tartalom dinamikus elrendezésének lehetősége által jobban megfelelnek a mai elvárásoknak. A gyors médiatovábbító technológia révén csökkent a gyorsítótárazás ideje, nőtt a megbízhatóság, miközben az erőforrások kihasználtsága gazdaságosabb lett.

2.2 A Windows Server 2003 termékcsalád tagjai

A Windows Server 2003 kiszolgálócsalád tagjai a Windows alapú kiszolgálók folyamatos fejlődésének következő fokát képviselik. A Windows Server 2003 megőrzi a Windows 2000 Server bizonyított megbízhatóságát, méretezhetőségét és kezelhetőségét.

A Windows Server 2003 termékcsaládnak 4 tagja van:

- **Windows Server 2003, Standard Edition** - Ez a megbízható kiszolgáló operációs rendszer képes kielégíteni bármilyen méretű vállalat mindennapi igényeit. Optimális megoldást jelent a fájl- és a nyomtatómegosztáshoz, biztonságos internetkapcsolatok kialakításához, valamint az alkalmazottak és ügyfelek hálózati környezetének kialakításához.
- **Windows Server 2003, Enterprise Edition** - A nagyvállalatok, valamint a kis- és közepes vállalkozások számára nyújt megoldást biztonságos alkalmazások, webszolgáltatások, valamint infrastruktúra fejlesztésére és bevezetésére. Magas szintű megbízhatóság és teljesítmény jellemzi. Az Enterprise Edition 32-bites és 64-bites változatban is kapható.
- **Windows Server 2003, Datacenter Edition** - Ez a változat olyan alkalmazások kiszolgálására szolgál, amelyek a méretezhetőség és a rendelkezésre állás legmagasabb fokát követelik meg. A Datacenter Edition 32-bites és 64-bites változatban is elérhető.
- **Windows Server 2003, Web Edition** - Ez a változat weboldalak kiszolgálására a legalkalmasabb, de megőrzi mindazokat az alapfunkciókat, amelyek a fokozott megbízhatóságot, felügyeletet és biztonságot nyújtják.

A Windows Server 2003 rendszerkövetelményei				
Követelmény	**Standard Edition**	**Enterprise Edition**	**Datacenter Edition**	**Web Edition**
Minimális processzorsebesség	133 MHz	• 133 MHz x86 alapú számítógép esetén • 733 MHz Itanium alapú számítógép esetén	• 400 MHz x86 alapú számítógép esetén • 733 MHz Itanium alapú számítógép esetén	133 MHz
Ajánlott processzorsebesség	550 MHz	733 MHz	733 MHz	550 MHz
Minimális RAM	128 MB	128 MB	512 MB	128 MB
Ajánlott RAM	256 MB	256 MB	1 GB	256 MB
Maximális RAM	4 GB	• 32 GB x86 alapú számítógép esetén • 64 GB Itanium alapú számítógép esetén	• 64 GB x86 alapú számítógép esetén • 512 GB Itanium alapú számítógép esetén	2 GB
Több processzor támogatása	Legfeljebb 4	Legfeljebb 8	• Legalább nyolc processzor befogadására alkalmas gép szükséges • Legfeljebb 64	Legfeljebb 2
Telepítéshez szükséges lemezterület	1,5 GB	• 1,5 GB x86 alapú számítógép esetén • 2,0 GB Itanium alapú számítógép esetén	• 1,5 GB x86 alapú számítógép esetén • 2,0 GB Itanium alapú számítógép esetén	1,5 GB

2.3 A .NET és a Windows Server 2003

A Microsoft .NET olyan technológiák együttese, amelyek segítségével információt, embereket, rendszereket és eszközöket összekapcsoló alkalmazásokat lehet készíteni. A .NET segítségével a kulcsfontosságú üzleti folyamatok XML-alapú webszolgáltatásokká alakíthatók, amelyekből könnyen lehet teljes üzleti megoldást építeni.

A Windows Server 2003 megbízható, méretezhető, nagy teljesítményű operációs rendszer. Alkalmas az XML-alapú webszolgáltatások készítésére, terjesztésére és kiszolgálására. A .NET-keretrendszer a Windows Server 2003 szerves része, így beépített eszközökkel támogatja az olyan webszolgáltatás-szabványokat, mint az XML (eXtensible Markup Language), a SOAP (Simple Object Access Protocol), a UDDI (Universal Description Discovery and Integration) vagy a WSDL (Web Service Description Language).

A Windows Server 2003 növeli a fejlesztők hatékonyságát is, mert olyan eszközöket biztosít, amelyek segítségével tetszőleges programnyelven lehet elosztott szolgáltatásokat létrehozni. A Windows Server 2003 több újrafelhasználható objektumot, beépített szolgáltatást adott a fejlesztőknek, és tartalmazza a .NET-keretrendszert.

A UDDI-szolgáltatások megkönnyítik a webszolgáltatások és más programozható erőforrások megkeresését, megosztását és újrafelhasználását. Javítják a fejlesztés és az üzemeltetés hatékonyságát. A rájuk épülő alkalmazások is megbízhatóbbak lesznek és javul a felügyelhetőségük. A Windows Server 2003-ban a vállalati UDDI (Enterprise UDDI) szolgáltatások szabványos webszolgáltatás-infrastruktúrát biztosítanak a magán UDDI-szolgáltatások használatához.

A Windows Server 2003 mindemellett az IIS legújabb változatát is tartalmazza. Az IIS 6.0 funkciói nagymértékben javítják a rendszerek teljesítményét és a megbízhatóságát. Az IIS-en futó webes alkalmazások hatékonyabban használhatják ki a többprocesszoros számítógépek teljesítményét. A végrehajtási szálak jobb elkülönítése és kezelése nagyobb megbízhatóságot eredményez. Az IIS 6.0 szerves része az ASP.NET-szolgáltatás (Active Server Pages .NET), amellyel könnyebb a nagy teljesítményű webszolgáltatások létrehozása.

2.4 Windows Server 2003 R2

A Windows Server 2003 R2 a Windows Server 2003 operációs rendszer frissítő kiadása, amely 2005 év végén jelent meg. A Windows Server 2003 R2 a Windows Server 2003 Service Pack 1 (SP1) változatára épül, kihasználja a már bevált programkód továbbfejlesztett stabilitási és biztonsági funkcióit, ugyanakkor új területekre terjeszti ki a kapcsolódási és a felügyeleti lehetőségek körét. A Windows Server 2003 R2 tartalmazza a Windows Server 2003 SP1 minden előnyét, továbbá jelentős előrelépést hoz a más telephelyen működő kiszolgálómegoldások, az identitás- és hozzáférés-kezelés, a tárolóeszközök üzembe helyezése és felügyelete, valamint az alkalmazásfejlesztés területén.

Egyszerűbb a kiszolgálók felügyelete

A Windows Server 2003 R2 valóra váltja az elképzeléseket, és biztosítja azokat az alaptechnológiákat, amelyekkel egyszerűbben integrálhatók a más telephelyen működő kiszolgálók. A Windows Server 2003 R2 kiadással megőrizhető a más telephelyen működő kiszolgálók teljesítménye, rendelkezésre állása és termelékenységi előnye, ugyanakkor elkerülhetők az ilyen kiszolgálómegoldásokkal általában felmerülő problémák, például a korlátozott kapcsolódási lehetőségek és a felügyelettel járó többletterhelés.

Egyszerűbb identitás- és hozzáféréskezelés

Új lökést kapott az identitás- és hozzáféréskezelés is, mivel a Windows Server 2003 R2-ben már lehetőség van az ADFS (Active Directory Federation Services) és az ADAM (Active Directory Application Mode) használatára is. Az ADFS lehetővé teszi, hogy két Active Directory, vagy akár több, eltérő platformon üzemelő címtár képes legyen együttműködni egymással, és ugyanazokat a felhasználókat tudják hozzárendelni saját erőforrásaikhoz. Az ADAM ezzel szemben egy lényegesen eltérő problémára nyújt megoldást: lehetővé teszi, hogy akár alkalmazásonként saját mini címtárat hozzunk létre, amiben eltárolhatóak az alkalmazások beállításai és felhasználói is.

Együttműködés más rendszerekkel

A Windows Server 2003 R2 képes mindenféle probléma nélkül együttműködni például a Unix-os NIS-sel. A Server for Network Information Services elősegíti a Windows és a UNIX alapú Network Information Service (NIS) integrálását. A jelszó-szinkronizálás pedig azzal járul hozzá a Windows és a UNIX kiszolgálók integrációjához, hogy leegyszerűsíti a biztonságos jelszavak folyamatos karbantartását.

Tárolási újdonságok

A Windows Server 2003 R2 új eszközöket tartalmaz, amelyek lehetőséget nyújtanak a tárolóeszközök központi megjelenítésére, a tárolási megoldások egyszerűbb megtervezésére, üzembe helyezésére és karbantartására, továbbá tökéletesített figyelési és jelentéskészítési funkciókat biztosítanak. Ezekkel az előnyökkel a rendszergazdák hatékonyabban kezelhetik a különféle informatikai erőforrások tárolási elemeit, és optimalizálhatják az erőforrásokon elérhető tárterület kihasználását.

Egyszerűsödött a hálózati tárolóeszközök (SAN) kezelése a Storage Manager for SANs révén, amivel a rendszer adminisztrátorai logikai egységekbe szervezhetik tárolóegységeiket. Már arra is lehetőség van az üvegszálas szállítási rendszerek esetében, hogy egy adott irányú adatforgalom egyszerre több célpontra érkezzen meg, ezáltal azonnal megoldva a replikációt is az adatok biztonságának szavatolására.

Az ugyancsak újdonságnak számító File Server Resource Management (FSRM) technológiával most már nem csak NTFS logikai meghajtókhoz adhatunk meg felhasználónként kvótákat, hanem akár egyes könyvtárakhoz is meghatározhatjuk, hogy ki mekkora területet foglalhat el benne, ráadásul a számunkra fontos változásokról már nem csak az eseménynaplón keresztül értesülhetünk, hanem akár levélben, vagy speciális kimutatásokban is.

Virtualizáció

A Virtual Server 2005 R2 újabb lépés a virtualizáció kiteljesedése felé a Windows platformon. A Virtual Server 2005 R2 már arra is képes, hogy a virtuális és valódi gépek, fürtök között automatikusan átterhelje a futó szoftvereket, ezáltal növelve a rendszer üzembiztonságát, rendelkezésre állását, és mégis csökkenti a működési költségeket.

Licencelés

A Windows Server 2003 R2 megjelenésével a licencelés is változott egy keveset, hiszen az Enterprise változatot megvásárolók egyszerre négy virtualizált példányt is használhatnak a licencszerződésük keretein belül, bármiféle külön költség nélkül.

.NET 2.0

Szintén érdekes újdonság, hogy a Windows Server 2003 R2-ben már megtalálható a .NET keretrendszer 2.0-s változata is, ami a webszerverként történő felhasználás esetében jelent további előnyt.

3. Biztonsági kérdések

A biztonsági kérdéseket alapvetően két fő részre bonthatjuk, a hálózat és a rendszer biztonságára. A rendszer alatt az operációs rendszert és a rajta futó alkalmazásokat értjük. A biztonság nemcsak a beállítások kérdése, hanem egy integrált rendszer, melynek a komponenseit a fizikai biztonság, az üzemeltetési biztonság, valamint a házirend teszik ki. Fizikai biztonság alatt a különböző eszközökhöz való fizikai hozzáférést értjük, így például a szerverszobába való bejutás tartozhat ide.
Az üzemeltetés biztonsága kiterjed a különböző jogosultságok beállítására, biztonsági mentésekre, vírusfrissítésre, különböző biztonsági frissítések telepítésére, felügyeleti tevékenységekre, hitelesítési kérdésekre.

3.1 Fenyegetések

A következőkben röviden ismertetném azokat a különböző fenyegetéseket, amelyek a hálózatunkat illetve rendszerünket, és az azokon tárolt adatokat veszélyeztethetik.

A különböző támadások alapvető célja többféle lehet:

- Hozzáférési támadás (access attack), ahol a támadó valamilyen erőforráshoz (fájlok, lemezek) akar hozzáférni.
- Módosítási támadás (modification attack), amelynek célja az információk megváltoztatására irányul.
- Szolgáltatás blokkolás (denial of service), ahol a támadás a hálózat, vagy bizonyos szolgáltatások blokkolását célozza meg.

3.2 Védekezés

Az előzőekben leírt fenyegetettségek elleni védekezés nem egyszerű feladat. A legfontosabb megjegyezni azt, hogy a teljes rendszer biztonsága a leggyengébb elem biztonsági szintje. Folyamatos vizsgálódással fel kell tárni a rendszer leggyengébb pontját, majd ezt ki kell javítani.
Alapvető feladat egy rendszerben, hogy tűzfalat és vírusirtót üzemeltessünk, és természetesen nem szabad megfeledkezni a biztonsági frissítések telepítéséről sem. Azonban a legelső és legfontosabb dolog, amit meg kell említeni, az a házirend. Emellett a másik fontos dolog, amely szorosan kapcsolódik a házirendhez, a jelszavak biztonsága.

