Széchenyi István Egyetem Távközlési Tanszék

Hálózati operációs rendszerek III.

jegyzet

Windows Server 2003 Történeti áttekintése

Az alapok:

- A Microsoft 1980-ban kezdett operációsrendszert gyártani először.
- DOS alapú rendszerek
 - Kezdetben az operációsrendszerek MS DOS alapú rendszerek voltak. Erre az alapra fejlesztettek egy GUI-t: Graphical User Interface. (felhasználó barát, multi task üzemmód)
 - Kezdetben verziószámok alapján nevezték el a termékeket (1.0, 1.1), a későbbiekben, pedig az évjárat alapján.
 - Az utolsó DOS alapú fejlesztés a ME volt.
- NT alapú rendszerek
 - Egy új operációsrendszert kifejlesztésén az IBM és a Microsoft együtt dolgozott és létrehozták az OS2-t.
 - Majd a Microsoft "kiszállt" ebből a fejlesztésből és létrehoztak egy új 32 bites operációs rendszert a WIN NT-t.
 - Ez az operációs rendszer alkalmas először domain létrehozására, központi erőforrás kezelésre.
 - Létezik kliens és szerver verziója is.



Windows Server 2003 termékcsalád bemutatása

A termékcsalád rövid bemutatása

1. Windows Server 2003, Web Edition:

Webes alkalmazások kiszolgálására optimalizált változat. Költségtakarékos. (Nem szükséges szerver operációsrendszer + IIS)

2. Windows Server 2003, Datacenter Edition:

High –End OS Legmagasabb szintű rendelkezésre állást, legnagyobb performanciát biztosító szerver. Kiszolgálás szempontjából mindent tud, amit az Enterprise Edition.

32 bites verzió: 32 CPU-t támogat és 64 GB RAM-ot 64bites: 64 CPU és 1TB RAM.

3. Windows Server 2003, Standard Edition:

Alkalmazások szempontjából nem limitált, mint a Web Edition. Alkalmas: alkalmazás szervernek, fájl szervernek, nyomtató szervernek, terminál szervernek. Nem alkalmas azonban cluster szervernek. HW szempontból limitált: 4 CPU és 4 GB Ram-ot támogat.

4. Windows Server 2003, Enterprise Edition:

Minden, ami támogatott a standard editonon az támogatott az enterprise editonon is. + A cluster funkció is. 32 bites verzió: 8 CPUt támogat és 32 GB RAM-ot 64bites: 8 CPU és 1 TB RAM.

R2: Megjelent a Windows Server 2003 R2: mely kiegészítő funkciókat tartalmaz az eredeti termékhez képest. Pl: File Server Manager, új MMC konzol. Változások az ADben (Active Directoryben) is.

Windows Server 2003 telepítése

Mivel előadáson a teljes installálási folyamat bemutatására nincsen lehetőség, ezért néhány screenshot bemutatásával beszéljük végig az installálási folyamatot. A hallgatóknak gyakorlaton lehetőségük lesz az installálásra.

lindows	Setup		
Proces	F2 to r	un Automated Sustem Recourse (ASP)	
11635	1 UJ 21	an natomatea ogstem necovery (non)	
Window	s Server	2003, Enterprise Edition Setup	
Windows	s Server	2003, Enterprise Edition Setup	
Windows	s Server	2003, Enterprise Edition Setup Please wait while Setup formats the partition	
Windows	s Server C: Par	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB (4988 MB free)	
Window	s Server C: Par	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB < 4988 MB free) on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].	
Window	s Server C: Par	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB < 4988 MB free) on 4997 MB Disk Ø at Id Ø on bus Ø on atapi [MBR].	
Window	s Server C: Par	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB < 4988 MB free> on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].	
Window	s Server	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB < 4988 MB free) on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].	
Window	s Server	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB (4988 MB free) on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].	
Window	s Server C: Par	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB (4988 MB free) on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR]. is formatting	
Window	Server	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB (4988 MB free) on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR]. is formatting	
Window	s Server	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB (4988 MB free) on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR]. is formatting 63%	
Windows	Server	2003, Enterprise Edition Setup Please wait while Setup formats the partition tition1 [New (Raw)] 4988 MB < 4988 MB free) on 4997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR]. is formatting 63%	



	Collect	Windows Setup
0	inform	Personalize Your Software
0	Dynam Update	software.
•	Prepar installa	Type your full name and the name of your company or organization.
0	Installi Windor	Name:
•	Finalizin installat	Organization:
Setu app	up w ill c roximat 33 minu	
		< Back Next >

Installálás során beállítandók:

- Regional & Language option (regionális és nyelvi opciók) Dátum, idő, pénznem, szám formátum Billentyűzet beállítások
- Név beállítások (saját adatok beállítása) Name Organization
- 3. Produkt Key (licensz kulcs)
- 4. Licenszelés
 Per Server (konkurens hozzáférések száma alapján)
 Per Device, Per User: Minden usernek saját kliens licensz kell
- 5. Computer Name / PWD (számítógép neve, jelszó)
- 6. Dátum és idő beállítások (időzóna beállítása)
- 7. Network Setting hálózat beállítások (ált. install után állítjuk be)
- 8. Workgroup or Domain (Workgroupba installálunk, később léptetjük domainbe a gépet)

Installálás utáni legfontosabb beállítások: (policytől függő lehet / nem teljesen részletes)

- Szükséges driverek bejátszása, frissítése.
- Szükséges komponensek installálása: Java, Directix, DotNEt...
- Windows komponensek installálása (IIS, FileServerMAnager...)
- Windows Javítások telepítése
- Automatikus frissítések letiltása

Szoftver frissítések, updatek:

A termék megjelenítése után folyamatosan adnak ki javításokat, mivel folyamatosan fedeznek fel hibákat. (biztonsági réseket)

- Automatikus frissítések
- Manuális install (SMS is)

Patchek: 1-1 dolgot javít

Service Packok: összefogja a korábbi javításokat, egyszerre több dolgot is javít.

Windows komponensek installlása

Start menü \ Settings \ Controll Panel Add or Remove Program Add or Remove Windows Component

A minta szerveren installálásra került:

Application Server

- > IIS
- ► FTP
- > SMTP

Management & Monitoring Tools

- File Server Management
- File Server Resource Manager
- Network Monitor

🐞 Add or Ren	nove Programs	
5	Windows Components Wizard	•
C <u>h</u> ange or Remove Programs	Windows Components You can add or remove components of Windows.	<u>28MB</u> arely
Add <u>N</u> ew Programs	To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.), 14. Nove
Add/Remove	Components: ✓ ➡ Accessories and Utilities ▲ Active Directory Services ▲ Active Directory Services ▲ Application Server	
components	Certificate Services 1.4 MB Certificate Services 1.4 MB Certificate Services 7 7 MB Description: Includes Windows Accessories and Utilities for your computer.	
	Total disk space required: 3.0 MB <u>D</u> etails Space available on disk: 12721.0 MB <u>D</u> etails	
	< <u>B</u> ack <u>N</u> ext > Cancel Help	

Jellemzően nem installálunk minden alkalommal külön szervert. Imageket készítünk, melyek aztán többször felhasználásra kerülnek.

Az telepítés további részei

- Hálózati beállítások. (IP, SM, GW, DNS, WINS, DNS utótag, DNS keresési listák—szervereknél nincs DHCP.)
- Szerver domainbe léptetése
- Vírusíró installálása
- Mentő és rendszerfigyelő kliensek installálása.
- RDP engedélyezése. (távoli hozzáférés engedélyezése Remote Desktopon keresztül max 2 session egy időben).

Domain fogalmának tisztázása

A tartomány az Active Directory alapvető szervezeti és biztonsági egysége. Kliensek, szerverek és egyéb hálózati erőforrások gyűjteménye, melyek közös címtáradatbázist alkotnak.

Windows Server 2003 management

Beépített Management eszközök - Computer Management

县 Számítógép-kezelés 📃 🗖 🗙							
💻 Eájl Mű <u>v</u> elet <u>N</u> ézet <u>A</u> blak <u>S</u> úgó							
← → 🗈 🖬 🖧 😫							
🖳 Számítógép-kezelés (Helyi)	Név	Típus	Leírás				
🕀 🦉 Rendszereszközök	🔃 Eseménynapló	Beépülő modul	Eseménynaplók megjeler				
Tárolás A a chuẩu nă chuẩu	🜏 Megosztott mappák		Megosztott mappák, akti				
🛨 😪 Szolgaltatasok és kiszolgaloi alkal	🔝 Helyi felhasználók és cs	Beépülő modul	Helyi felhasználók és cso				
	🖉 Teljesítménynaplók és ri	Beépülő modul	Teljesítményi adatnaplók				
	📕 Eszközkezelő		Eszközkezelő				

🖳 Computer Management				
🗐 Eile Action View Window H	jelp 🗟	_ & ×		
← → II Computer Management (Loca) Computer Man	Name System Tools Storage Services and Applications			
Services and Applications Image: Services and Applications Telephony Services WMI Control Indexing Service Internet Information Service				

Szinte minden Management Tool megtalálható külön is. Ez a program egy összefoglaló áttekintést ad. A management eszközök elérhetők a Start menü\programok\administrativ tools alatt.

Computer Management

I. Rendszereszközök:

1. Event Viewer (Esemény napló):

Ha probléma van egy rendszerrel, ajánlott először ránézni az Eseménynaplóra, mely könnyen kezelhető, és az egyik leginformatívabb eszköz az NT alapú Windowsokban. Hiba esetén nagy esélye van, hogy naplózva lett az esemény, és utólag talán ez az információ segít a hibakeresésben.

Alkalmazás-napló: a számítógépre telepített alkalmazásokkal kapcsolatos információkat tekinthetjük meg itt. A programoktól származó üzenetek és hibák ide kerülnek bejegyzésre

Biztonsági-napló: a sikeres és sikertelen események kerülnek ide.

Rendszer-napló: ebben a részben a rendszerrel kapcsolatos vagy által generált eseményeket találhatjuk meg. Pl. beléptetési hiba, valamelyik szolgáltatás nem indult el, esetleg egy-egy hotfix vagy Service Pack telepítése.

Bejegyzések fajtái:

- Információ: egy esemény sikeres végrehajtása, pl. egy szolgáltatás elindítása.
- Figyelmeztetés: nem túl jelentős, de hibához vezethet.
- Hiba: jelentős probléma, mely veszélyes lehet a rendszerre.
- Sikeres események: ha a biztonsági naplózás be van kapcsolva, ide kerülnek a sikeres események.
- Sikertelen események: ha a biztonsági naplózás be van kapcsolva, ide kerülnek a sikertelen események.

Lehetőség van a bejegyzések szűrésére, hogy csak a minket érdeklő információkat lássuk. Ehhez a megfelelő napló (alkalmazás, biztonsági, rendszer) nevén jobb klikk, majd Tulajdonságok / Szűrő fül. Az öt lehetséges szempontot a neve melletti check-boxban jelölhetjük ki.

System Properties		? >
General Filter		
Event types	☐ Success audit ☐ Faijure audit	
E <u>v</u> ent source:	eventlog	-
Category:	(All)	•
Event I <u>D</u> :		
Us <u>e</u> r:		
Co <u>m</u> puter:		
Erom: First Event	2008. 09. 07. 💌 12:16:32	÷
To: Last Event	▼ 2008. 09. 14. ▼ 12:00:00	
	<u>R</u> estore Defa	aults
	OK Cancel	Apply

Egyéb műveletek:

- Megnyitás.
- Mentés
- > Export
- Logolás beállítása.
 - o Logfájl méretének beállítása.
 - Logolás módjának beállítása.

2. Megosztott mappák / Shared Folders

- Megosztások / Shares: milyen megosztásaink vannak a szerveren
- Munkamenetek / Sessions: mely userek csatlakoznak a megosztásainkhoz
- Nyitott fájlok / Open Files: Mely fájlok vannak megnyitva.

3. Helyi felhasználok és csoportok / Local Users & Groups

Felhasználók / Users

A számítógépet használó userek felsorolása. Installáláskor létrejött felhasználók:

- Administrator (enable)
- Guest (disable)
- Support_388945a0 (disable)
- Csoportok / Groups

A felhasználók csoportokba rendezhetők, ami a jogosultság kezelést megkönnyíti.

Néhány a beépített csoportok közül

Administrators: A rendszergazdáknak teljes és korlátozás nélküli elérésük van a számítógéphez/tartományhoz.

Backup Operators: Felhasználók, akik a "Biztonsági másolat" ("Backup") programján keresztül hozzáférhetnek a rendszerfájlokhoz is a mentés ideje alatt. Más esetben nem.

Guest: A vendégek hozzáférése alapértelmezés szerint azonos a Felhasználók csoport tagjainak hozzáférésével, kivétel a vendégfiók, amelynek korlátozottabb a hozzáférése.

Power Users: A kiemelt felhasználók néhány megszorítással birtokolják a rendszer felügyeleti jogait.

- Telepíthetnek olyan programokat, amelyek nem módosítják az operációs rendszerhez tartozó fájlokat, és nem telepítenek rendszerszolgáltatásokat.
- Testre szabhatják a rendszer közös erőforrásait, például a Nyomtatók, a Dátum és idő, az Energiagazdálkodási lehetőségek beállításait és a Vezérlőpult egyéb erőforrásait.
- Létrehozhatnak és kezelhetnek helyi felhasználói fiókokat és csoportokat.
- Leállíthatnak és elindíthatnak olyan rendszerszolgáltatásokat, amelyek alapértelmezés szerint nem indulnak el.

Nincs engedélyük ahhoz, hogy felvegyék magukat a Rendszergazdák csoportba, és nem férhetnek hozzá más felhasználók NTFS-köteten levő adataihoz, kivéve, ha ehhez megfelelő jogosultságot kaptak az adott felhasználótól.

*Print Operators:*Kezelhetik a nyomtatók beállításait, illetve hozzáférési jogaikat, de újat nem telepíthetnek.

Remote Desktop Users: Ennek a csoportnak a tagjai megkapják a távoli bejelentkezésre vonatkozó engedélyt.

Users: A felhasználók sem véletlenül, sem szándékosan nem tudnak a rendszerre kiterjedő változásokat végrehajtani. Futtathatják a hitelesített alkalmazásokat, de a régi típusú alkalmazások többségét nem. A *Felhasználók csoport* a legbiztonságosabb környezetet biztosítja a programok futtatásához. A felhasználó nem módosíthatja a rendszerleíró adatbázis egész rendszert érintő beállításait, az operációs rendszerhez tartozó fájlokat vagy a programfájlokat. A felhasználó leállíthatja a munkaállomást, de a kiszolgálót nem. A felhasználó létrehozhat helyi csoportokat, de csak az általa létrehozott helyi csoportokat kezelheti. A felhasználó teljes hozzáféréssel rendelkezik saját adatfájljai eléréséhez (%userprofile%) és a rendszerleíró adatbázis saját részéhez (HKEY_CURRENT_USER). A felhasználó nem telepíthet más felhasználók által is használható programokat (így elkerülhetők a trójai faló programok). Nem férhet hozzá más felhasználó saját adataihoz és Asztal-beállításaihoz sem.

📃 Com Reference		
📃 Eile Action View Window	New User ? 🔀	_ 뭔 ㅗ
 Lie Action yew window Computer Management (Local) System Tools Event Viewer Shared Folders Local Users and Groups Groups Groups Performance Logs and Device Manager Storage Removable Storage Disk Defragmenter Disk Management Services and Applications 	Liser name: peldaus Eull name: Pelda User Description: Pelda user letrehozasho Password:	- B
🚛 start 🕑 😂 🛛 💾 C	omputer Manageme	HL 💔 13:08

Feladat: Példa felhasználók és csoportok létrehozására.

📃 Computer Manageme	nt	
Eile Action View	Window Holo Group	?×
Computer Manage Computer Manage System Tools Event Vie Shared For Local User Group Users Group Performal	up name: Pelda cription: Pelda csoport letrehozashoz nbers: Select Users	s have complete and u tors can override secu allowed to launch, acti the same access as me is group can have som bis group have remote
E Service Ma Storage B Storage Disk Defra Disk Mana B Services and	<u>S</u> elect this object type: Users or Built-in security principals <u>F</u> rom this location: MSERVER	Dbject Types
	Enter the object names to select (<u>examples</u>):	<u>Check Names</u>
	Advanced	OK Cancel
🍠 Start 🛛 🚱 🥌	🖳 Computer Manageme	🔣 🚺 🚺 13:07

4. Teljesítmény naplók és riasztások (performance logs & alerts)

A Teljesítménynaplók és riasztások eszköz segítségével részletesen megfigyelhető az operációs rendszer erőforrás-hasznosítása.

Számlálónaplók (counter logs):

Időközönként adatokat gyűjt, csak nem a képernyőn jeleníti meg, hanem egy naplófájlban rögzíti a merevlemezen, ezzel lehetővé válik hosszabb távú elemzések készítése, kiértékelése. A naplófájlt később fel lehet dolgozni és grafikusan megjeleníteni.

System Overview Properties
General Log Files Schedule
Current log file name:
C:\PerfLogs\System_Overview.blg
This log begins when it is started manually.
Counters:
Memory/Pages/sec \PhysicalDisk(_Total)\Avg. Disk Queue Length \Processor(_Total)\% Processor Time
Add Objects Add Counters Remove
Sample data every:
Interval: 15 📑 Units: seconds 💌
Run Ag: <default> Set Password</default>
OK Cancel Apply

Nyomkövetési naplók (trace logs)

A számlálónaplóval ellentétben nem úgy működik, hogy bizonyos időközönként menti a kijelölt számláló állapotát, hanem egy esemény bekövetkezte váltja ki a naplózást.

Riasztások (alerts)

Beállítható, hogy bizonyos esemény bekövetkezésekor riasztás "hajtódjon" végre.

Az esemény bekövetkeztekor a következő műveletek hajthatók végre.

	?	Σ
Általános	Művelet Ütemezés	
Riasztá:	kor:	
🔽 <u>B</u> eje	yyzés az alkalmazások eseménynaplójába	
<u> </u>	zati üzenet küldése a következőnek:	
🔄 T <u>e</u> lja	sítménynapló indítása:	
	×	
📃 A kä	vetkező program f <u>u</u> ttatása:	
	T <u>a</u> llózás]
<u>P</u> ar	ancssori parameterek	
Példa p	irancssor-paraméterekre:	
''l,2008	/09/14-13:26:55.757,\Object\Counter,20.0,több, mint 10,0"	
	OK Mégse Alkalma	Z

5. Eszközkezelő

Lehetővé teszi a telepített hardvereszközök és a hozzájuk kapcsolódó meghajtó programok áttekintését és beállítását.