3.3 Házirendek

A házirend kérdése kicsit bonyolultabb a hálózat- és rendszerbiztonsági kérdéseknél, hiszen nehezen megfogható problémáról beszélünk. Szükség van biztonsági szabályozásra, hiszen csak a technológiai alapokra építve nem lehet teljes a teljes hálózatunk biztonsága. Ezek a biztonsági szabályok nem mások, mint különböző rendelkezések összessége, amelyek érvényesek a hálózati felhasználókra. A szabályoknak tartalmazniuk kell mindazon tevékenységeket, amelyeket egyrészt a felhasználóknak tilos, másrészt pedig kötelező végrehajtani. A biztonság létrehozásánál nagyon fontos, hogy egy olyan rendszert hozzunk létre, ahol a fizikai védelem és a házirendek együttesen, megfelelő arányban elosztva alkotnak meg egy komplett védelmi rendszert. Nem ér semmit például egy fejlett behatolás figyelő rendszer, ha a házirend közben megengedi egyszerű jelszavak használatát.

Többféle házirend is létezik:

- **Rendszergazdai házirend:** az üzemeltetés során az üzemeltetési személyzet számára készülő házirend, amely a napi tevékenységeket írja le. A frissítések elvégzése, a naplózás figyelése tartozik ide. Rugalmasnak kell lennie, hiszen a nem várt eseményeket is kezelni kell.

- **Fejlesztési házirend:** a használt, fejlesztett rendszerek tekintetében is szükségünk van házirendre, mely leírja azokat a követelményeket, hogy fejlesztett vagy vásárolt rendszerrel lesz dolgunk. Célja, hogy az alkalmazások oldaláról a biztonsági fenyegetettségeket kiiktassuk.
- **Katasztrófa elhárítási terv:** a katasztrófa elhárítási terv elkészítése, tesztelése, naprakészen tartása időigényes feladat. A katasztrófa terv része a mentési - visszaállítási terv is. A katasztrófa elhárítási terv bármely hiba esetén a szükséges tevékenységeket írja le, kinek, mit kell tennie, hogy a megadott időre a hiba el legyen hárítva.
- **Információ védelmi házirend:** itt határozzuk meg az egyes információk keletkezését, tárolását, besorolásának módját. Természetesen az információ a hálózaton keresztül továbbítódik, ezért a hálózat-biztonsági kérdések is a házirend részei.
- **Biztonsági házirend:** a biztonsági házirend írja le a rendszerek és hálózatok konfigurációját. Ide tartozik a telepítés, a vírusirtó szoftverek, a titkosítás, a jelszó kezelésével kapcsolatos kérdések, mint például a jelszó hossza. A házirendhez tartozik az információ védelme, és a hozzáférési szabályok is.
- **Felhasználó kezelési házirend:** a felhasználók felvételével, a jogosultsági rendszer használatával kapcsolatos eljárások találhatók meg a házirendben. Ide tartoznak azon tevékenységek, amelyek akkor szükségesek, ha illetéktelen hozzáférésre derül fény, illetve itt írjuk le a felhasználók távozása esetén követendő tevékenységeket.

3.4 Jelszavak

A rendszer biztos védelme érdekében olyan jelszó házirend kialakítására van szükség, ami kellően bonyolult elemeket tartalmaz és nehéz csak úgy kitalálni. Meg kell határozni, hogy mi az a jelszó bonyolultság és jelszó hossz, amit a rendszer biztonsági szintje megkövetel. Egy jó jelszó szabályrendszer esetében bizonyos időközönként meg is kell változtatni ezeket a jelszavakat. A jelszavakra vonatkozó követelmények a legkevésbé függhetnek a felhasználók kényelmi érzeteitől. Attól függően, hogy mekkora a védeni kívánt érték, ennek függvényében szükséges kialakítani a hitelesítési folyamatokat is.

3.5 Hitelesítés

A Microsoft termékei számos hitelesítési eljárást használtak és használnak mind a mai napig. A Windows termékek, mint asztali operációs rendszerek jelentek meg először. A Microsoftnak a kezdetek kezdetén nem volt szerver terméke, ezért a szerver termékeket gyártó cégekkel együttműködve alakítottak ki különböző biztonsági eljárásokat.

3.5.1 A LAN Manager (LM) hitelesítés

Az IBM OS2 operációs rendszer kompatibilitása miatt használta a Microsoft a Windows for Workgroup, Windows 95, Windows 98 és Windows ME termékeiben. Napjainkban már ez a legkevésbé biztonságos eljárás a hitelesítések közül. A szükséges felhasználói nevet és jelszót tárolni kell. Ez pedig a hálózaton megy keresztül, és ha valaki egy ilyen csomagot elkap, akkor az erre a célra alkalmas eszközzel visszanyerhető a felhasználói név és a hozzátartozó jelszó.

NTLM verzió 1

A LAN Manager hibái persze kiderültek egy idő után, és a Microsoftnak ki kellett találnia valamit a problémára, méghozzá úgy, hogy az operációs rendszer drasztikus átalakítása nélkül megvalósítható legyen. Az ötlet persze egyszerű és nyilvánvaló is, titkosítani kell az adatfolyamot, amely a hitelesítési információkat tartalmazza. Mivel a Microsoft piacra dobta a Windows NT termékcsaládot, gondoskodnia kellett a biztonságról. Ezért a hitelesítési folyamat egy 56 bites titkosítási algoritmus segítségével történt. A Microsoft ezek után úgy gondolta, hogy tökéletes módszert alkotott meg. Azonban a gépek rohamos fejlődésével, a teljesítmények növekedésével eljött az az idő, amikor az 56 bites titkosítás visszafejtése már nem okozott gondot.

NTLM verzió 2

Ez az egyik legbiztonságosabbnak tekintett hitelesítés, mivel ez már 128 bites titkosítási algoritmust használ, éppen ezért a Windows Server 2003 is támogatja ezt. Napjaink számítógépeinek teljesítménye még kevés a 128 bites kulcs hatékony feltöréséhez, ehhez még

jó pár évet várni kell. A jelenlegi gépek teljesítményével a visszafejtéshez szükséges idő 10, vagy akár 100 években mérhető. Azonban gondoskodni kellett a régebbi rendszerekről is. Windows NT4 esetén a SP4 jelenthet megoldást, Windows 95, Windows 98 és Windows ME rendszereknél pedig a Windows Server 2003 CD-n található DSClient.exe javítja fel a termékeket, hogy képesek legyenek kommunikálni NTLMv2-vel.
Azonban a fejlődés sosem áll meg, ez a módszer sem tekinthető már elégséges védelmi fokozatnak. Ha csak tehetjük, szabaduljunk meg ettől az eljárástól. Ennek feltétele, hogy a hálózatban már csak Windows 2000 és afeletti operációs rendszer működjön.

3.5.2 A Kerberos hitelesítés

Mivel a Windows 2000 rendszer óta ez az alapértelmezett hitelesítési eljárás, ezért több figyelmet fordítok ennek bemutatására. Ez a módszer hitelesítési jegyekkel (ticket) dolgozik, ami nem más, mint egy speciális adathalmaz, ami a hálózaton halad és nem tartalmazza a felhasználó jelszavát. Maga a jegy egy speciális hitelesítési formát képvisel, ami a UNIX világból került át a Microsofthoz.
A Windows 2003 rendszer erőforrásainak eléréséhez a felhasználónak hitelt érdemlően azonosítania kell önmagát. Ez az azonosítás általában a rendszerbe való belépéskor történik meg, ezután a felhasználó egy testre szabott access token-t kap, ami tartalmazza jogosultságait is. A szolgáltatást nyújtó eszközök ezt az access token-t ellenőrzik, majd ez alapján döntik el, hogy a felhasználó hozzáférhet-e egy erőforráshoz (megosztott fájlhoz, számítógéphez), vagy sem.
Az NTLM hitelesítésnek köztudottan több hátránya van: egyrészt, a kapcsolatfelvétel során a felhasználó jelszavából létrehozott kivonat (hash) többször megjelenik a hálózaton. Ez ugye nem igazán biztonságos. Másrészt pedig a tartományok közötti hitelesítés folyamata kettőnél több tartomány esetén olyannyira bonyolulttá válik, hogy gyakorlatilag nem is lehetséges.

A protokoll áttekintése

A Kerberos hitelesítő protokoll egy kommunikációs kapcsolat résztvevőinek kölcsönös azonosítását teszi lehetővé olyan környezetben, ahol az átvitt adat illetéktelenek által látható, módosítható, egyszóval a biztonságos adatátvitel nem garantálható. Ez a környezet nagyon

hasonlít napjaink Internetéhez, ahol az illetéktelen behatoló átveheti akár az ügyfél, akár a kiszolgáló szerepét, és így értékes információkhoz juthat. A feladat tehát egy olyan biztonságos kommunikáció megvalósítása, amely az első kapcsolatfelvételtől kezdve kizárja az illetéktelen hozzáférést.

Egy példa

A Kerberos protokoll alapja a közös titkon alapuló hitelesítés. Az elv egyszerű: ha egy titkot csak két ember ismer, azok a közös titok segítségével könnyedén azonosíthatják egymást.
Vegyünk egy példát, az angolszász világban népszerű párost, Alizt és Bobot. Tegyük fel, hogy Aliz gyakran küld üzeneteket Bobnak, Bob viszont szeretne biztos lenni abban, hogy az Aliztól kapott leveleket valóban Aliz írta. Elhatározzák, hogy együtt választanak egy jelszót, amit nem árulnak el kettőjükön kívül senkinek sem. Ha Aliz üzenetén valahogy látszik, hogy ismeri a közös titkot, Bob biztos lehet abban, hogy a levél valóban Aliztól származik.

Adódik azonban egy probléma: honnan derül ki, hogy Aliz valóban ismeri a titkot? Ha Aliz beleírná azt az üzenetbe, akkor egy harmadik személy (ő legyen Carol) elég, ha csak egy ilyen üzenetet elkap a hálózaton, a titok máris nem titok többé. Valami más megoldásra van szükség: anélkül kell jeleznünk a jelszó ismeretét, hogy azt beleírnánk az üzenetbe.
A Kerberos ezt közös kulcsú (más néven szimmetrikus kulcsú) titkosítás segítségével oldja meg. A szimmetrikus titkosítás lényege, hogy egy adott, közös kulcs segítségével titkosított üzenetet ugyanazzal a kulccsal tudunk csak megfejteni. A kommunikáció résztvevői pedig ezt a kulcsot használják közös titokként. A titok ismerete egyszerűen bizonyítható: egyik részről az üzenet titkosítása, másik részről a megfejtése a bizonyíték, hiszen a közös kulcs ismerete nélkül ezek egyike sem lehetséges.

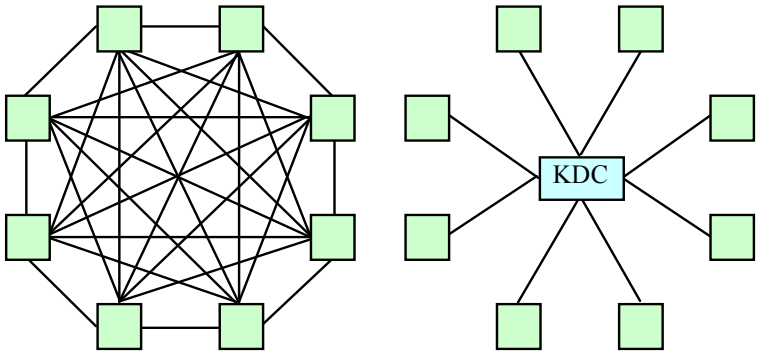
Lássuk kicsit részletesebben, Aliz és Bob példáján. Aliz a felhasználó, aki szeretne hozzáférni Bob egy szolgáltatásához.

1. Aliz egy üzenetet küld Bobnak, amely a saját nevéből, valamint egy, a közös kulccsal titkosított hitelesítőből áll. Ebben a példában a hitelesítő két adatmezőt tartalmaz: az egyik valami, ami azonosítja Alizt, mondjuk a neve. A másik pedig az Aliz számítógépén mért pontos idő.