II. Tárolás

1. Cserélhető tároló \ Removable Storage

A Cserélhető tároló beépülő modul lehetővé teszi a cserélhető adathordozók (szalagok és optikai lemezek) egyszerű nyomon követését, valamint az ezeket tartalmazó szalagtárak (cserélők és lemeztárak) kezelését.

2. Lemeztöredezettség mentesítő \ Disk Defragmenter

A Lemeztöredezettség-mentesítő egységesíti a számítógép merevlemezén talált töredezett fájlokat és mappákat, így minden fájl és mappa egyetlen összefüggő helyet foglal el a kötetben. Ennek eredményeként a rendszer hatékonyabban éri el a meglévő fájlokat és mappákat, és hatékonyabban menti az újakat. A fájlok és mappák töredezettségének megszüntetésével a Lemeztöredezettség-mentesítő a kötetben rendelkezésre álló szabad lemezterületet is egységesíti, így csökken az új fájlok töredezettségének valószínűsége.

3. Lemezkezelés \ Diskmanagement

A Lemezkezelés rendszer segédprogram a merevlemezek, valamint az azokon található kötetek és partíciók kezelésére szolgál. A Lemezkezelés segédprogrammal lemezeket inicializálhat, köteteket hozhat létre, köteteket formázhat.



III. Szolgáltatások és kiszolgálói

Szolgáltatások

A szolgáltatás egy háttérben futó alkalmazási típus.

A Szolgáltatások beépülő modul az alábbiakra használható: Szolgáltatások indítása, leállítása, felfüggesztése, folytatása vagy letiltása távoli és helyi számítógépeken A szolgáltatások indításához, leállításához, felfüggesztéséhez, újraindításához vagy letiltásához rendelkeznie kell a megfelelő engedélyekkel.

Feladat: Automatic Update szolgáltatás leállítása és letiltása.

topatic Update	s Deposition (Local Computer)	21
icomatic opuati	es Propercies (Local Computer)	Ŀ.
General Log On	Recovery Dependencies	
1 -		
Service name:	wuauserv	
Display name:	Automatic Updates	
Display <u>H</u> ame.		
Description:	 Enables the download and installation of Windows undates. If this service is disabled, this computer w 	. 🔺
		···· 王
Path to executat	ole:	
C:\WINDOWS\	system32\svchost.exe -k netsvcs	
1		
Startup typ <u>e</u> :	Disabled	-
Service status:	Started	
<u>S</u> tart	Stop Pause Resum	e
	·	
You can specify	the start parameters that apply when you start the ser	vice
nom nere.	· · · · · · · · · · · · · · · · · · ·	
Start parameters		
	,	

WMI vezérlő: Windows Management Instrumentation

A Windows operációs rendszerek beépített szolgáltatása, amely lehetővé teszi a gépek távoli felügyeletét és menedzselését a hálózaton keresztül. Ezen szolgáltatáson keresztül egy komplett hálózat minden programozható, aktív összetevője elérhető, lekérdezhető és módosítható. Például a számítógép minden hardver és szoftver összetevőjének paraméterei, tulajdonságai, egy

hálózati útválasztó táblája. Segítségével beolvashatja a számítógépekkel kapcsolatos konfigurációs adatok legtöbbjét (beleértve a kiszolgáló alkalmazásokat is), vagy módosításokat hajthat végre a számítógépeken.

A Microsoft Management Console használata

A Microsoft Management Console (MMC) segítségével felügyeleti eszközök csoportjai, úgynevezett konzolok hozhatók létre, menthetők és nyithatók meg. A konzolok többek között a következőket tartalmazzák: beépülő modulokat, bővítményeket, figyelésvezérlőket, feladatokat, varázslókat, valamint a Windows hardver-, szoftver- és hálózati összetevőinek kezeléséhez szükséges dokumentációt. A meglevő MMC-konzolok további elemekkel egészíthetők ki, vagy új konzol hozható létre és állítható be adott rendszerösszetevő felügyeletéhez.

Feladat: Az MMC megnyitása.

Megjegyzés

Az MMC megnyitásához kattintson a Start, majd a Futtatás parancsra. A Megnyitás mezőbe írja be a következőt: mmc.

🚡 Console1 - [Console Root]		- 8 ×
📸 Eile Action View Favorites Window Hel;	p	. 8 ×
Console Root	Name	
 ⊕ S Local Users and Groups (Local) ⊕ S Performance Logs and Alerts ⊕ S Local Computer Policy 	Sci Local Users and Groups (Local) Breformance Logs and Alerts Scoal Computer Policy	
	Add/Remove Snap-in	
	Standalone Extensions	
	Use this page to add or remove a stand-alone snap-in from the console.	
	Snap-ins added to: Console Root Add Standalone Snap-in	<u> ? ×</u>
	Available standalone snap-ins:	
	Performance Logs and Alerts Snap-in Vendor	_
	S Local Computer Policy	
	Sective Directory Sites and Services Microsoft Corporation	
	Active Directory Users and Compu Microsoft Corporation	
	ActiveX Control Microsoft Corporation	
	Gatilistation Manager Microsoft Corporation Catilista Tandates	
	Certificates Microsoft Corporation	
	Description Certification Authority Microsoft Corporation	
	Component Services Microsoft Corporation	-
	Description Allows you to configure the .NET Framework 1.1	
	Add Remove About	
	Add	e
뿣 Start 🛛 🕑 🥔 👘 🎼 Console 1 - [Conso	Je R 🔣 😥	13:21

Local Computer Policy:

Lokális gépre vonatkozó policy / házirend beállításokat tartalmazza.

- Felhasználók beállításai
- Számítógépre vonatkozó beállítások A számítógépre vonatkozó beállítások, függetlenül attól, hogy milyen felhasználó jelentkezik be kiértékelődik. (Általános szoftverek beállításait és a windows beállításait tartalmazza.)

Feladat: Példán keresztül bemutatni a policy működését:

Startmenüből eltüntetni a shut down parancsot és megjeleníteni a logoff parancsot.

Remove & Prevent access to Shut Down Remove Logoff on the Start menu

A policyknak 3 értéke lehet:

- Not configured
- ➢ Enable
- > Disable



Megosztások\Sharek létrehozása, jogosultságok beállítása:

Megosztások \Sharek

A hálózat egyik alapvető feladata az erőforrás-megosztás. A dokumentumok és egyéb iratok központi tárolásának a mai napig az egyik legelterjedtebb módja a fájl-megosztás használata.

Feladat: Fájl megosztás készítése.

megosztas tulajdonsa	ágai	? 🗙	355 589 KB	WinRAR archive
Általános Megosztás Ezt a mappát mappa megos	Biztonság Testreszabá megoszthatja a hálózat ti ztásához kattintson a Me	is öbbi felhasználójával. A egosztva az alábbi néven	8 484 KB	Adobé Acrobat Doc Fájimappa
lehetőségre.				
Nincs megosztva				
Megosztva az ala	Joi neven]		
Megosztási név:	megosztas			
Megjegyzés:				
Felhasználói korlát:	Nincs korlátozás			
	🔿 A felhasználók m			
A kapcsolat nélküli h megadásához katint: A Windows tűzfal úgy mappa megosztását a <u>A Windows tűzfal beál</u>	vzzárérés beállításainat ion a Gyorsítótár gomb van beállítva, hogy leh hálózat más számítógé (tásainak megtekintése UK	Csopot vagy leľhasználó neve:	Hozzáadás	Ekávolítás s Meciaciadás
		Teles hozáriés Módosítás Olvasás		
		ОК	Mégse	Alkalmaz

Jogosultság állítások: mappákon

<u>Feladat: konkrét jogosultság beállítása egy felhasználónak a korábban létrehozott mappán.</u>

(az újonnan létrehozott felhasználónak, az újonnan létrehozott diszken található mappára Write jogosultságot beállítani)

- Share törlése.
- Mappa törlése.

További Management eszközök bemutatása

File Server Resource Manager:

Fájl szerverek nagyon hasznos eszköze.

Alkalmas:

- Kvóták létrehozására: megadható, hogy egy adott könyvtárban mennyi adatot tárolhatunk.
- Fájlok szűrésére: megadható, hogy bizonyos fájltípusokat adott mappákba nem tárolhatunk.



🚪 File Seizer Resource Manager		<u>_ 8 ×</u>
Eile Action View Help		
File Server Resource Manager (Local) Cuota Management Quotas Quota Templates File Screening Management Storage Reports Management	Filter: Show all: 0 items Quot % L Q Sou Ma Q	Actions Quotas ▲ ② Create Qu ③ Refresh View ▲ ③ Help

Hálózati kártya beállításai:

2 –vagy több kártya esetén team konfigurálása.(trunk)

Team típusai:

- Load Balance= Terhelés elosztás.
- ➢ FailOver= Hibatűrő

Teamen állítva:

- ➢ IP cím
- DNS szerver
- > DNS suffix
- ➢ WINS: NetBios névfeloldás: Windows Internet Name Service

My Computer\Sajátgép Properities\Tulajdonságok

- General: általános jellemzők
- Computer Name
 - o Név megadás
 - Domainbe léptetés
 - Primary DNS suffix megadáse
- ➢ Hardware
 - Device Manager
 - o Drivers
 - Nem windows által tesztelt driverek
 - Mit tegyen, ha driver frissítés szükséges
- > Advanced
 - o Performance Option: CPU ütemezés, memória használat
 - o Virtuális memória beállításai
- Automatic Update
- Remote: RDP engedélyezése.

Active Directoryhoz és a Domainhez tartozó fogalmak bemutatása:

Domain\ Tartomány

1. A tartomány az Active Directory alapvető szervezeti és biztonsági egysége. Kliensek, szerverek és egyéb hálózati erőforrások gyűjteménye, melyek közös címtáradatbázist alkotnak.

2. Azt a hálózatot vagy hálózatrészt, amelyet egyetlen közös címtárral felügyelnek, nevezzük tartománynak.

Tartomány vezérlő\ Domain Controller

A tartomány fizikai megjelenése a címtár adatbázis. A címtár adatbázist a tartományvezérlő tárolja.

A tartomány címtárába felvett felhasználók elvileg a tartomány összes gépén jogosultak bejelentkezni. Vagy a számítógépek erőforrásaihoz hálózaton keresztül hozzáférni.

Szervezeti egység\ Organizational Unit

A számítógépeket, felhasználókat, egyéb erőforrásokat egységbe lehet szervezni. Ezzel a tartományon belül leképezhetjük akár a szervezeti egységeket is. Ezeket az egységeket nevezzük organizational unitoknak. Ezekhez külön jogokat lehet állítani, így a rendszergazda feladata megosztható, korlátozható.

Trust:

Több tartomány is összekapcsolható. Az összekapcsolás alapja a tarományi meghatalmazási kapcsolat vagy más néven trust. Ez lehetővé teszi, hogy a tartomány felhasználói egy másik tartomány erőforrásait igénybe vegye. A meghatalmazásos kapcsolatok útján a tartomány először fába szervezendő. Ez azt jelenti, hogy a tartományok között hierarchiát alakítunk ki. A tartományfa első tartomány a root, vagy gyökér tartomány.

Tree, Forest

A tartományfa tartományai egy névhierarchiát használnak. Vannak olyan esetek azonban, amikor nem használhatnak a tartományok egy névhierarchiát, ilyenkor több gyökértartománynak kell lennie, mert nem minden tartomány legfelső szintű neve egyforma. Ebben az esetben a tartományokból erdő hozható létre.

Account, Resource

A tartományban alapvetően 2 féle objektum lehet, fiók (account) és az erőforrás (resource).



Egy tartományban minimum 2 tartomány vezérlőnek kell lennie. Ez azért fontos, ha az egyik megsérül, a másik át vehesse a feladatait. A tartományi adatbázisoknak mind a 2 tartomány vezérlőn ugyanazokat az adatokat kell tartalmaznia, konzisztensnek kell lennie. Az adatbázis változásokat replikálni kell a tartományvezérlők között.

Globális katalógus szerver\ Global Catalog Server:

Ha a hálózatot nem egyetlen tartományban, hanem tartományfába szervezzük, akkor szükséges a global catalog szerver. Ez egy olyan adatbázist tartalmazó szerver, melyben egy helyen fel van sorolva minden olyan objektum, mely az erdőt alkotó címtáradatbázisokban szerepel. Azonban minden adata nincsen meg, csak néhány attribútuma. Ezek általában olyan attribútumok, melyek egyértelműen azonosítanak egy objektumot és könnyen megtalálhatóvá teszik ezért. Globál katalog nincs jelen minden tartományvezérlőn, csak néhány kitüntetetten.

Kitüntetett szerepkörök

Tartomány feletti főkiszolgálók:

Domain Naming Master:

Minden DC-n van arról információ, hogy a tartományt tartalmazó fa milyen tartományokból épül fel, és ezek milyen kapcsolatban vannak egymással. Ez a struktúra azonban csak egy kiszolgálón változtatható meg ez a tartományvezérlő a Domain Naming Master. Ezért ebből minden erdőben csak egy van.

Shema Master:

A címtár szerkezete: leírja, hogy a címtárban milyen objektumok tárolhatók, és az egyes objektumoknak milyen attribútumai vannak. Az erdőben egy shema master van. Az Exchange szerver telepítése shema bővítést von maga után.

Tartományon belüli főkiszolgálók

PDC emulátor:

Nem minden kliens tudja használni, az AD szolgáltatásait. Ezért szükséges ez a szerepkör. Pl.: Az NT Domainben a jelszóváltoztatások csak a PDCn volt lehetőség. A régebbi kliensek ezért továbbra is a PDC-n szeretnék megváltoztatni a jelszavukat. Időszinkront is a PDC emulátor végzi.

RID Master:

Minden objektumnak szükséges egyedi azonosítója: ez a GUID:globally unique identifier. A hozzáféréseknél a rendszer azonban nem ezt az azonosítót használja, hanem a SID-et. (Security Identifier) SID 2 részből áll: tartományi azonosítóból és az objektum azonosítóból. Az objektum azonosítója a RID: Relativ Identifier. Mivel az ADben minden DC –n lehet objektumot létrehozni, ezért szükség volt egy DCre, amely a RIDeket "legyártja" így nem fordul elő, hogy egy tartományban 2 objektumnak azonos a SIDje.

Infrastructure Master:

Feladata: többi tartományban történő változások figyelése. Figyeli a trustolt tartományban levő objektumok változásait. (pl. megvan-e az a user, aki a mi tartományunkban szerepel egy csoportban.)

AD-DNS

Az AD üzembe helyezéséhez szükséges egy DNS kiszolgáló, és legalább egy DNS zóna, amely az adott DNS kiszolgáló hatókörébe tartozik.

Ha nem telepítünk előre DNS-t, akkor az AD telepítésekor automatikusan települni fog egy DNS szerver is, és létrejön a DNS zóna is.

Példa a TK-ből.

Szak.local tartomány első tartomány vezérlőjének telepítése. Ez a tartomány egy tartományfa gyökértartománya. Mivel a teljes erdőben az egyetlen tartományfa, ezért az erdő gyökértartománya is egyben.

Telepítés menete:

Startmenü\Run\DCPROMO: ez a program menüből nem érhető el.

Directory Installation	Wizard
	Welcome to the Active Directory Installation Wizard
7	This wizard helps you install Active Directory services on this server, making the server a domain controller.
	If this is the first time you have installed Active Directory, it is recommended that you first read the overview in <u>Active</u> <u>Directory Help</u> .
	To continue, click Next.
	< Back Next > Cancel
ve Directory Installation	n Wizard
Dperating System Comp Improved security setting Windows.	atibility gs in Windows Server 2003 affect older versions of
Domain controllers runni require clients and other secure way.	ng Windows Server 2003 implement security settings that servers to communicate with those domain controllers in a more
Some older versions of V earlier, do not meet thes Apple Mac OS X and SA	Windows, including Windows 95 and Windows NT 4.0 SP3 or e requirements. Similarly, some non-Windows systems, including MBA clients, might not meet these requirements.
Some older versions of V earlier, do not meet thes Apple Mac DS X and S/ For more information, see	Windows, including Windows 95 and Windows NT 4.0 SP3 or e requirements. Similarly, some non-Windows systems, including MBA clients, might not meet these requirements.

Figyelmeztetést kapunk, hogy a hálózatunkban levő Win95 és Win NT SP3 előtti kliensek nem fognak tudni bejelentkezni a hálózatba. Ennek oka az alapértelmezett biztonsági beállítások nem támogatják a nem biztonságos hitelesítést.

Domain Controller Type Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
C Additional domain controller for an existing domain
Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
< <u>B</u> ack <u>N</u> ext > Cancel

Választhatunk, hogy egy új Domain domain controllere lesz-e gépünk, vagy egy meglévő tartományba telepítünk-e tartományvezérlőt.

Create New Domain Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
C Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
O Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< <u>B</u> ack <u>N</u> ext > Cancel

Azt is ki kell választanunk, hogy egy új tartományfát hozunk-e létre, vagy egy meglévő fa tartománya alá rendeljük.

Active Directory Installation Wizard
New Domain Name Specify a name for the new domain.
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).
Eull DNS name for new domain:
I
Const.
< <u>B</u> ack <u>N</u> ext > Lancel

Tartomány teljes DNS nevének megadása.

Active Directory Installation Wizard
NetBIOS Domain Name Specify a NetBIOS name for the new domain.
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.
Domain NetBIOS name: KIADO
< <u>B</u> ack <u>N</u> ext > Cancel

Tartomány Netbios neve: Tartomány régi típusú, NT-számára is értelmezhető név. (Max. 15 karakter hossz lehet).

tive Directory Installation Wizard
Database and Log Folders Specify the folders to contain the Active Directory database and log files.
For best performance and recoverability, store the database and the log on separate hard disks.
Where do you want to store the Active Directory database?
Database folder:
C:WINDOWS/NTDS Browse
Where do you want to store the Active Directory log?
Log folder:
C:WINDOWS\NTDS Browse
< <u>B</u> ack <u>N</u> ext > Cancel

Adatbázis és a tranzakciós naplójának helye. Javasolt, nem az alapértelmezett helyen meghagyni, hanem egy másik rendszer partíciótól független partícióra tenni.

Active Directory Installation Wizard
Shared System Volume Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Eolder location:
C:\WINDOWS\SYSVOL Browse
< <u>B</u> ack <u>N</u> ext > Cancel

Megosztott rendszer könyvtárak helyének megadása. A Sysvol könyvtár az, melyekből az ügyfélgépek kiolvashatják a rájuk vonatkozó adatokat. (pl. group policy)



DNS kiszolgáló beállítása: Ha van DNS szerverünk, csak nem állítottuk be jól, lehetőségünk van ezt javítani. Telepíthetünk egy újat, ha nincsen.