2. Bob megkapja Aliz üzenetét. Az üzenetből azonnal látszik, hogy olyasvalaki küldte, aki Aliznak mondja magát. Bob a közös kulccsal megfejti a hitelesítőt, és így hozzáfér Aliz valódi nevéhez, valamint az Aliz számítógépén mért időhöz. A protokoll működéséhez fontos, hogy Bob és Aliz számítógépének órái szinkronizálva legyenek. Tegyük fel, hogy a két óra közötti eltérés soha nem nagyobb, mint öt perc. Bob tehát összehasonlítja a hitelesítőben kapott időt és a saját óráját. Ha az eltérés kevesebb, mint öt perc, Bob majdnem biztos lehet abban, hogy az üzenetet Aliz küldte. Azért csak majdnem, mert lehetséges, hogy Aliz hitelesítőjét valaki a hálózaton elkapta, majd változatlanul, de öt percen belül újraküldte. Ez a megismételt hitelesítő a fentiek alapján még érvényesnek számítana. Bob ezt úgy kerülheti el, hogy megjegyzi az Aliztól utoljára megérkezett hitelesítő időpontját, és ha annál régebbi, vagy azzal megegyező időpontú hitelesítőt kap, akkor gyanakodni kezdhet. Ha azonban minden rendben van, akkor biztos lehet abban, hogy az üzenet Aliztól érkezett.
3. Most Bobon a sor: kiveszi az időpontot az Aliztól kapott hitelesítőből, azt a közös kulccsal újra titkosítja, majd visszaküldi Aliznak.

Fontos megjegyezni, hogy Bob nem a teljes hitelesítőt küldte vissza, hiszen arra bárki képes lenne, hanem annak csak egy részét. Aliz így biztos lehet abban, hogy Bob rendelkezik a közös kulcs egy példányával, hiszen képes volt megfejteni az üzenetet, módosítani a tartalmát, majd újra titkosítani azt.
Miután Aliz megkapja Bob üzenetét, visszafejti a titkosított adatokat, majd a kapott időpontot összehasonlítja az ő általa küldött adattal. Ha a két időpont megegyezik, akkor Aliz biztos lehet benne, hogy üzenetét Bob kapta meg, hiszen a közös kulcsot csak ők ketten ismerik.

Központosított kulcskezelés (Key Distribution)
Ez azonban még korántsem jelent megoldást minden problémára. Az előbb megnéztük Aliz és Bob példáját, ami viszonylag egyszerű volt. De mi a helyzet akkor, ha nem kettő, hanem mondjuk nyolc személy szeretne biztonságosan kommunikálni? A zűrzavart úgy kerülhetjük el, ha kijelölünk egy központi egységet, akinek mindenki megadja a saját kulcsát, és ha valaki kommunikálni szeretne, ugyancsak tőle kéri el a címzettnek szóló kulcsot. Az alábbi ábrán jól látszik, hogy mennyivel kisebb lesz a hangzavar.



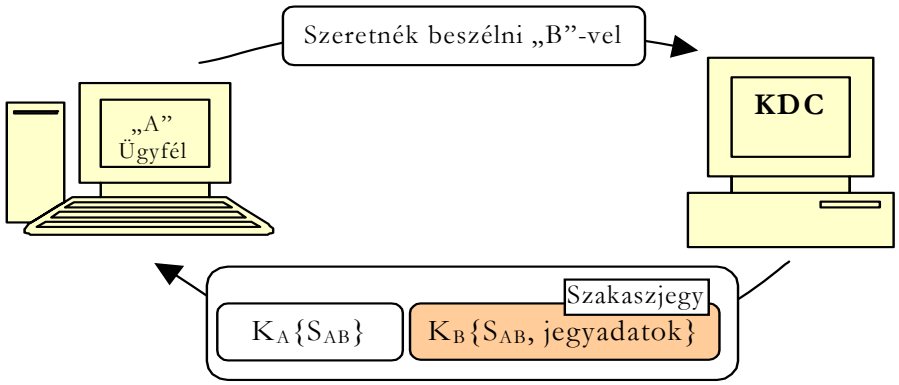
A görög mitológiából ismert Kerberos (pontosabban Cerberus), az alvilág kapuját őrző háromfejű kutya volt. Az elnevezés nem véletlen, hiszen a modern Kerberos három feje a következő: az ügyfél, aki a szolgáltatást igénybe szeretné venni, a kiszolgáló, aki a szolgáltatást nyújtja, valamint a harmadik fél, aki segít abban, hogy az ügyfél és a kiszolgáló végül egymásra találjon.

Ez a harmadik fél, mint a fenti ábrán is látszik, a Key Distribution Center (KDC). A KDC egy megbízható, biztonságos kiszolgálón fut, ő kezeli a Kerberos tartomány biztonsági adatbázisát. A Kerberos tartomány egyébként egyenrangú a Windows 2003 tartománnyal, tehát minden Windows 2003 tartományban található legalább egy KDC, amely a helyi feladatokkal foglalkozik. A KDC és az ügyfél egymás közti kommunikációjuk során az ügyfél úgynevezett hosszú távú kulcsát (long-term key) használják, amit előzőleg általában a felhasználó jelszavából állítanak elő. A KDC természetesen a tartomány minden felhasználójának és számítógépének ismeri a hosszú távú kulcsát.

Ha tehát egy ügyfél szeretné felvenni a kapcsolatot egy kiszolgálóval, előbb szól a KDC-nek, aki az ügyfél és a kiszolgáló jövőbeli kapcsolatára egy eldobható, úgynevezett rövid távú kulcsot (session key) állít elő. Minden új ügyfél-kiszolgáló kapcsolathoz új rövid távú, más néven szakaszkulcs tartozik. A KDC ezt a rövid távú kulcsot az ügyfél hosszú távú kulcsával titkosítva elküldi az ügyfélnek, a kiszolgáló hosszú távú kulcsával titkosítva elküldi a kiszolgálónak, azok megfejtik az üzenetet és az új, közös szakaszkulcs segítségével máris indulhat a kommunikáció.

Szakaszkulcsok (Session Tickets)

A valóságban azonban ez egy kicsit másképp működik. A szakaszkulcsot a KDC csak az ügyfélnek küldi el, mégpedig úgy, hogy a visszaküldött csomagba – az ügyfél hosszú távú kulcsával titkosított szakaszkulcs mellé – beletesz egy adatstruktúrát, amely a kiszolgáló számára titkosított, és amely a szakaszkulcs mellett még más hasznos információkat is tartalmaz, amit persze az ügyfél se visszafejteni, se módosítani nem képes.

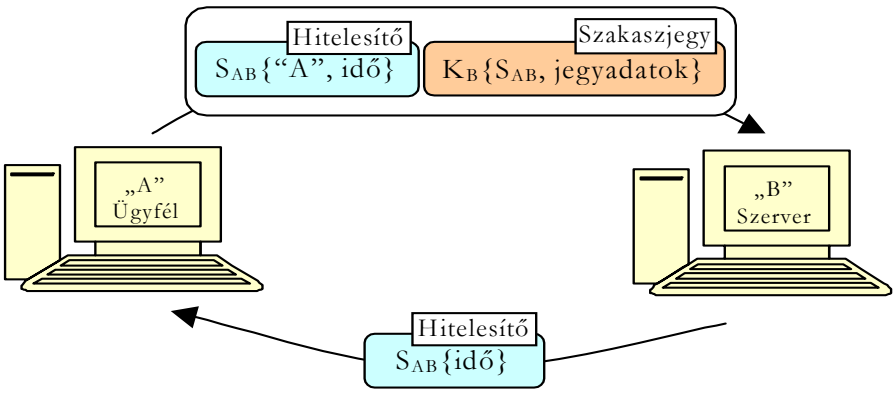


A KDC működés közben (K_A az ügyfél, K_B a kiszolgáló hosszú távú kulcsa, S_{AB} a KDC által a kapcsolathoz generált szakaszkulcs)

Ezt a beágyazott adatcsomagot hívjuk szakaszjegynek (session ticket), mégpedig azért, mert az ügyfél ezt a jegyet bemutatva tudja majd felvenni a kapcsolatot a kiszolgálóval. A KDC nem foglalkozik azzal, hogy az üzenetek valóban eljutnak-e a címzetthez, ugyanis semmi baj nem történik, ha a válasz elveszik, legfeljebb az ügyfél később újabb kulcsot kér.

Lássuk, mihez kezd az ügyfél a visszakapott csomaggal. Egyrészt a saját hosszú távú kulcsával kicsomagolja a szakaszkulcsot, és biztonságos helyre teszi. A szakaszjegyet a kulcs mellé helyezi. Amikor a konkrét kapcsolatfelvételre sor kerül, a szakaszkulccsal előállít egy hitelesítőt (authenticator-t), majd ezt és a címzetthez érvényes szakaszjegyet elküldi a kiszolgálónak. A kiszolgáló a csomagból kiveszi a neki szóló szakaszjegyet, a saját hosszú távú kulcsával megfejti azt, kiveszi belőle a szakaszkulcsot és jegy egyéb adatait. Ha az adatok alapján úgy dönt, hogy szóba áll az ügyféllel, a szakaszkulcs segítségével kicsomagolja a kapott hitelesítőt, ellenőrzi az időt, törli a hitelesítő egy részét, a maradékot a

szakaszkulccsal visszacsomagolja, és visszaküldi az ügyfélnek. Az ügyfél a visszakapott hitelesítőt visszafejti, ellenőrzi a tartalmát, és ha minden rendben ment, a szakaszkulcs segítségével már indulhat a titkosított kommunikáció. A hitelesítő visszaküldésével az ügyfél és a kiszolgáló azonosították egymást.



Kerberos azonosítás (S_{AB} a KDC által a kapcsolathoz generált szakaszkulcs, K_B a kiszolgáló hosszú távú kulcsa)

A megoldás másik előnye, hogy az egyes kiszolgálóra szóló jegyek újrafelhasználhatók, tehát az ügyfélnek nem kell minden kapcsolat előtt a KDC-hez fordulnia. A biztonság érdekében azonban minden jegy csak egy adott ideig érvényes (ez az idő alapértelmezésben általában 8 óra), melyet a jegy adatmezőjében tárolunk. Az érvényességi idő lejárta után az ügyfél kénytelen lesz megújítani a jegyet. Ha az ügyfél kilép a rendszerből, a számítógépén tárolt jegyek elvesznek, tehát belépéskor mindenképpen szükség lesz új szakaszjegyek kérésére.

Jegy a jegyekhez (Ticket-Granting Ticket – TGT)

A felhasználók hosszú távú kulcsát a jelszóból állítják elő, mégpedig egy egyirányú titkosító, úgynevezett hash-algoritmus segítségével. A KDC adatbázisában megtalálható az összes tartományi felhasználó és számítógép hosszú távú kulcsa. Amikor Aliz a munkaállomásán bejelentkezik, az általa beírt jelszóból előáll egy kulcs, amit a bejelentkezéshez használni fog. A KDC ugyanezt a kulcsot a saját adatbázisából veszi, így lesz képes azonosítani a felhasználót.

A hosszú távú kulcsot egy munkamenetben mindössze egyszer állítják elő, mégpedig akkor, amikor a felhasználó először bejelentkezik a rendszerbe. A bejelentkezés után a felhasználó kap egy speciális szakaszjegyet, amit azután minden kapcsolat felépítéséhez és kezdeményezéséhez használhat (és használnia is kell).

A KDC az, aki az ügyfél és a kiszolgálók közötti azonosítást lehetővé teszi. Az ügyfél tehát, mielőtt a kiszolgálóhoz menne, a KDC segítségére szorul (szakaszjegyet kell kérnie tőle a kiszolgálóhoz), ezért a legelső szakaszjegy, amire az ügyfélnek szüksége van, magához a KDC-hez szól, hogy ezentúl ne kelljen a hosszú távú kulcsot használva azonosítania magát.
Ez a speciális szakaszjegy a Ticket-Granting Ticket (TGT), azaz a jegy a jegyekhez. Az ügyfél a bejelentkezés után ennek a jegynek a bemutatásával kérhet további szakaszjegyeket a KDC-től. A TGT egyébként teljesen hasonló az általános szakaszjegyekhez, hiszen tulajdonképpen ez is csak egy jegy egy szolgáltatáshoz (mégpedig a KDC jegyárusához).

Amikor tehát a felhasználó azonosítása megtörtént, a KDC a további jegyek kiadásához generál Aliz számára egy szakaszkulcsot (ez a bejelentkezési szakaszkulcs, logon session key). Ezt a szakaszkulcsot a felhasználóra vonatkozó adatokkal együtt becsomagolja és a saját hosszú távú kulcsával titkosítja. Ez a titkosított adatcsomag maga a TGT. Látható, hogy a felhasználó a TGT-t se elolvasni, se módosítani nem tudja, hiszen azt a KDC titkosította. A KDC ezután a szakaszkulcsot betitkosítja a felhasználó hosszú távú kulcsával is (hiszen a kulcshoz azért neki is hozzá kell férnie), és néhány TGT-re vonatkozó információ mellett az egész csomagot visszaküldi a felhasználónak.