Ictive Directory Installation Wizard	×
Permissions Select default permissions for user and group objects.	
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.	
 Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain. 	
< <u>B</u> ack <u>N</u> ext> Cancel	

Meghatározzuk, hogy milyen hozzáférési jogok kerüljenek beállításra. Ez attól függ, van-e a tartományban W2K előtti kiszolgálók.

ative Disastany Tastallation Illiand
Directory Services Restore Mode Administrator Password This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see <u>Active Directory Help</u> .
< <u>B</u> ack <u>N</u> ext > Cancel

Rendszergazda jelszó megadása. Ez nem azonos a címtárbeli rendszergazda jelszavával. Vannak olyan karbantartási műveletek, melyek nem hajthatók végre, működő címtár mellet. Ezért szükség van egy olyan felhasználóra, akivel akkor is be lehet lépni, ha a címtár nem használható. Az AD telepítése során, törlődik a helyi felhasználó adatbázis. Ezt újra létre kell hozni. Ebben a felhasználó adatbázisban keletkezik egy rendszergazda fiók, ennek a jelszavát kell megadni itt.

Active Directory Installation Wizard
Review and confirm the options you selected.
You chose to:
The new domain name is kiado.szak. This is also the name of the new forest.
The NetBIOS name of the domain is KIADO
Database folder: C:\WINDDWS\NTDS Log file folder: C:\WINDDWS\NTDS SYSVDL folder: C:\WINDDWS\SYSVDL
The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.
The password of the new domain administrator will be the same as the password of the administrator of this computer.
To change an option, click Back. To begin the operation, click Next.
< <u>B</u> ack <u>N</u> ext > Cancel

Összefoglaló képernyő. Ha valamin módosítani szeretnénk, vissza lehet lépni, javítás céljából.

Ezután kezdődik meg a tényleges konfiguráció.

AD ellenőrzése:

- 1. Az AD telepítése után az eseménynaplóban megjelenik 2 új menü.
 - Directory Services: az AD alapfunkcióit biztosító szolgáltatás üzeneti.
 - ▶ File Replication Services: fájlreplikációs üzenetek.
 - → Ha DNS is fut a gépen, akkor a menü bővül egy DNS naplóval is.
- 2. DNS ellenőrzése. SRV rekordok keresése.
- 3. Sharek ellenőrzése: Net Share
- 4. felügyeleti eszközök ellenőrzése
 - ADUC: címtárban tárolt objektumok kezelésére szolgál.
 - AD Site & Services: tarományok közötti replikácioók irányítása, telephelyek létrehozásának felügyelete.
 - Active Directory Domain & Trust: aktuális tartományszerkezet bemutatása, kapcsolatok kezelése.

Fiókok és az erőforrások címtári nyilvántartása.

Az ADben a" nyilvántartás" objektumokként jelenik meg. Minden fióknak, szervezeti egységnek egy objektum felel meg. Az objektumnak típusától függően attribútumai vannak, ezek tartalmazzák az adatait.

Active Directori Users & Computers (ADUC)

A címtár nyilvántartásának kezelésére alkalmas eszköz az ADUC. Ennek segítségével lehet felhasználói csoportokat, számítógép fiókokat, OUkat kezelni.

A címtárban tárolt objektumokat a címtáradatbázis speciális része, az u.n. séma írja le.

Container (tároló): más objektumokat tartalmaznak. Pl: Organizational Unit, melynek segítségével strukturálható az AD.

Alapértelmezett tárolók:



Feladat: 3 OU / 2 Al OU létrehozása

Számítógépek Felhasználók Csoportok Security Disztribúciós

Feladat: Felhasználó létrehozása:

w Object - User		
Create in:	kiado.szak/Kiadó Users	
<u>F</u> irst name:	Minta Initials:	
Last name:	Bela	
Full name:	Minta Bela	
User logon name:		
mintabe	@kiado.szak	
User logon name (pre	-₩indows 2000):	
KIADO\	mintabe	
	< Back Next > Can	icel

A felhasználó objektum legfontosabb attribútumai:

- GUID: globális egyedi azonosító
- SID: biztonsági azonostó
- Bejelentkezési név: mintabe

Elsődleges felhasználó név: UPN: User Principal név: mintabe@kiado.szak

- Teljes név
- ➢ E-mail cím
- ➤ Jelszó

.

- Csoporttagság

ι	Jser			
Minta Bela Propertie	5			<u>? ×</u>
Remote control	Term	inal Servic	es Profile	COM+
Member Of	Dial-in	Envi	ironment	Sessions
General Address	Account	Profile	Telephones	Organization
🥵 Minta Be	ela			
<u>F</u> irst name:	Minta		Initials:	
Last name:	Bela			
Di <u>s</u> play name:	Minta Bela			
Description:				
Offi <u>c</u> e:				
				[
Lelephone number:	J			Uther
E- <u>m</u> ail:				
Web page:				Othe <u>r</u>
		ОК	Cancel	Apply

Legfontosabb műveletek felhasználókkal:

🍜 Active Directory Users and Computers						
🎻 Eile Action Yiew Window He	lp					
⇐ ⇒ 🗈 📧 🐰 🛍 🗙 😭	ē 🔒 🛙	2 💷 🦉 💯 边	7 🍕 🙍			
Active Directory Users and Computer	Kiadó User	• s 1 objects				
Hand Queries	Name		Туре		Description	
	🕵 Mint	Copy	User			
Computers Computers PoreignSecurityPrincipals Users Kiado Computers Kiadó Users Kiadó csoportok	k 	Add to a group Digable Account Reset Password Moye Qpen Home Page Send Maji All Tas <u>i</u> s • Cut Delete Rena <u>m</u> e				
		Properties				
		Help				

Tartományi csoportok:

Users tároló alatt találhatók a tartományi csoportok.

or the sector of	uters				
G Eile Action View Window He	łp				
← → 🗈 🗷 💼 💣 🙆 🖻	🖻 💵 🦉 🖉 🕍 🖓 🍕 📷				
Active Directory Users and Computer	Users 21 objects				
Saved Queries	Name	Type	Description		
E 🖓 kiado.szak	G Administrator	Liser	Built-in account for admini		
E Builtin	G ASPNET	User	Account used for running		
Computers Optrollers	Cert Publishers	Security Group	Members of this group are		
EcreignSecurityPrincipals	2 DnsAdmins	Security Group	DNS Administrators Group		
lisers	2 DnsUpdateProxy	Security Group	DNS clients who are permi		
<u> </u>	Domain Admins	Security Group	Designated administrators		
	Domain Computers	Security Group	All workstations and serve		
	2 Domain Controllers	Security Group	All domain controllers in th		
	Bomain Guests	Security Group	All domain guests		
	Domain Users	Security Group	All domain users		
	BEnterprise Admins	Security Group	Designated administrators		
	Group Policy Creator Owners	Security Group	Members in this group can		
	Guest	User	Built-in account for guest		
	1 HelpServicesGroup	Security Group	Group for the Help and Su		
	1 IIS_WPG	Security Group	IIS Worker Process Group		
	IUSR_MSERVER	User	Built-in account for anony		
	1WAM_MSERVER	User	Built-in account for Intern		
	RAS and IAS Servers	Security Group	Servers in this group can		
	Schema Admins	Security Group	Designated administrators		
	50 SUPPORT_388945a0	User	This is a vendor's account		
	1 1 TelnetClients	Security Group	Members of this group ha		

Csoportok kezelése AD-ben:

Type (típus) szerint megkülönböztetett csoportok:

- Security (biztonsági) csoport—jogosultság állításhoz, erőforrás hozzárendeléshez
- Distribution (terjesztési) csoport—felhasználók összefogásához (csoportos levélküldéshez)

Csoportok hatókör (scope) szerint:

Azt határozza meg, hogy egy csoport mely tartományokból kaphat tagokat, illetve, mely tartományokban használható

Domain Local: tartományon belüli csoportok: Tagjai lehetnek más domainből származók. (Más tartomány globál v universál csoportja, felhasználója)

Globál: egy erdőn belül bármely csoportba felvehetők. Tagokat, azonban csak a saját tartományából tartalmazhat.

Univerzál: tetszés szerinti tartományból lehetnek tagjai, és tetszés szerinti tartományban felhasználhatók tagként. (csak natív üzemmódban). Fizikailag nem kötődnek az erdő egyetlen tartományához sem. Minden adatuk a globális katalógusban tárolódik.

Feladat: Tartományi csoport létrehozása.