Az ügyfél tehát válaszul kap egy csomagot, ami két részből áll: az első rész a felhasználó saját hosszú távú kulcsával titkosított információ és a szakaszkulcs egy példánya, amit a KDC-vel való további kapcsolatok titkosítására majd felhasználhat. A második rész a KDC kulcsával titkosított TGT, amivel pedig azonosíthatja magát. Az ügyfél a dekódolt szakaszkulcsot, az adatokat, és magát a TGT-t biztos helyre menti.
A felhasználó jelszavát és hosszú távú kulcsát ekkor el is felejthetjük, hiszen a KDC felé a TGT, más kiszolgálók felé pedig a KDC-től kapott szakaszjegyek segítségével jöhet létre a kapcsolat.

Hitelesítés tartományok között

A KDC feladata kettős: egyrészt hitelesítő szolgáltatás (Authentication Service) TGT-ket gyárt, másrészt a jegykiszolgáló (Ticket-Granting Service) a már TGT-vel jelentkező ügyfelek részére szakaszjegyeket gyárt. Ez a kettősség teszi lehetővé, hogy a Kerberos azonosítás tartományi határokat átlépve is működhessen. Lehetséges, hogy az ügyfél az egyik tartomány KDC-jétől kapott TGT segítségével egy másik tartomány KDC-jétől kérjen szakaszjegyet egy szolgáltatáshoz. A KDC szakaszjegyeket mindig csak a saját tartományába tartozó szolgáltatásokhoz adhat, hiszen csak a saját tartományában található felhasználók és számítógépek hosszú távú kulcsával rendelkezik.

Ha azt szeretnénk, hogy a két tartomány között létrejöhessen Kerberos hitelesítés, a tartományok között is meg kell osztanunk egy közös titkot, egy speciális kulcsot. Ez a tartományok közötti kulcs, az inter-domain key.

A Windows 2003 a tartományok közvetlen megbízotti viszonyának kialakításakor ezt a tartományok közötti Kerberos kulcsot is létrehozza. Az egymással közvetlen megbízotti viszonyban álló Windows 2003 tartományok tehát rendelkeznek közös tartományok közötti kulccsal.

Alprotokollok

A Kerberos protokoll valójában három alprotokollból áll:

- **Authentication Service Exchange (AS):** hitelesítő szolgáltatás, ez azonosítja a felhasználót és állítja elő számára a TGT-t.
- **Ticket-Granting Service Exchange (TGS):** a jegykiszolgáló szolgáltatás, ami az érvényes TGT-ket bemutató ügyfelek számára más szolgáltatásokhoz érvényes szakaszjegyeket készít.
- **Client/Server Exchange (CS):** az ügyfél és a kiszolgáló közötti azonosítás, a TGS-től kapott szakaszjegy alapján.

Mint ahogy bemutattam, a Kerberos hitelesítés elég bonyolult, és nehéz lenne akár egy olyan pontot is találni rajta, ami akárcsak egy kicsi támadási lehetőséget is hagyna a támadóknak.

4. Hálózatbiztonság

A számítógép-hálózatok és a különböző hálózati szolgáltatások rohamos terjedése miatt egyre fontosabb szerepet kap a hálózaton mozgó adatok biztosítása. A különböző támadások jelentős része hálózaton belülről érkezik, ezért van nagy jelentősége a biztonságos adatátvitelnek. Vannak olyan hálózatok, ahol annyira túlsúlyban vannak ezek a belső támadások, hogy nem is üzemeltetnek tűzfalakat, hanem inkább az adatokat védik. A Microsoft Windows-ban sok olyan lehetőség van, amelyek megoldást biztosítanak ezen a területen is.

4.1 Hálózati protokollok

A Windows 2003 alapértelmezett protokollja a TCP/IP. A TCP/IP több protokoll gyűjteménye, alapszolgáltatásait az IP, ARP, ICMP, IGMP, TCP és az UDP protokollok adják. Feladata, hogy két számítógép között adatokat továbbítson több hálózati szegmensen keresztül. A protokoll az egyes gépekhez egy címet rendel, ez az IP cím. Alapvetően unicast felépítésű, azaz egy gép kezdeményezi a forgalmat és a másik gép a fogadó, tehát egy-egy a kapcsolat alapja. Azonban a korszerű hálózatokban egyre jelentősebb a multicast forgalom is. Ez egy speciális címtartományú forgalmat jelent, az adatforgalom itt is egy gépből indul ki, de jellemzően több gép is részt vesz a csomagok vételében. A TCP/IP routolható, ami azt jelenti, hogy több részhálózatot útválasztókkal kapcsolhatunk össze, és útválasztáskor a protokoll tulajdonságai alapján eldönthető, hogy melyik irányba kell továbbítani a csomagot. A Windows 2003 is lehet ilyen útválasztó abban az esetben, ha több hálózati kártya van a szerverben, azonban az útválasztást külön konfigurálni kell.

4.2 A biztonság és a Windows Server 2003

A Microsoft Windows Server 2003-ban felhasználható megoldások a TCP/IP protokollrendszer különböző szintjein működnek, és különböző területeken használhatók. A legegyszerűbb TCP/IP biztonsági beállítás a csomagszűrés (packet filtering). Használatával beállíthatjuk, mely protokollokat, mely címekről engedélyezünk, illetve mely protokollokat mely címek felé engedélyezünk. A csomagszűrést beállíthatjuk az IP csomagoknál a protokoll típus szerint (kivétel ez alól az IPSec, ICMP, IGMP, UDP protokoll), valamint TCP/UDP port szám alapján.
A másik lehetséges módszer az IP Security (IPSec). Ennek használata esetén azonban fontos megjegyezni, hogy viszonylag nagy rendszer-erőforrásokat igényel a titkosítás kódolása és dekódolása miatt.
IPSec-et az alábbi fontosabb esetekben célszerű használni:

- Két kliens közötti kapcsolat, ahol az adatok titkosítottak.
- Szervereken tárolt bizalmas információk esetén a szerver és a kliensek között.
- Távoli elérés esetén, betárcsázós vagy VPN kapcsolat esetén.
- WAN kapcsolat esetén a két útválasztó közötti kapcsolat titkosítására.

A TCP/IP négy rétegű modelljében az alkalmazás, az adattovábbítás, az internet, és a hálózati réteg épül egymásra. Az IPSec az adattovábbítási rétegen működik. Ennek az a legfőbb előnye, hogy bármilyen, felsőbb rétegen működő alkalmazás adatai védhetők vele. Hasonló biztonsági szolgáltatások az alkalmazási rétegen is rendelkezésre állnak. Ezek közül az egyik legfontosabb a Secure Socket Layer (SSL), amit annak az alkalmazásnak is támogatni kell, amelynek adatait ily módon kezeljük.

4.3 Az IP Security

A belső hálózatok manapság az IP protokollt használják. A hálózaton utazó csomagok sokféle támadási felületet hagynak, ezek ellen az IP Security (IPSec) nyújthat védelmet. Ez egy szabványos megoldás, ami azt jelenti, hogy nem csak a Microsoft kliensekkel képes együttműködni, hanem más rendszerek is használhatják az IPSec szolgáltatásokat. Sokféle

támadás ellen nyújt védelmet, azonban hátránya ennek a megoldásnak, hogy az adatok teljes mértékben titkosítva közlekednek, amelyet a tűzfalak nem képesek értelmezni.
Az IPSec protokoll kétféle megoldást biztosít. Egyik az autentikációs fejléc megoldás (Authentication Header - AH), amely csak végpont azonosítást biztosít. A másik megoldás az Encapsulating Security Payloads (ESP), amely már titkosítást is biztosít, tehát további biztonsági problémák ellen is véd. Az IPSec megoldások kétféle üzemmódban használhatók. Transzport módban az adatok végponttól végpontig védettek, míg csatorna üzemmódban csak az út egy részén védi az adatokat az IPSec.
Az IPSec tűzfalon keresztüli átengedéséhez szükség van a forrás és cél számítógép IP címeire, valamint az alábbi protokollokat és portokat kell átengedni a megfelelő irányban:

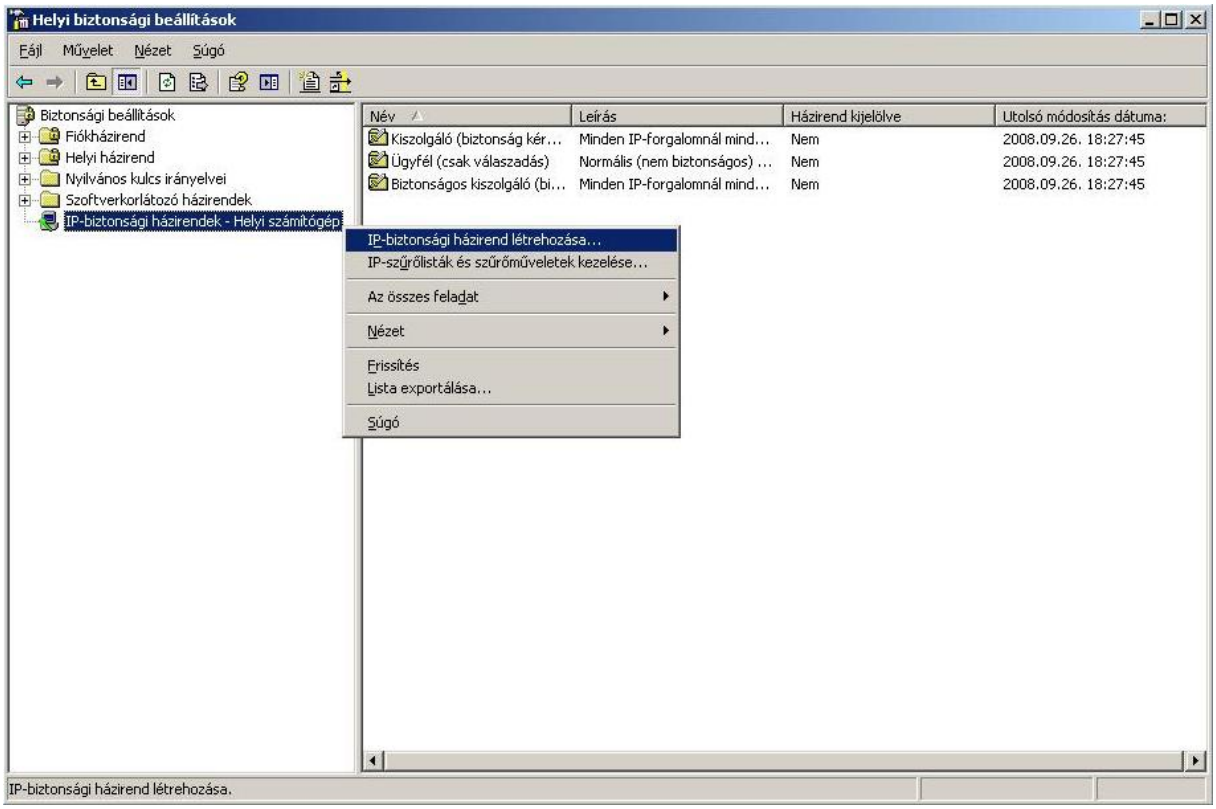
- IP 50 (0x32) port, amely az ESP forgalom
- IP 51 (0x33) port, amely az AH forgalom
- UDP 500 (0x1F4) port, amely az Internet Key Exchange (IKE) forgalom

IPSec beállítások
Az IPSec beállítását kliens és szerver rendszereknél is a biztonsági házirendek (Security Policy) alatt tudjuk megtenni. IPSec házirendet kell létrehozni, majd pedig hozzárendelni a számítógéphez. Ezek a beállítások tartományi környezetben, a csoportházirendek segítségével is beállíthatók.
A Microsoft rendszerekben három előre definiált házirend található, ezek általános beállításokat tartalmaznak, és könnyen felhasználhatók:

- A szerver (Server - Request Security) házirend igényli a biztonságos kommunikáció használatát, de ha a kliens nem képes rá, akkor nyílt kommunikációra is képes.

- A kliens (Client - Respond Only) beállítások nem írják elő az IPSec használatát, de a rendszer válaszol minden ilyen jellegű kérésre.

- A biztonságos szerver (Secure Server - Request Security) kizárólag IPSec segítségével forgalmaz a hálózaton, ha a kliens erre nem képes, akkor nem épül fel kapcsolat.



Az IPSec házirendek IPSec szűrőkből épülnek fel. Új házirend kialakításakor szűrőket kell megadni, amelyek a különböző típusú adatforgalom kezeléséről rendelkeznek. A szűrő paramétere a forrás és cél számítógép IP címe, a protokoll típusa, és a forrás illetve cél TCP vagy UDP port száma. Ezekkel a beállításokkal szelektív IPSec beállítások adhatók meg.