Active Directory Lisers and Comn	uters
New Object - Group	x
Create in: kiado.szak	Kiadó csoportok
E Group name:	
MintaCsop	
Group name (pre- <u>W</u> indows 2000):	
MintaCsop	
Group scope	Group type
C Domain local	
	C Distribution
C Universal	
	OK Cancel

MintaCsop Properties	<u>? ×</u>
General Members Member Of Managed By	
MintaCsop	
Group name (pre- <u>W</u> indows 2000): MintaCsop	
Description: minta security csoport	
E- <u>m</u> ail:	
Group scope	
● <u>G</u> lobal ○ <u>G</u> lobal	
O <u>U</u> niversal	
Notes:	
	-
OK Cancel A	pply

MintaDLCsop Properties	<u>? ×</u>
General Members Member Of Managed By	
MintaDLCsop	
Group name (pre- <u>W</u> indows 2000): MintaDLCsop	
Description: Minta DL Csop	
E · <u>m</u> ail:	
Group scope	
C Domain local C Security	
Global O Distribution	
O Universal	
<u>N</u> otes:	
	A V
OK Cancel A	pply

🐗 Active Directory Users and Compu	ıters			_ 8 ×
🌍 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> el	þ	Ť		_ 8 ×
⇔ → 🗈 🖬 🖷 📽 🖻	🖻 🖬 🎽 🖉 🦉 🙋 🔽			
Active Directory Users and Computer	Kiadó csoportok 2 objects			
E - Saved Queries	Name	Туре	Description	
E Builtin	22 MintaCsop	Security Group - Global	minta security csoport	
Computers	MintaDLCsop	Distribution Group - Global	Minta DL Csop	
Oomain Controllers ForeignSecurityPrincipals				
Users				
Kiadó csoportok				

Legfontosabb tulajdonságainak ismertetése:

- > Members
- ➢ Member Of
- Managed By

Computer account létrehozása

炎 Active I	Directory Users and Computers							
🎻 Eile 👍	Action <u>V</u> iew <u>W</u> indow <u>H</u> elp							
⇐ ⇒	n ■ ● ● ■ ● ■ ● ■ ● ■ ● ■ ● ■ ● ■ ● ■ ●							
Active	lew Object - Computer							
⊡-∰ ki	Create in: kiado.szak/Kiado Computers							
±								
	Computer name:							
	TesztComputer							
	Computer name (pre-Windows 2000):							
	TESZTCOMPUTER							
	The following user or group can join this computer to a domain.							
	User or group:							
	Default: Domain Admins							
	Assign this computer account as a pre-Windows 2000 computer							
	Assign this computer account as a backup domain controller							
	< Back Next > Cancel							

TesztComputer Pr	operties		? ×
Delegation General	Location	Managed E System	y Dial-in MemberOf
Teszt	Computer		
Computer name (p	ore- <u>W</u> indows 2000):	TESZTCOM	PUTER
D <u>N</u> S name:			
<u>R</u> ole:	Workstation or ser	ver	
Description:			
	04	Can	cel <u>Apply</u>

Tulajdonságai a computer tényleges domainbe léptetésével aktiválódnak. Ha nem hozom létre accountot a beléptetéskor a Computers tárolóba jön létre.

Lekérdezések:

Feladat: felhasználók listázására, lekérdezés készítése:

New Query		? ×
<u>N</u> ame:		
Mintalekerdezes		
Description:		
felhasznaok a domainben		
Query root:		
\kiado		Browse
✓ Include <u>subcontainers</u>		
Query string:		
		D <u>e</u> fine Query
J		
	0K.	Cancel

рι	ıters			
le	þ			
¢	0 🗈 😫 🖬	整整物下	7 4 😰	
ř	Mintalekerdezes	8 objects		
	Name	Туре	Description	
	🕵 Administrator	User	Built-in account for admini	
	😰 ASPNET	User	Account used for running	
	Sociest 😥	User	Built-in account for guest	
	IUSR_MSERVER	User	Built-in account for anony	
	IWAM_MSER	User	Built-in account for Intern	
	5 krbtgt	L Edit Query	<u>? ×</u>	
	😰 Minta Bela	L Name		
	SUPPORT_38	L <u>Name.</u>		
		Mintalekerd	🍕 Find Common Queries 🛛 🔹 🤶 🗙	
		Description:		L
		felhasznaok	Fing: Common Queries	L
		-	Users Computers Groups	L
		Query root:		L
		\kiado	Define the variables of your query.	L
		1	Name: Is not null	L
		🔽 Include :		L
		Query string:		L
		C (abiaa)Ca	Disabled accounts	L
			Non expiring passwords	L
		,//	Dave sizes last leases	L
			Days since last logon.	L
1				
			UK Cancel	
1				

Jogosultságok a címtár objektumokhoz

- Mindenki ahhoz férjen hozzá, amihez kell.
- Rendszergazdai feladatok megosztása lehetséges
- > NTFS jogosultságokhoz hasonló jogosultság állítás
 - o Felület
 - Öröklődés (kikapcsolható allow inheritable permisson from)

Minden objektumon állítható, de OUn szokás, különben átláthatatlan lesz a struktúra

 Properities\Security (speciális lehetőséget be kell kapcsolni: View\Advanced Features)

- FC(Full Controll)
- R (Read)
- W (Write)
- Jogok kiértékelődése
 - o Összeadódnak a jogosultságok
 - Deny+Allow= Deny a tiltás mindig erősebb

Delegálás

- > ADUC \ OU segéd menü: Delagate Control
 - Felhasználók hozzáadása
 - Jogosultság meghatározása, mely műveletek elvégzésére jogosult
 - Delegate the following Common Task
 - Create custom task to delegate



Support tools

A Support Tools egy segédprogram gyűjtemény, mely megtalálható minden Windows 2000-es és XP-s telepítő lemezen. A csomag része számos diagnosztikai, biztonsági és a mindennapi munkát megkönnyítő program. Vannak köztük parancssorból elérhetők és grafikus interfésszel rendelkezők egyaránt. A repertoárban megtalálhatók Active Directory tartományvezérlők kezeléséhez, teszteléséhez és replikáció diagnosztikához kiválóan alkalmas programok is.

Installálása:

	-2)	2								
	1	Console1						X			
C	E	\\192.168.1	l.11\d\$\ora_tartas\ora_3					_O×			
	🐌 C	🔯 Ejle Edit View Favorites Iools Help 🛛 🧗									
	For	For 🗿 Back + 🕥 - 🏂 🔎 Search 🏷 Folders 🔯 💓 🗙 🆃 📰 -									
L	_	Address 🛅 \\1	.92.168.1.111d\$iora_tartasiora_3	I				- 🖪 😡			
at		Name A	🔄 C:\temp\supporttools						- 🗆 🗵		
			Eile Edit View Favorites	<u>T</u> ools <u>H</u> elp							
			🔇 Back 🔹 🕤 🗸 🎓 🐻	indows Support Tools Setu	p Wizard		×				
My			Address 🛅 C:\temp\su	Destination Directory			11 N	[🔻 🔁 Go		
			Folders	Please select an appropriate de	stination directory for Windo	ws Support Tools.	P	Modified	Attributes		
			🗄 🚜 3.5 Floppy (A:					3. 03. 04. 16:28	A		
			🖃 🥯 Local Disk (C:)	nstall Windows Support Tools to			Browse				
14			ADFS		•		510100				
			E C Admin								
			🗄 🧰 A; 🕠	Available space on local hard dis	ks:						
N			i⊇ Ci	Volume Di:	sk Size Available	Required	Difference				
			E 👷 Fa	■C:	15GB 10GB	24MB	10GB				
	Ch		🗉 🧰 Lo								
			i Mi								
	U+										
			🛅 Pr	4							
			C Se								
					< Back	Install Now	Cancel				
			🗀 Te								
			E 🚞 All Users								
			🗄 🛄 Derault User								
			🗄 🧰 Program Files								
			🗄 🧰 StorageReports								
			E Conservation temp								
			Supporttools								
			E 🚞 WINDOWS								
2	Star	t 🔞 🥭	📸 Console1	🔞 Character Map	🗀 \\192.168.1.11\d\$\o	ra 🔯 C:\temp)	supporttools	😸 Windows Su	pport T	HU	11:32

ResourceKit

További alkalmazások, kiegészítő programok találhatók a ResourceKit csomagban.

ADSI Edit

- Support tools része. Advanced felhasználóknak ajánlott.
- Futtatás\adsi edit.msc

SUDST Edit			_ 8 ×
Sile Action View Window Help			
📣 ADSI Edit	Name	Class	Distinguished Name
Domain [mserver.kiado.szak] D	There a	are no items to sho	w in this view.
CN=Computers	=Administrator Properties		<u>? ×</u>
Image: Controllers Image: Controllers Image: Controllers <td></td> <td>ancel</td> <td>mi mi mi mi mi mi</td>		ancel	mi mi mi mi mi mi
⊕	4		
🐮 Start 🛛 🎯 🧑 🚽 🍕 ADSI Edit			1

LDAP: Lightweight Directory Access Protokol

Directory szolgáltatások elérését szabályozza, ahol gyakoriak a kereséséek, de a struktúra változás nem gyakori.

LDAP szintaxis bemutatása:

- CN: Common Name: objektum neve saját környezetében
- OU: Organizational Unit: Tároló
- ➢ DC: Tartomány
- DN: Distinguished Name: egyedi, teljes útvonallal azonosítja az objektumot
- > RDN: Relative Distinguished Name: OU-n belül egyedi.

Group policy management console

- Le kell tölteni
- Installálása:

- Indítása: Adminisztratív eszközök közül
- > Használata: Policy objektumok hozhatók létre, szerkeszthetők
- Domain létre hozásakor 2 policy jön létre
 - Default domain policy
 - o Default Domain Controller policy

Kerberos autentikáció

A Kerberos V5 működése – áttekintés:

A Kerberos V5 hitelesítési mechanizmus jegyeket ad ki a hálózati szolgáltatások eléréséhez. Ezek a jegyek titkosított adatokat tartalmaznak (egy titkosított jelszóval együtt), amelyek bizonyságot adnak a felhasználó identitásáról a kért szolgáltatás számára. A jelszó bevitelén, illetve az intelligens kártya hitelesítő adatainak beírásán kívül az egész hitelesítési folyamat láthatatlan a felhasználó számára.