5. Biztonsági frissítések

A szoftverekben létező biztonsági réseket kihasználó támadások szolgáltatások bénítására, adatok megszerzésére irányulnak. A biztonsági szoftverfrissítések folyamatos telepítésével lehet kivédeni ezt a támadást.
A vírusok az egyik legkomolyabb fenyegetettséget jelentik a rendszerünkre. Különböző típusai vannak, de egyéb, vírusokhoz hasonló fenyegetettséget jelentenek a különböző trójai falovak, férgek is.
Talán az egyik legfontosabb eleme egy számítógép működésének, hogy a naponta vagy hetente megjelenő különféle vírus-variánsok és férgek ellen hatékonyan lépjünk fel. Nyilvánvaló, hogy egy vírusellenőrző program egymagában nem nyújt megfelelő védelmet.

Többféle megoldást alkalmazhatunk a biztonsági frissítések kezelésére:

- **Windows Update (WU):** az internetről, a Microsoft weblapjáról való letöltés. Ennek utódja a Microsoft Update (MU) szolgáltatás, amely több Microsoft termékhez szolgáltat frissítéseket, nem csupán a Windows-hoz.

- **Microsoft Baseline Security Analyzer (MBSA):** ez egy segédprogram, amellyel a gépünk biztonsági frissítését ellenőrizhetjük.

- **Windows Server Update Services (WSUS):** segítségével megoldható az elosztott frissítés.

- **System Management Server (SMS):** nagyvállalati deszktop felügyeleti megoldás, amely a frissítéseket kezeli.

5.1 Windows Update

A legegyszerűbb megoldást a Windows Update webfelületének használata jelenti, amelyet két helyről is megnyithatunk. Egyrészt a Start menüben találunk egy Windows Update ikont, másrészt az Internet Explorer eszközök (tools) menüpontja alatt szintén megtalálhatjuk. Ezután megnyílik a kívánt weboldal, ahol egy ActiveX vezérlő segítségével folyik a kommunikáció első része, amely továbbítja a Windows Update webhely felé a számítógépünk aktuális állapotát. Az állapot elemzését követően kapunk egy listát, hogy melyek a kritikus frissítések, és milyen további frissítések letöltése javasolt még.

A Windows Update paraméterezése
A beállításokat a Vezérlőpult – Automatikus frissítések pontjában végezhetjük el. Alapértelmezésben ez a funkció be van kapcsolva.

Négy választási lehetőségünk van:

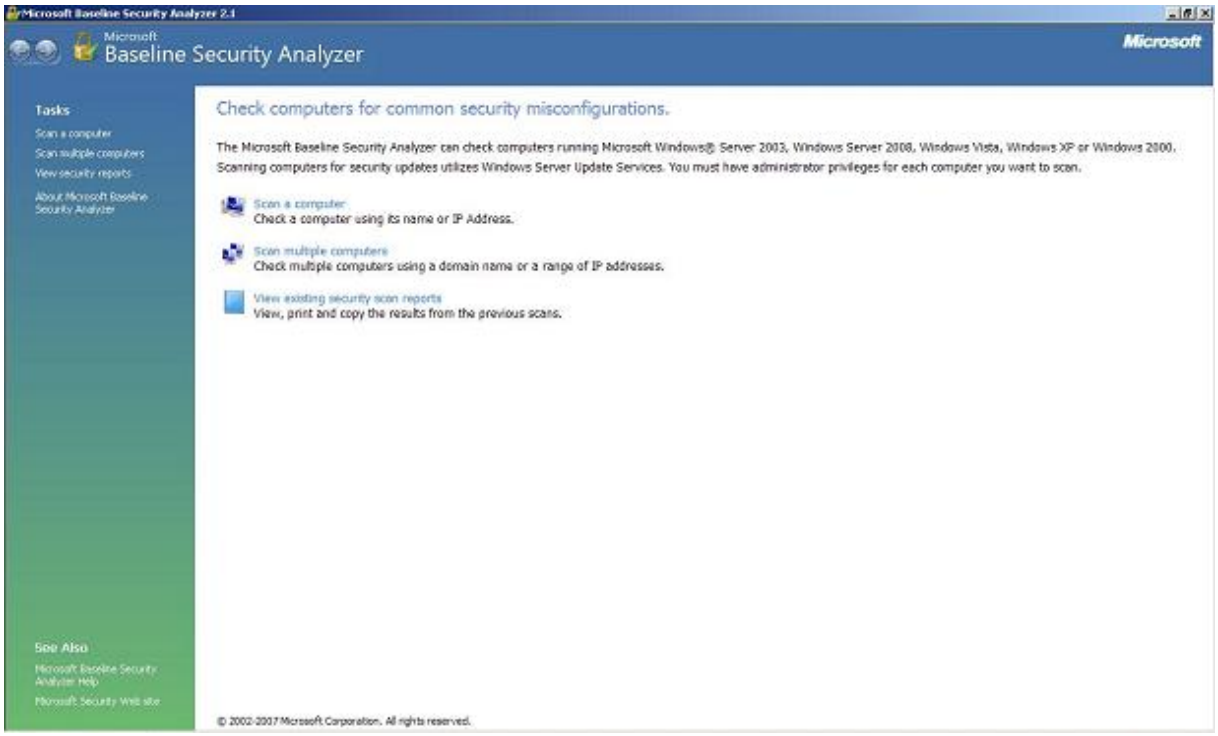
- Automatikus beállítás, megadott időszakonként, megadott időpontban.
- Letölti a frissítést, majd értesít minket, ha készen áll a telepítésre. (manuális telepítés)
- Értesít, ha új frissítés jelenik meg. (a letöltés és a telepítés is manuálisan történik)
- Automatikus frissítés kikapcsolása.

5.2 Microsoft Baseline Security Analyzer (MBSA)

A javítócsomagok és rendszerünk aktuális állapotának megvizsgálásához szükség van egy olyan eszközre, amely megmondja, hogy elegendő-e az általunk telepített csomagok mennyisége. Ennek a felderítéséhez a legkézenfekvőbb megoldás, ha letöltjük a Microsoft honlapjáról elérhető MBSA eszközt. A Windows Server termékei mellett asztali operációs rendszerekre is telepíthetjük akár.

A Microsoft Baseline Security Analyzer nemcsak az operációs rendszert, hanem a meglévő más Microsoft termékek aktuális frissítettségét is ellenőrzi. Kivétel ez alól az Office alkalmazás, melyet csak a lokális gépre bejelentkezve és azon futtatott MBSA eszközzel ellenőrizhetünk.

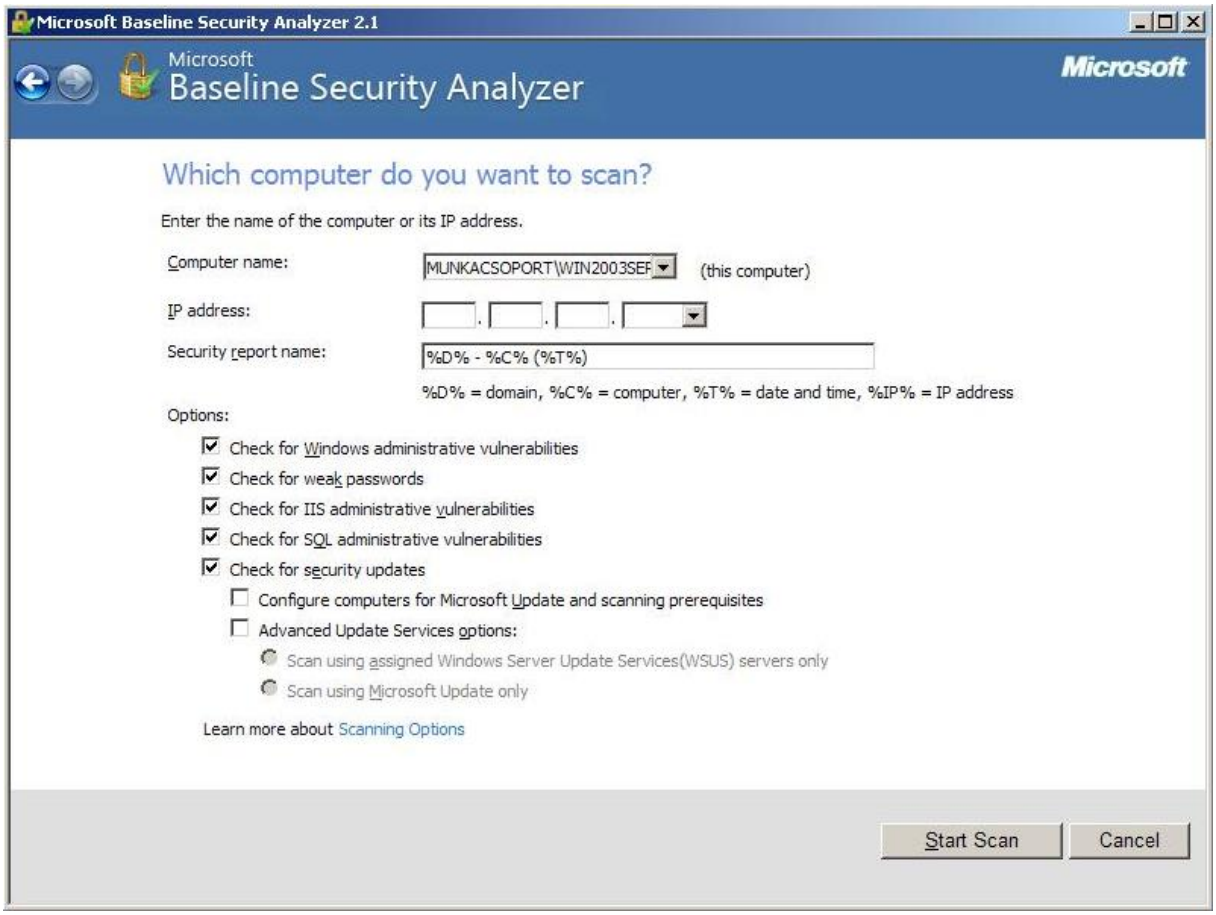
Az MBSA csomagot letöltve és telepítve az alábbi lehetőségek közül választhatunk:



- **Scan a computer:** egy számítógépet választhatunk ki név vagy IP cím alapján, amin a létező összes Microsoft komponens, illetve a biztonsági rések felderítése történik meg.

- **Scan multiple computers:** egyszerre több számítógépet lehet kiválasztani tartomány név vagy IP tartomány alapján.

- **View existing security scan reports:** a már lefuttatott ellenőrzések összegzését tekinthetjük meg. Különböző szűrési lehetőségeink vannak időrend, számítógép neve, vagy IP címe alapján.

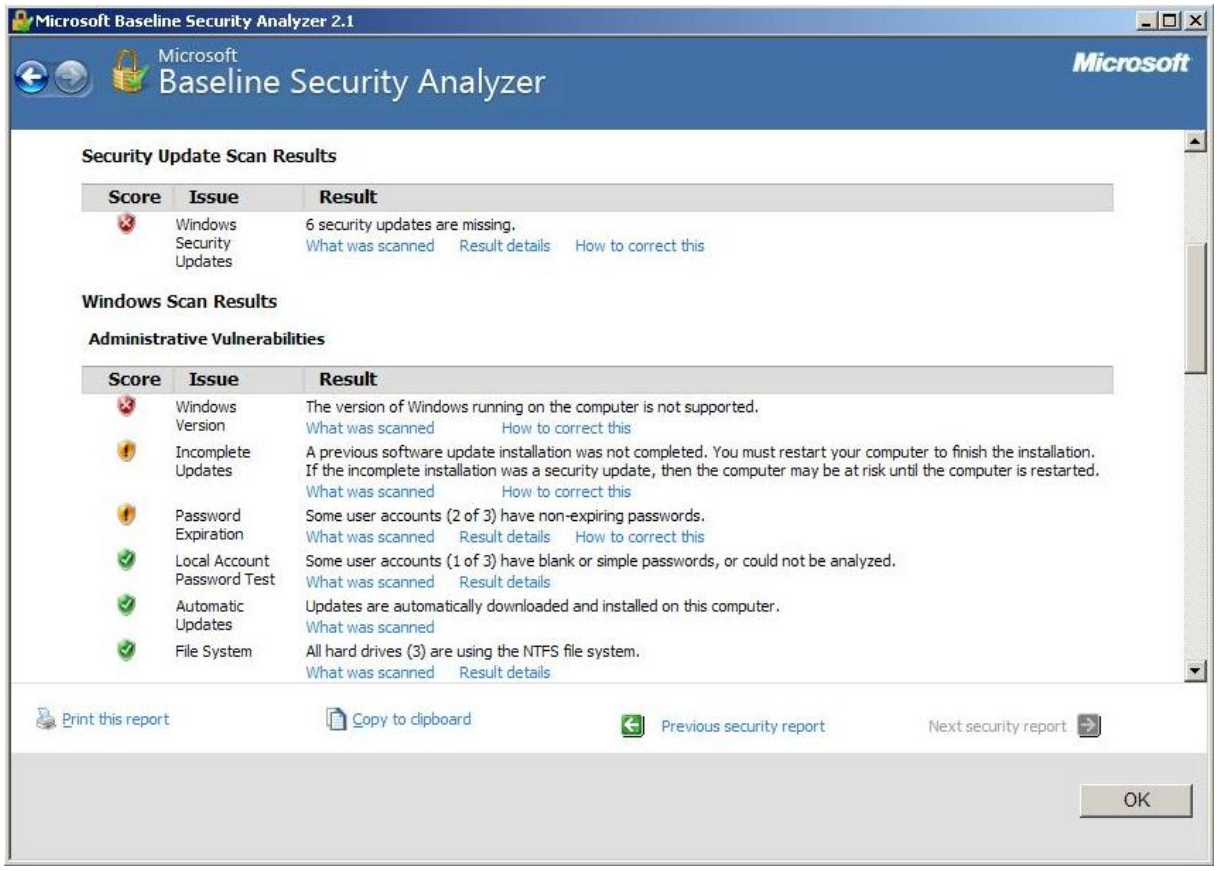


Az ellenőrzés elvégzéséhez szükség van egy referencia adatbázisra, amivel összehasonlíthatja, hogy a gépünk jelenlegi állapota mihez képest jó vagy rossz. Ez lehet a Windows Update weboldala, vagy akár lokális WSUS szerverünk. A program egyébként parancssori módban is futtatható, ami természetesen gyorsabb, mint a grafikus felület.