A Kerberos V5 fontos szolgáltatása a kulcsszolgáltató (KDC). A kulcsszolgáltató az ügyfelek jelszavait és a fiókok adatait tartalmazó Active Directory címtárszolgáltatás részeként minden tartományvezérlőn fut.

A Kerberos V5 hitelesítési folyamata a következőképpen működik:

- 1. Az ügyfélrendszeren lévő felhasználó jelszó vagy intelligens kártya használatával hitelesíti magát a kulcsszolgáltató számára.
- A kulcsszolgáltató speciális jegymegadó jegyet biztosít az ügyfélnek. Az ügyfél ezt a jegymegadási jegyet használja a jegymegadási szolgáltatás (TGS) elérésére, amely a tartományvezérlőn lévő Kerberos V5 hitelesítési mechanizmus része.
- 3. Ezután a jegymegadási szolgáltatás szolgáltatásjegyet biztosít az ügyfélnek.
- 4. Az ügyfél ezt a szolgáltatásjegyet mutatja be a kért hálózati szolgáltatásnak. A szolgáltatásjegy az ügyfelet is hitelesíti a szolgáltatás számára, és a szolgáltatást is az ügyfél számára.

A Kerberos V5 szolgáltatásai minden tartományvezérlőn telepítve vannak, és a Kerberos-ügyfél minden munkaállomásra, illetve kiszolgálóra telepítve van.

Minden tartományvezérlő kulcsszolgáltatóként működik. Az ügyfél DNSlekérdezéssel keresi meg a legközelebbi tartományvezérlőt. Ezután ez a tartományvezérlő szolgál kulcsszolgáltatóként a felhasználó számára a bejelentkezés alatt. Ha az elsődleges kulcsszolgáltató elérhetetlenné válik, a rendszer új kulcsszolgáltatót keres a hitelesítés végrehajtásához.

<u>Replikáció</u>

A Windows Server családban a replikáció a tartományok vezérlőinek adatbázis frissítését takarja. Minden tartományvezérlőn az adatbázis ugyanazon példánya kell, hogy fusson a tartomány megfelelő működése érdekében. Ezen rendszer segítségével a rendszergazda a tartomány bármelyik tartományvezérlőjén végezhet módosításokat. Hiszen ha a tartományban több vezérlő van akkor bármelyik vezérlő végezhet hitelesítést. Ezt nevezzük multi-master rendszernek.

A címtáradatbázis részei:

- tartomány partíció objektumok, userek, groupok
- konfigurációs partíció az erdő felépítése, kapcsolatok
- séma partíció az objektumok fajtái, attribútumai
- alkalmazás partíció nincs user, csoport, illékony adatok(DNS)
- globális katalógus minden az erdőben megtálalható objektum benne van, alapértelmezetten egy kell a tartományok közötti átjáráshoz,

A replikáció folyamata:

Az adott szerver melyen változás történt, 15 percenként vizsgálja felül, hogy történt-e a címtáradatbázisban változás. Ha igen, elküldi a szomszédos tartományvezérlőnek a "hírt", hogy változás történt mely ezek után letölti azt.

Az AD-beli replikáció pull ("lekéréses"), nem pedig push ("leküldéses") típusú. A konzisztencia-ellenőrző szolgáltatás (KCC = Knowledge Consistency Checker) létrehoz egy site linkekből (helyek közötti hivatkozásokból) álló replikációs topológiát, a definiált helyeket használva a forgalom szabályzására. A site-on belüli (intrasite) replikáció gyakran és automatikusan megtörténik: minden változási értesítés egy lekéréses replikációs ciklust indít meg.

Ez tömörítetlen adatforgalmat jelent, ami RPC kapcsolaton keresztül továbbítódik. A site-ok közötti (intersite) replikáció ritkábban, megadott időközönként történik és nem használja a változási értesítéseket, ám ez konfigurálható akár a site-on belüli replikációval megegyezőre is. Tömörített adatforgalom, amely RPC vagy SMTP kapcsolaton keresztül történik. Az ISTG szolgáltatás alakítja ki az általában nem redundáns replikációs útvonalat. Különböző "költségeket" lehet az egyes helyek közötti hivatkozásokhoz rendelni (pl. a DSL vonallal összekötött telephelyeken a replikáció "olcsóbb"

lehet, mint ISDN vonal használatakor), és a site linkek topológiáját a KCC ehhez igazodva változtatja meg. A tartományvezérlők közötti replikáció történhet tranzitív módon, több site linken keresztül (az azonos protokollt használó site link bridge-eken), ha az azokhoz rendelt költség alacsony, bár a KCC automatikusan alacsonyabb költséget rendel a közvetlen site-site kapcsolódásokhoz, mint a tranzitívekhez. Két site közötti replikáció beállítható úgy is, hogy egy-egy bridgehead server ("hídfőállás kiszolgáló") között történjen, amik aztán site-on belüli replikációval adják át a változásokat a site-on belül.

Site-ok közötti replikációnál több beállítási lehetőség is rendelkezésre áll. Itt meg lehet adni az ütemezett feladatokhoz hasonlóan mikor történjen replikáció, de alapértelmezettként 180 percenként vizsgálják meg a címtáradatbázist.

Csoportházirend

Az Active Directory alkotta hálózatokban, Windows 2000 és XP munkaállomásokkal a Csoportházirend (GPO - Group Policy Objects) szolgáltatáson keresztül gyakorlatilag teljesen megoldható a felhasználók és munkakörnyezetük viselkedésének és jogosultságainak szabályozása. Mindez rengeteg beállításon keresztül. Sokszor csak azért nem valósulnak meg bizonyos dolgok, mert nem világos, hogy mit és hol lehet beállítani és hogy egyáltalán a csoportházirend képes-e erre?

néhány példa:

- Szabályozható az asztal megjelenése.
- Testre szabhatjuk az intéző és web böngésző (IE) kinézetét.
- Szabályozhatjuk, milyen programok indulhatnak el.
- Felhasználók könyvtárainak beállításai, jogosultságai.
- Előírhatjuk milyen programok települjenek automatikusan rendszerünkre.

A csoportházirend akkor használható jól, ha több gépre ugyanazon beállításokat szeretnénk használni, nem pedig minden gépre sajátos beállítást alkalmazunk.

A csoportházirend által lehetővé válik a munkaállomások hibatűrő üzemeltetését, amely az jelenti, hogy a meghibásodott munkaállomás helyére rakott "üres" gépet automatikusan telepíti és előkészíti a munkára.

Ennek 3 fő alapeleme van:

- Az Active Directory, mely lehetővé teszi a hálózat központi felügyeletét
- A Távtelepítő szolgáltatás (RIS Remote Installation Service) mely a hálózatról képes Windows-t telepíteni.
- A Csoportházirend, ez irányítja a programok telepítését, biztosítja a munkaállomások biztonsági és környezeti beállításait.

Csoportházirend-objektumok

A csoportházirend úgynevezett csoportházirend-objektumok (GPO) formájában jelenik meg az Active Directory-ban, ám itt csak az azonosítóik vannak felsorolva. A tényleges beállítások a tartományvezérlők **SYSVOL** könyvtár alatti könyvtárstruktúrában találhatók, innen töltik le az ügyfélgépek a rájuk vonatkozó beállításokat.

A csoportházirend-objektumok tartalma a SYSVOL alatti POLICIES könyvtár alatt található, az egyes csoportházirend-objektumok könyvtárai kapcsos zárójelek közötti hosszú 16-os számrendszerbeli számok jelzik.

Minden csoportházirend-objektum 2 részből áll:

- Számítógépre vonatkozó beállítások: a munkaállomás egészére vonatkozó beállításokat tartalmazza
- Felhasználóra vonatkozó beállítások: a munkaállomás aktuális felhasználójának munkakörnyezetét határozza meg.

A munkaállomásokra valójában több csoportházirend is érvényesülhet, melyeknek "összege" adja meg a tényleges beállításokat. Az összeg azt jelenti, hogy minden olyan beállításra hatással lesz a csoportházirend, amelyek valamelyik csoportházirend-objektumban definiálva vannak. Természetesen itt vigyázni kell az öröklődésre, hiszen egy beállításra csak egy definíció fog érvényesülni.

A csoportházirend-objektumok hozzárendelése szervezeti egységekhez.

A csoportházirendek önmagukban nem tartalmaznak információt mely számítógépek beállításait szabályozza. Ahhoz hogy a GPO-k működjenek is az adott hálózatban, hozzá kell rendelni egy szervezeti egységhez. Majd a szervezeti egység beállításainál lesz módunk ezeket a beállításokat módosítani.

A tartományban kezdetben 2 alapértelmezett GPO foglal helyet. Az egyik a tartományra, míg a másik a tartományvezérlőkre vonatkozik. Így érik el, hogy a tartomány egészéhez egységes biztonsági beállítások érvényesüljenek.

A csoportházirendek érvényre jutása a következő:

- 1. A *startup* és *shutdown* script a bejelentkezés előtt és a kijelentkezés után futnak le, pl.: programok telepítése, frissítések letöltése.
- 2. *logon* és *logoff* script a bejelentkezés után és a kijelentkezés előtt futnak le, pl.: az adott felhasználó jogosultságainak beállítása.