Néhány fontosabb dolog, amit az MBSA vizsgál:

- Windows sebezhetősége
- Gyenge jelszó
- Biztonsági frissítések állapota
- Internet Explorer biztonsági beállításai
- SQL
- Internet Information Services biztonsági beállításai
- Lokális gépen futtatva az Office termékeket

Az alábbi ábrán egy ilyen vizsgálat eredményét láthatjuk, ahol a felderített fenyegetettségek szerepelnek:



MBSA 2.1

Jelenleg ez a verzió a legfrissebb, amit le tudunk tölteni a Microsoft honlapjáról. Legfontosabb tulajdonsága, hogy a WSUS-sal kompatibilis, azaz képes kezelni a WSUS frissítési adatbázisát. Képes kezelni a 64 bites Windows verziókat is. A következőkben néhány oldalban ismertetném a WSUS szolgáltatást is.

5.3 Windows Server Update Services (WSUS)

A Microsoft honlapjáról ingyen letölthető termék, amely egy arra alkalmas számítógépre telepítve tulajdonképpen lokális Windows Update szolgáltatásként működik. Ennek köszönhetően képes a Windows 2000, és e feletti rendszerek számára a beállított és letöltött frissítéseket telepíteni. A WSUS telepítése egyébként önmagában nem elegendő, hiszen csoportházirend segítségével tudjuk a hálózaton lévő számítógépek számára beállítani a szolgáltatás kötelező használatát.

A WSUS a SUS továbbfejlesztett változata, mely képes a számítógépek telepítettségét ellenőrizni, a szükséges frissítéseket telepíteni, visszavonni, elutasítani. Csak olyan szerver termékre tudjuk telepíteni, amelyen fut az IIS Web szerver. Minimális követelmény az IISv5, tehát Windows 2000 szerver, vagy e feletti szerver termékek jöhetnek szóba. A korábbi SUS továbbfejlesztéseként már nem csak az alapértelmezett webhely mellé települ, hanem meg lehet adni egy másikat is. A Microsoft honlapján található ajánlás szerint 500 felhasználó alatt minimum Pentium III 750 MHz-es processzor (1 GHz-es ajánlott), és 512 MB RAM (1 GB ajánlott) szükségeltetik. 500 felhasználó felett 1 GHz-es Pentium III vagy nagyobb processzor, illetve minimálisan 1 GB RAM szükséges. Ezek mellett akár több tíz GB tárterületre is szükség lehet. Mivel a fontos információk SQL adatbázisban tárolódnak, ezért vagy a szerverre telepít egy MSDE motort (Microsoft SQL Server Desktop Engine), vagy egy meglévő SQL szervert használ fel.

A WSUS topológiák az alábbi szerint alakulhatnak:

- **Egyetlen WSUS szerver:** Az internetre kapcsolódó WSUS szerver tölti le a frissítéseket, a kliensek telepítését csoportok szerint engedélyezhetjük, miután letöltődtek a beállított frissítések.
- **Több, egymástól független WSUS szerver:** Lehetőség van több, különálló szervert is üzemeltetni. A két szerver nem szinkronizálja az adatait. Akkor érdemes ilyet használnunk, ha nagy hálózatunk van. Az egyik szerver lesz a felelős például a Windows XP kliensekért, a második pedig az esetlegesen más operációs rendszert futtató gépekért (Windows 2000, Vista).
- **Több, egymással összekapcsolt szerver:** Az előző megoldáshoz hasonló, de itt már több WSUS szervert használunk, például földrajzi elhelyezkedés, vagy más okból. Ilyenkor egy WSUS szerver tölti le a frissítéseket, majd továbbítja a többieknek.

Telepítés

A telepítőkészlet letölthető a Microsoft letöltő központjából. Windows 2003 szerver esetén előfeltétel a telepített IIS 6, és a .NET Framework 2.0. Ezeket egyébként a Windows-összetevők varázsló segítségével szükség szerint telepíthetjük.

Az üdvözlőképernyő után a telepítő a biztonsági frissítések tároló helyét kérdezi. Alapértelmezés a helyi tárolás. A megadott mappának NTFS formázottnak kell lennie, és legalább 6 GB méretű szabad hely szükséges.

Mivel a WSUS SQL szerveren tárolja az adatbázist, ezért a következő képernyőnél vagy egy meglévő szervert kell beállítani, vagy a települő SQL Server Desktop Engine helyét kell megadni. Az előzőhöz hasonlóan a megadott mappának itt is NTFS formázott köteten kell lennie, és legalább 2 GB méretű szabad hely szükséges, helyben tárolt frissítések esetén természetesen ez már 8 GB.

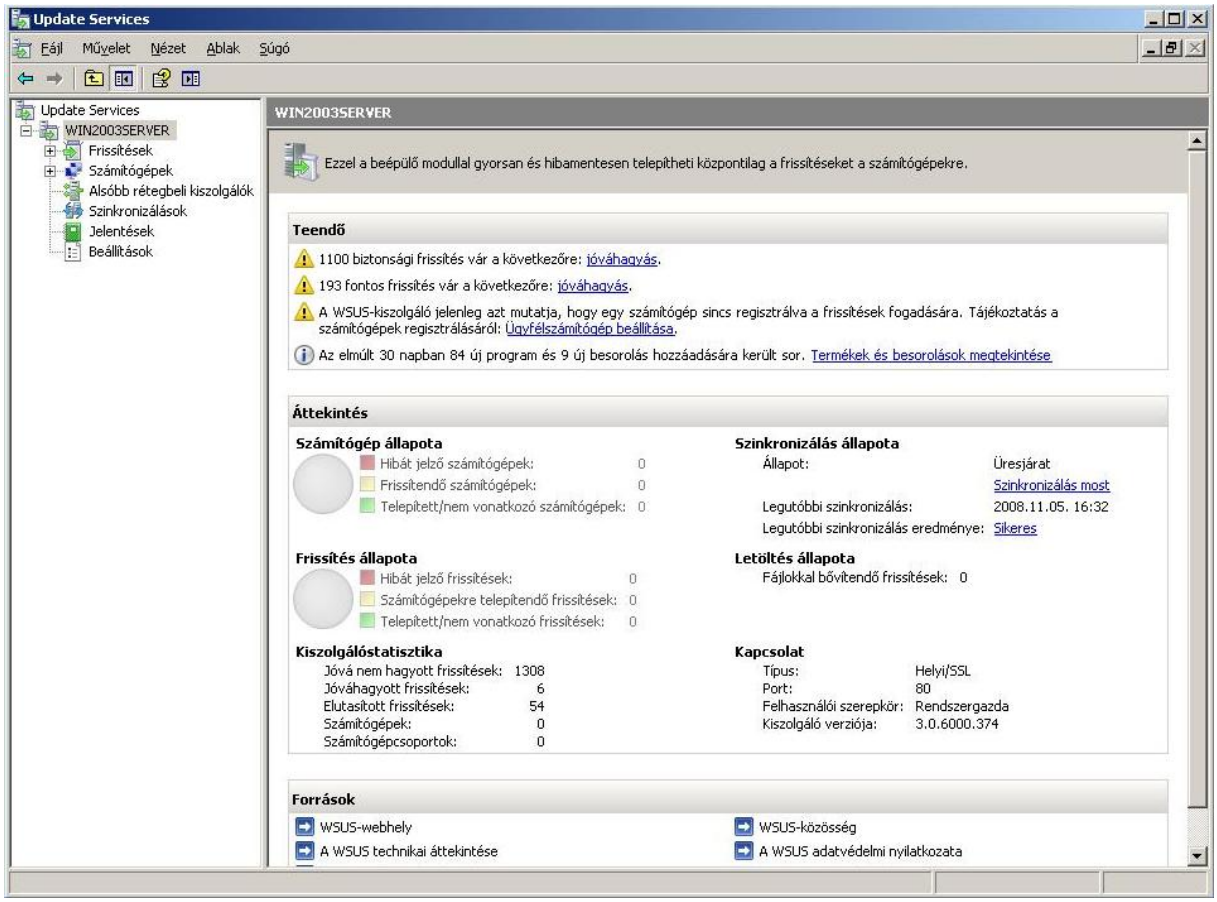
Ezután következik az IIS beállítása. Vagy az alapértelmezett weblapon hozzuk létre, vagy külön helyet hozunk létre a WSUS számára.

A következő lépésben a tűzfalat kell konfigurálni, hogy a WSUS működni tudjon. Engedélyezni kell a 80-as (HTTP) és 443-as (HTTPS) portokat. Ha a Windows saját belső tűzfalát használjuk, akkor azt nem kell konfigurálni, mivel a kapcsolatot a WSUS kezdeményezi, amit a belső tűzfal átenged.

A következő beállításokat akkor kell figyelembe venni, ha már van másik, telepített WSUS szerver, és azt szeretnénk, ha az új szerver innen frissítene. Ekkor meg kell adnunk a kiszolgáló nevét és port számát. Az alapértelmezés egyébként a Microsoft Update webhellyel való szinkronizáció.

Ezek után, ha szükséges, akkor proxykiszolgálót adhatunk meg, majd beállíthatjuk a frissítés nyelvét is. A következőkben ezután kiválaszthatjuk azokat a termékeket, amelyeket frissíteni szeretnénk, illetve megadhatjuk a szinkronizálás fajtáját is (manuális vagy automatikus).

A telepítés végeztével elindíthatjuk a felügyeleti konzolt, illetve megindulhat az első szinkronizáció is.



A WSUS felügyeleti konzolja

A Frissítések nézet összegzi a frissítések jelenlegi állapotát.

A Szinkronizálások pontban nézhetjük meg a jelenleg is folyamatban lévő, illetve a már elvégzett sikeres szinkronizálások adatait.

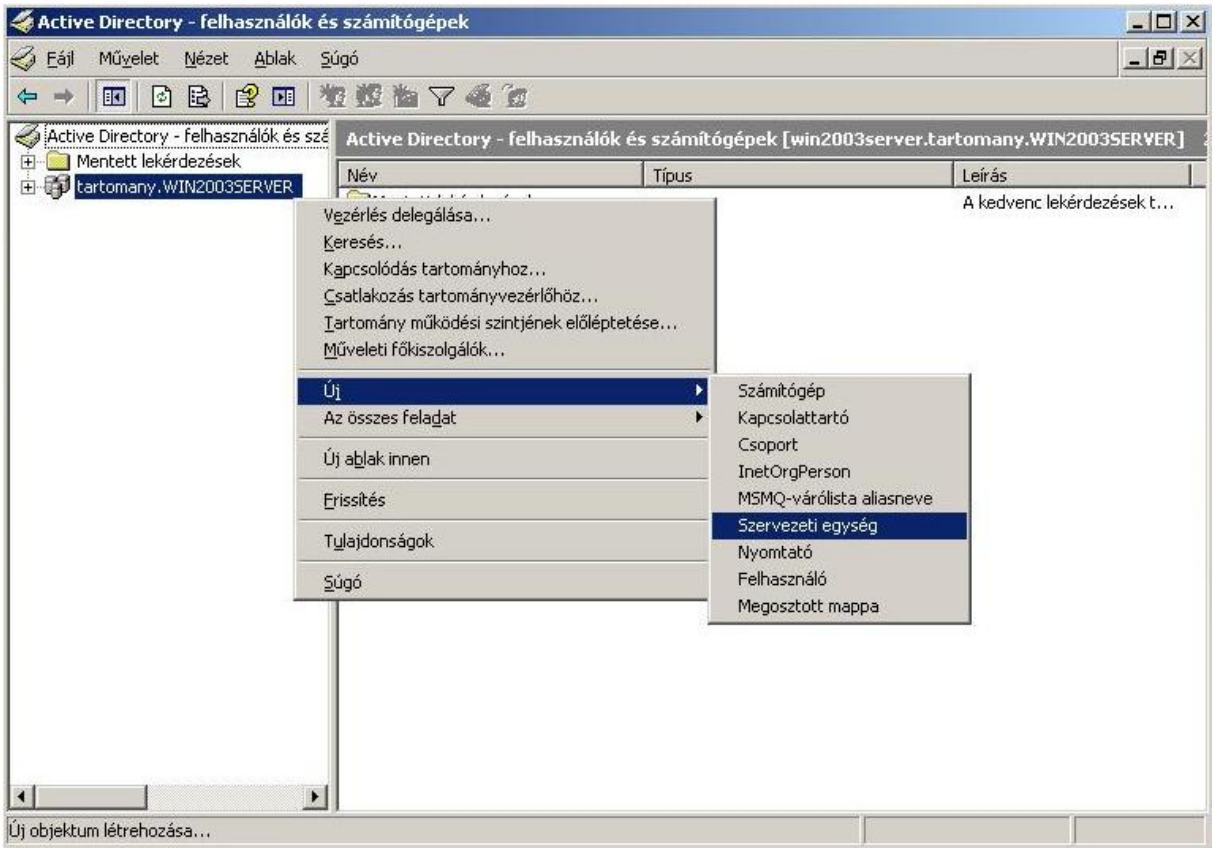
A Jelentések nézetben különböző elérhető jelentéseket tekinthetünk meg: frissítési-, számítógép-, és szinkronizálási jelentések láthatóak.

A Beállítások pontban különféle frissítéssel, szinkronizációval, és más egyéb beállításokkal találkozhatunk.

A WSUS konfigurálása

Mint ahogyan a bevezetőben már említettem, a WSUS szerver telepítése egymagában nem elegendő. A klienseken be kell állítani, hogy ne a Windows Update szerverről kapják a továbbiakban a frissítéseket. A csoportházirendet hívjuk segítségül. Mivel csoportházirendről van szó, természetesen csak tartományba kötött gépeknél fog működni.

A csoportházirend elemei közé fel kell vennünk a WSUS elemeit. Először is létrehozunk egy szervezeti egységet, ahová átmozgatjuk a munkaállomásokat és szervereket. Majd a szervezeti egységhez tartozó csoportházirendet megnyitjuk, és mivel itt még nincs házirend, ezért hozzáadunk egyet, ami a WSUS beállításokat fogja tartalmazni. Ezután a létrehozott új házirendhez készítünk egy sablont, amelyhez hozzáadjuk a wuau.adm állományt. Ezzel a sablon be is került a csoportházirendbe.



6. Tűzfalak

A tűzfal (firewall) célja annak biztosítása, hogy illetéktelen személyek a hálózaton keresztül ne hatolhassanak be rendszerünkbe, olyan szoftveres, vagy hardvereszköz, amelynek segítségével belső hálózatunkat megvédhetjük a külső hálózatról érkező betörések ellen.

Azt hiszem, hogy egy mindenki számára ismert eszközről van szó, ezért nem szentelnék most időt ennek részletes bemutatására. Azonban van annyira fontos, hogy nem mehetünk el mellette szó nélkül. Mivel dolgozatom témája a Windows Server 2003, így néhány oldalban azért bemutatnám, hogy milyen lehetőségeink is vannak ezen a rendszeren.

6.1 Internet Connection Firewall (ICF)

Az ICF a Windows Server 2003, és emellett a Windows XP beépített tűzfalprogramja. Ez egy állapotérzékeny tűzfal, csak a bejövő forgalom blokkolására képes. A tűzfalat a Vezérlőpult – Windows tűzfal ikonra való kattintással nyithatjuk meg.

Ha bekapcsoljuk, akkor minden kívülről jövő forgalmat letilt, ami a szerver felé irányul, kivéve a megadott kivételeket persze. A kivételek fülön megtaláljuk alapértelmezésben például a fájl- és nyomtatómegosztás, és a távoli kapcsolat engedélyezését. Ezeket módosíthatjuk, vagy akár felvehetünk új portokat is. Megadhatunk IP címtartományt is, vagy egyedi címeket, amelyekre érvényes lesz a beállítás. Megadhatjuk azt is, hogy értesítsen-e minket a rendszer, ha a tűzfal blokkolt egy programot.

A beépített tűzfal a rendszer része, azonban elég korlátozott beállítási lehetőségekkel bír. Ha a hálózatunkat védeni akarjuk, akkor valódi tűzfalra van szükség.

6.2 Microsoft Internet Security and Acceleration Server (ISA)

Mint bemutattam, a Windows Server 2003 is számos biztonsági szolgáltatással rendelkezik, azonban egy teljes informatikai hálózat biztonsági problémáinak kezelésére ezek sem elegendőek.

A Microsoft 2000-ben jelentette meg ISA Server 2000 néven ismert tűzfalmegoldását, mely egyszerű felület segítségével tette lehetővé a hálózaton átfolyó csomagok útjának szabályozását. Azonban mint első generációs termék, ez is komoly hiányosságokkal rendelkezett, nem igazán volt képes felvenni a versenyt más platformokon elérhető

szoftverekkel. Az ISA Server 2004 már nem csak egyszerű kezelhetőségével, de aprólékos konfigurálási lehetőségei révén is erős ellenfele a konkurens termékeknek, és végre bármilyen hálózati topológiára alkalmazhatóak biztonsági szolgáltatásai.

Az ISA Server kétféle változatban kapható: Standard, illetve Enterprise Edition.

ISA 2004

Az ISA Server 2004 háromféle szabálytípust különböztet meg egymástól. Ezek határozzák meg a tűzfalon keresztül lefolytatott kommunikáció tulajdonságait:

- Az általános tűzfalképességek az *Access szabályokkal* használhatóak ki. Minden Access szabályhoz megadható, hogy a forráshálózatokból mely célhálózatokba, milyen protokollokra és feltételekre, milyen tartalomtípusra, és mely felhasználókra, csoportokra érvényesek. Ha a szabály engedélyező, akkor a leírt kommunikációt az ISA Server 2004 lehetővé teszi. Tiltó szabály esetén nincs lehetőség az adattovábbítás elvégzésére.
- *Server Publishing szabályok* a hálózati szerverek tűzfalbeállításainak meghatározására használhatóak. Az ISA Server 2004 engedélyezi a megadott hálózatok számára a szerver adott szolgáltatásaihoz tartozó hálózati erőforrások elérését. A szolgáltatások közül kiválasztható többek között a DNS Server, az IPSec Server, a Microsoft SQL Server, a levelezésre használt POP3, SMTP is.
- A harmadik csoportba a *Web Publishing szabályok* tartoznak. Ezekkel adható meg, hogy a hálózatok webszerverein futó honlapok milyen címen érhetőek el. A rendszer támogatja az SSL kommunikációt is, amit kétféleképpen lehet igénybe venni: az SSL Tunneling választásával az ISA Server 2004 egyszerűen továbbítja a célszervernek a kódolt lekérést, míg az SSL Bridging esetében a kódolt adatmennyiség tartalmának vizsgálatára is lehetőség nyílik.

A *Show System Policy* funkció segítségével megtekinthető az operációs rendszer által használt szabályok csoportja ugyanabban a listában, mint ahol a tűzfal szabályait felvesszük, és innen akár módosíthatóak is. Ezek a listaelemek nem tartoznak az eddig érintett három szabálycsoport egyikébe sem. A rendszerszabályok minden esetben a legnagyobb prioritásúak, ezért ezeket felüldefiniálni nem lehet.

Az *Administration Delegation* varázsló segítségével három különböző jogosultsági szintet állíthatunk be a rendszer felhasználóinak és csoportjainak: Basic Monitoring, Extended Monitoring és Full Administrator.

Az ISA Server 2004 egységes kezelést biztosít a Windows Server 2003 VPN csoportjainak adminisztrációjára is. A VPN (Virtual Private Network) olyan kívülről történő hálózati elérést biztosít az egyes számítógépek számára, amivel a szerverre történő bejelentkezés után a belső, védett hálózat erőforrásait is használhatják. Ilyenkor a becsatlakozó számítógépek saját IP címet kapnak a belső hálózatban, és ugyanolyan jogosultságok állíthatóak be rájuk, mint bármely belső hálózati gépre, erőforrásra.

Az ISA Server 2004 képes a *VPN karantén* technológiát is alkalmazni, ami egy többlépcsős beléptetési rendszert takar. Segítségével a VPN-en keresztül belépni szándékozó számítógép nem válik azonnal a belső hálózat részévé, hanem előbb a VPN karantén zónájába lép. A VPN karanténon belül található számítógépekhez egyedi elérési jogok adhatóak meg, így a VPN kliens a szervereket és erőforrásokat nem látja. A karanténba kerülés után az ISA Server megkísérelhet lefuttatni beállított biztonsági teszteket az érintett számítógépen, hogy ellenőrizze, megfelel-e a belépni szándékozó gép az általa támasztott követelményeknek. A rendszer megkövetelheti a tűzfal, vagy a legfrissebb patchek telepítését, esetleg a legújabb vírusdefiníciós fájlok meglétét, hogy az újonnan érkező szereplő ne fertőzhesse meg a belső hálózat többi számítógépét.

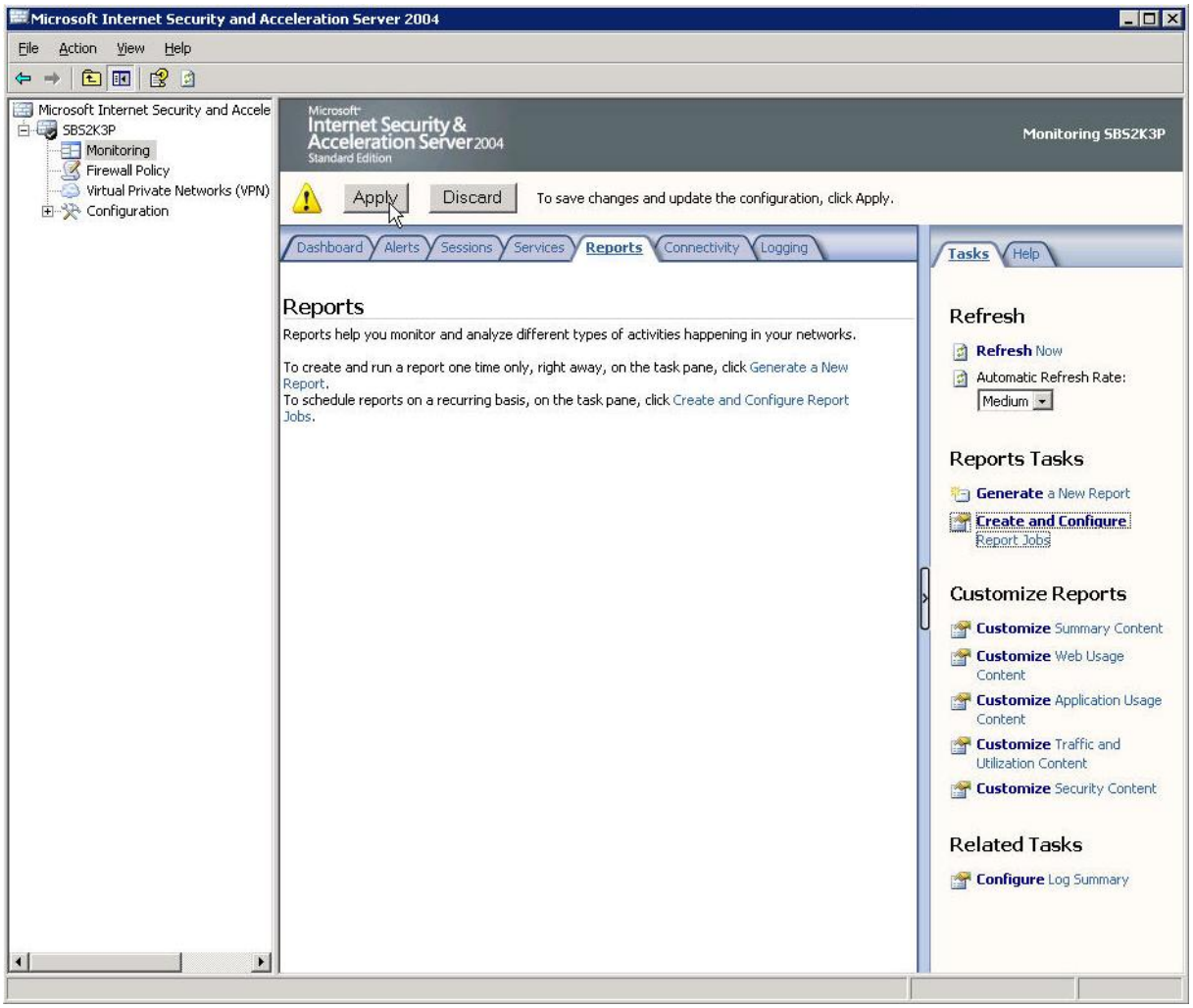
Amennyiben a VPN kliens a beállított időtartam alatt nem tudja biztonságosságát garantálni, a konfigurációtól függően kikerülhet a karanténból is. Ha azonban sikerül megfelelnie a követelményeknek, beléphet a belső hálózatra, és legközelebb már nem is szükséges ez a karantén.

A Microsoft ISA Server 2004-ben az aktuális adatok és események megtekintésére szolgál az alkalmazás *Dashboard* elnevezésű oldala. Itt egyszerre láthatóak a rendszert érintő legfontosabb állapotok, események és teljesítménymutatók.

A Microsoft IIS szolgál a legtöbb Windows szerver webszervereként, ezért az ISA Server 2004 tűzfalas megoldása ajánlott minden ilyen rendszerben, emellett számos újdonság is található a szoftverben, ami segíti a honlapok publikálását.

Lehetőségünk van jelentéseket készíteni, például megadott időtartamokról. Ezek tényleges elkészítéséért az ISA Server felelős. A naplózásnál jól használható felület segítségével oldható meg a lementett események szűrése és visszakeresése.

A Microsoft ISA Server 2004 segítségével komplex hálózati infrastruktúrák védelme is egyszerűen kivitelezhető.



7. A Windows Server 2008

A Windows Server 2008 a Windows Server 2003 operációs rendszer sikerére és erősségeire, valamint a Service Pack 1 csomagban és a Windows Server 2003 R2 kiadásban foglalt újdonságokra épül. A Microsoft idén év elején hivatalosan is bejelentette megjelenését.

A Microsoft Windows Server 2008 a Windows Server operációs rendszer következő generációját képviseli. Minden eddiginél biztonságosabb, megbízhatóbb és robusztusabb kiszolgáló környezetet eredményez. A Windows Server 2008 új előnye, hogy helytől függetlenül minden felhasználónak garantálja a hálózat minden szolgáltatásának elérését. A Windows Server 2008 ezen kívül részletes és alapos információkkal szolgál az operációs rendszerről, és diagnosztikai lehetőségeket is tartalmaz.

7.1 Újdonságok

A biztonság mindenekelőtt

A Windows Server 2008 a Windows Vistával közös kódbázisra épülő szervertermék. Fejlesztésénél nagy hangsúlyt fektettek a biztonságra, ez nem csak a fejlesztési folyamatra érvényes, hanem magát a terméket is úgy tervezték meg, hogy minimalizálják a kockázatokat.

A *szerep szerinti telepítés* segítségével a Windows Server 2008-nak csak azok a komponensei települnek, amelyek egy adott funkcióhoz valóban szükségesek, ezáltal csökken a lehetséges támadási felület. Ennek egyik példája a *Server Core telepítés*, amikor csak néhány szerepkör elérhető, még grafikus kezelőfelület sem fut. Ennek a megoldásnak az erőforrásigény csökkentése mellett a lehető legnagyobb biztonság elérése a célja, a felesleges komponensek minimumra csökkentésével.

Szintén a biztonságot hivatott növelni a *csak olvasható tartományvezérlő (Read-only Domain Controller)* bevezetése. Ha a tartományvezérlő csak olvasható, nem lehet az adatait helyben

módosítani, így kizárható annak lehetősége, hogy valaki a szerver feltörésével és az Active Directory erdő (forest) módosításával jogosultságokat szerezzen. További új biztonsági funkció, hogy az *Active Directory objektumainak módosításai naplózhatók*, így később visszakereshetők, ellenőrizhetők. Újdonság még, hogy a tartományban az egyes csoportokhoz akár *eltérő jelszóházirendek* is kialakíthatók.

A Windows Server 2008 már támogatja a *Network Access Protection*-t (NAP). A NAP a nem megfelelően konfigurált gépeket (pl. elavult operációs rendszer, régi vírusirtó) nem engedi fel a hálózatra egészen addig, amíg a szoftvereket nem frissítették a kívánt verzióra. Az adminisztrátorok természetesen maguk határozhatják meg, hogy milyen szempontok alapján akarják engedélyezni vagy szűrni a hálózati hozzáférést.

Az új Windows Server fontos újdonsága a *továbbfejlesztett terminálszolgáltatás*, amely már támogatja a Remote Desktop Prorocol (RDP) 6.0-t. A Windows Server 2008 képes RDP-n keresztül akár egyetlen alkalmazás képernyőjét is megosztani, nem csak az egész felhasználói felületet. A Terminal Services Gateway lehetővé teszi számítógépek csatlakozását Terminal Server-en vagy RDP-n keresztül HTTPS kapcsolatot használva, VPN nélkül, vagyis a HTTPS mellett nem kell további portokat nyitni a tűzfalon, ami szintén a biztonságot hivatott fokozni. A Terminal Services Web Access segítségével a terminálszolgáltatás webes interfészen keresztül is elérhető.

A szoftver újdonságai közé tartozik még *hibatűrő fürtök* egyszerű telepítése és konfigurálása, a korábbinál *fejlettebb terhelésmegosztás*, a *dinamikus particionálás*, valamint a hálózati szolgáltatások automatikus finomhangolása. Ezek szintén a biztonságot, valamint a rendelkezésre állást növelni hivatott fejlesztések.

Egyszerűbb felügyelet

A Windows Server 2008-ban az új *Server Manager konzol* hivatott a telepítés és felügyelet egyszerűsítésére. Azokat a feladatokat, amelyeket a Server Manager-en keresztül egyetlen helyen el lehet végezni, a Windows Server 2003-ban még több menüben kellett végrehajtani.

A Windows Server 2008-ban is helyet kapott a *Windows PowerShell parancssor*, amelynek segítségével a rendszergazdák egy C#-hoz hasonló nyelven írt szkriptekkel egyszerűsíthetik és automatizálhatják a teendőket.

Webszolgáltatások

A Windows Server 2008-ban megérkezett a Microsoft új webszervere, az *Internet Information Services 7 (IIS7)* is. Az IIS7 a Windows Server 2008 szellemében már moduláris felépítésű, telepítéskor kiválaszthatjuk a szükséges komponenseket. A biztonsággal kapcsolatos jelentős újítás még, hogy az IIS7 egymástól elkülöníti a weboldalakat és alkalmazásokat, így az egyiknek az esetleges hibája vagy rosszabb esetben feltörése nincs hatással a többire.

A webszerver az új IIS Manager-ről irányítható, ami egy feladat alapú menedzsmentfelület, de parancssorból is lehetőség van felügyeleti feladatok végrehajtására. Az üzemeltetést tovább egyszerűsíti az integrált webszerver-diagnosztikai és hibakereső segéd. Az egyes alkalmazások felügyeletét delegálni is lehet, a webszerver XML-alapú konfigurációs állományait pedig egy új API-n keresztül is lehet szerkeszteni.

Az IIS7 esetében nem csak a biztonságra, hanem a teljesítményre is nagy hangsúlyt fektettek a fejlesztők, így aztán az egyik leggyorsabb PHP-, Perl- és Ruby-futtatási környezetet sikerült létrehozni, miközben szorosabb lett az integráció az ASP.NET-tel is.

Hyper-V

A Windows Server 2008 áttörést jelentő újdonságai közé sorolható a *Hyper-V* névre keresztelt virtualizációs réteg. A Hyper-V lényegében egy mikrokerneles hypervisor, ami képes a szerver erőforrásainak (memória, processzor, stb.) megosztására, ezáltal lehetővé téve több operációs rendszer párhuzamos futtatását egy szerveren.

A Hyper-V kezdetben legfeljebb 16 processzormagot és 2 terabájt memóriát támogat, a futtatható virtuális gépek száma nincs korlátozva, azoknak csak a rendelkezésre álló erőforrások szabnak határt. A Hyper-V számos különféle operációs rendszert futtathat, legyen

szó akár Windows-változatokról, Linuxról, de később várható a Solaris x86-os változatának támogatása is. A Standard változat csak egy, az Enterprise négy, a Datacenter viszont már korlátlan számú példányban futtatható. A Hyper-V csak 64-biten támogatott.

7.2 A Windows Server 2008 termékcsalád

A Windows Server 2008 összesen 8 különféle változatban kapható:

- **Windows Server 2008, Standard** - Továbbfejlesztett beépített webes és virtualizációs szolgáltatásai révén fokozza a megbízhatóságot és rugalmasságot.
- **Windows Server 2008, Enterprise** - Nagyvállalati felhasználásra alkalmas platformot biztosít kritikus fontosságú alkalmazások használatához.
- **Windows Server 2008, Datacenter** - Ez a kiadás nagyvállalati felhasználásra alkalmas platformot biztosít virtualizációs megoldások kiépítéséhez.
- **Windows Web Server 2008** - Az újratervezett IIS 7.0 kiszolgálóval, valamint az ASP.NET technológiával és a Microsoft .NET-keretrendszerrel integrált Windows Web Server 2008 rendszer segítségével gyorsabban üzembe helyezhetjük webalkalmazásainkat és webszolgáltatásainkat.
- **Windows Server 2008, for Itanium-Based Systems** - A Windows Server 2008 for Itanium-Based Systems kiadás nagyméretű adatbázisok, és egyéb nagy erőforrás-igényű alkalmazások kiszolgálására optimalizált változat. A magas rendelkezésre állás mellett akár 64 processzorral is üzemeltethető.
- **Windows Server 2008, Standard without Hyper-V** - A már említett verziótól annyiban különbözik, hogy nem tartalmazza a Windows Server Hyper-V technológiáját.
- **Windows Server 2008, Enterprise without Hyper-V** - A már említett verziótól annyiban különbözik, hogy nem tartalmazza a Windows Server Hyper-V technológiáját.
- **Windows Server 2008, Datacenter without Hyper-V** - A már említett verziótól annyiban különbözik, hogy nem tartalmazza a Windows Server Hyper-V technológiáját.

8. Összefoglalás

A hálózati biztonság egyike a rendszergazdák számára legfontosabb területeknek. Magam is azt gondolom, hogy napjaink legfontosabb kérdései közé tartozik hálózatunk biztonsága. Fontos megérteni, hogy a biztonság nem állapot, hanem egy véget nem érő folyamat. Folyamatosan, újra és újra át kell vizsgálni rendszerünket, hogy naprakészen fogadhassuk az új fenyegetéseket.

A Microsoft is felismerte, hogy napjainkban a biztonság az egyik legfontosabb kérdés, és a Windows Server 2008 fejlesztésénél már különös gonddal jártak el, nagy hangsúlyt fektettek a biztonságra.

A Windows Server 2003 hálózati megoldásai címszó nagyon nagy területet takar. Sok száz oldal dokumentum is kevés lenne minden egyes szolgáltatás, hálózati megoldás bemutatására.

Dolgozatomban ezért - mivel magam is fontosnak tartom a biztonság témakörét - megpróbáltam rávilágítani azokra a legfontosabb biztonsági kérdésekre, problémákra, eszközökre, megoldásokra, amelyek szóba jöhetnek Windows Server rendszerek üzemeltetése kapcsán.

Remélem sikerült.

9. Köszönetnyilvánítás

Itt ragadnám meg az alkalmat arra, hogy köszönetet mondjak Dr. Krausz Tamásnak a szakdolgozatom elkészítéséhez nyújtott szakmai segítségért, és a rendelkezésemre bocsátott dokumentumokért.

10. Irodalomjegyzék

William Boswell: Inside Windows Server 2003, Addison Wesley, 2003.

Blair Rampling: Windows Server 2003 Security Bible, John Wiley & Sons, 2003.

Dr. Thomas W. Shinder, Debra Littlejohn Shinder: Dr. Tom Shinder's Configuring ISA Server 2004, Syngress, 2004.

Andrew S. Tanenbaum: Számítógép-hálózatok, Panem, 2003.

Tom Thomas: Hálózati biztonság, Panem, 2005.

Craig Zacker: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Training Kit), Microsoft Press, 2004.

IEEE Communications Magazine, 1994, 32. köt., 9. sz., 33-38 p.

http://www.microsoft.com/

http://www.netacademia.net/

http://www.microsoft.com/hun/windowsserver2003/r2_datasheet.mspx

http://web.mit.edu/Kerberos/

http://technet.microsoft.com/en-us/security/cc184923.aspx

http://technet.microsoft.com/hu-hu/wsus/default(en-us).aspx

http://technet.microsoft.com/en-us/windowsserver/default.aspx

http://www.microsoft.com/windowsserver2008/en/us/overview.aspx