<u>A különböző programok automatikus telepítése csoportházirend</u> <u>segítségével</u>

Mindenekelőtt szükségünk van telepíteni kívánt program telepítő csomagjára, amely lehetőleg *Windows Installer* kompatibilis telepítőkészletet jelent (*.msi*). Ezt a csomagot kell egy kiszolgáló megfelelően megosztott könyvtárába tenni, mely elérhető az egész hálózatról vagy azokról a munkaállomásokról melyeknél a csoportházirend előírja a program telepítését. A megosztott könyvtár előkészítése után jegyezzük fel annak elérési útját a \\kiszolgáló\megosztás formában.

A windows installerrel nem kompatibilis alkalmazások előkészítése

Létre kell hoznunk egy .zap segédállományt, melynek tartalma például a következő lehet:

```
[Application]
FriendlyName=Microsoft Office 97
SetupCommand=setup.exe /unattend
DisplayVersion=8.0
Publisher=Microsoft
[Ext]
DOC=winword.exe
DOT=winword.exe
```

•••

Ebből a *SetupCommand* és az *Ext* rész ami fontos, az előbbi megmondja a telepítő indításául szolgáló program nevét, a másik szekció pedig leírja milyen kiterjesztések kezelésére alkalmas.

A jegyzet nem tér ki a csoportházirend összes beállítási lehetőségeire hiszen azok terjedelme ezen jegyzet többszöröse lenne.

Hálózati szolgáltatások Windows 2003 szerver alatt

A windows 2003 server beépített kiszolgálója az IIS (Intenet Information Services) a UNIX like rendszerekhez képest egy beépülőben képes ellátni a web/mail/ftp szerver funkciókat. Bár az IIS-nél sokoldalúbb mail/ftp szerverek vannak windows rendszerre (3rd party sofware) az IIS az egyik legjobb webkiszolgáló a Microsoft platformjára.

Az IIS a Windows NT, Windows 2000, és Windows XP operációs rendszerekben is megtalálható, de nem része a Windows95/98/ME, és a Windows XP Home rendszereknek.

Telepítése a következőképpen zajlik: Programok Telepítése/törlése \ Windows összetevők \ IIS

Ezen bellül számtalan plusz telepíthető beépülőt találunk melyek az IIS sokoldalúságát szolgálják.

Az IIS telepítéséhez szükségünk van a fent említett operációs rendszerek telepítő médiumára.

🙀 Add/Remo	ve Programs						
Change or	Currently installed programs: Windows Components Wizard	Sort by: Name					
Remove Programs	Windows Components You can add or remove components of Win	To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subgomponents of Internet Information Services (IIS):					
Add New Programs Add/Remove Winn is Comporents	To add or remove a component, click the ch part of the component will be installed. To s Details. Components: Implement formation Services (IIS) Implement and Monitoring Tools Implement	Image: Common Files 1.0 MB Image: Common Files 1.0 MB Image: Common Files 3.5 MB Image: Common Files 0.1 MB Image: Common Files 0.0 MB Image: Common Files 1.3 MB Image: Common Files 1.4 MB Image: Common Files 5.0					
	Space available on disk: 3324.0 M	<back next=""> Cancel Cancel</back>					

Az IIS a weblapokat a *c:\InetPUB/www_root* könyvtárból hosztolja alapértelmezetten, ez telepítéskör automatikusan létrejön.

Az IIS beállításait a számítógép kezelés \ szolgáltatások és alkalmazások \ IIS alatt találjuk. Ahhoz, hogy a web szerver működjön szükségünk van még az alapértelmezett dokumentumok engedélyezésére, ezt a dokumentumok fülön találjuk.

E Computer Management		No. of Concession, Name		1 - 1 - 1	
Action View Action View Tree Tree Construction Shared Folders Device Manager Device Manager Cost Users and Groups Storage Disk Management Disk Defragmenter Logical Drives Removable Storage Services and Applications Removable Storage Services MMI Control Services Internet Information Services WMAP Services MAPP Services Service	Name Scripts Scripts IISAdmin IISSamples MSADC Printers images about.htm contact.htm home.htm index.htm	WAP Properties Web Site Documents Documents T Enable Defa It Index It Index It Index It Index It Index It Index It Index It Index It Index It Index It It It It It It It It It It	Performance Directory Security	ISAPI Fiters	Add Bemove Browse
<u> </u>	<u> </u>		OK 4	Cancel Ar	pply Help

A szerver elindítását már csak a saját weblapunkra kattintva és a szolgáltatások ablakban az elindít gombot lenyomva érhetjük el.

Ellenőrzésképpen a web böngészőnkbe irjuk be:

http://{ a gép IP cime}

Bár mint azt fentebb említettük, nem a legelőnyösebb a IIS beépített FTP szolgáltatása, gyorsan beállítható ezért igen elterjed. Az FTP beépülőt az IIS alatti FTP (File Transfer Protokoll) kiválasztásával telepíthetjük.

Majd ezek után az Adminisztrációs eszközök $\$ Internet szolgáltatások alatt az IIS-re kattintva megjelenik az új FTP oldal készítése.

Az új FTP varázsló végigvezet bennünket azokon a lépéseken amelyek feltétlen fontosak az ftp szerver üzemeltetéséhez.

Ezek sorra a következők:

- Az FTP szerver leírása
- Az FTP szerver IP címe, és alapértelmezett portja
- A következő oldalon több választási lehetőségünk van,
 - ftp felhasználóit el lehet különíteni a windows 2003 Α felhasználótól, így létre lehet hozni olyan csoportot mely használhatja az FTP szervert de nem belépni tud а számítógépünkre.
- A következő lépés az FTP szerverünk mely könyvtárat ossza meg.
- Majd a jogosultságok globális megadására van módunk (read only ftp)

Továbbá lehetőségünk van *anonymous* kapcsolódásra, melyet a ftp szerver tulajdonságainál engedélyezhetünk.

Site	Security	Accounts	Messages	Home Director	y Direct	tory Security
All	gw anon;	mous conr	nections			
Use t	he follow	ving Windo	vs user acco	unt for anonym	ous acces	i51
User	name;	IUSR				Browse
Pass	word:				_ 1	
	í	Allow of	nly anonymo	us connections		

Az IIS mail szerver szolgáltatása

Az internetes ajánlások az IIS beépített SMTP szolgáltatása helyett az EAsendmail service SMTP szervert ajánlják a Microsoft platformjára, de eme jegyzetben csak a Windows komponensekre van mód bővebb kifejtésre.

A telepítés a már jól megszokott módon a a Windows összetevők $\$ IIS $\$ SMTP beépülő telepítésével történik.

📲 Internet Info	rmation Services		
File Action V	iew Help		
⇐ ⇒ 🗈 🖪	1 🚯 🗟 😰		
Internet Inform	nation Services	Domain Name	Туре
D-LWONG	(local computer) tes t SMTP Virtual Server	SD-LWONG	Local (Default)
	New 🕨	Domain	
Contraction of the second	View 🕨	12 20	
	Refresh Export List		
	Help		
Adds a new domain	k:		

Majd a IIS beállításai alatt létrehozunk egy új mail domain-t.

Itt csak a Domain nevét kell megadni. Ezek után a létrehozott mail domain tulajdonságaiban lehet megadni a felhasználók adatait, valamint a hozzáféréseket illetve az SMTP- specifikus beállításokat (pl.: EHLO/HELO stb.)

Az SMTP modul alapértelmezetten létrejön, ez pedig nem más, mint a c:\Inetpub\mailroot könyvtár.

A DNS szolgáltatás Windows 2003 Server alatt

A DNS szolgáltatás tette lehetővé, hogy a manapság használt Domain nevekkel lehessen egy adott kiszolgálót elérni, nem pedig annak IP címét megjegyezve. Ezekhez az internetet úgynevezett zónákra osztották, és a zónákhoz rendeltek hozzá egy névkiszolgálót, mely tárolja, hogy milyen IP címhez milyen hosztnév tartozik.

(A DNS működése és a névfeloldás folyamata nem képezi a tárgy részét.)

A DNS szerverek lehetnek elsődleges vagy másodlagos névkiszolgálók egy adott zónára vonatkoztatva. Hiszen egy névkiszolgáló lehet egy zóna elsődleges, de egy másik zóna másodlagos névkiszolgálója is.

A zónák tartalmát és az erőforrásrekordok hozzáadását mindig csak az adott zóna elsődleges névkiszolgálóján módosíthatjuk, majd ezek automatikusan átkerülnek a másodlagos szerverekre is. Ezeket a SOA rekordon belül megszabott időközönként másolják le a névkiszolgálók az elsődleges szerverről.

AXFR - Teljes zónaátvitel: ha az elsődleges zónafájlban változás történik, a másodlagos névkiszolgálók a teljes zónafájlt átmásolják.

IXFR – Növekményes vagy részleges zónaátvitel: ha az elsődleges zónafájlban változás történik, a másodlagos névkiszolgáló csak a megváltozott erőforrásrekordokat másolja le.

A DNS telepítése

A Domain Name System (DNS) telepítése a megszokott módon Windows összetevők hozzáadásával történik.

(A feltelepített DNS szerver hálózati beállításaiban az elsődleges DNS szerver automatikusan kitöltésre kerül: 127.0.0.1)

A klienseknél ezt magunknak kell beállítanunk, abban az esetben ha ezt az opciót nem DHCP szerver segítségével osztjuk ki.

Rekordok hozzáadása a zónához.

A zónafájlokban először is a zónára vonatkozó beállításokat kell megadni (TTL, Serial, expire, refresh ...). Valamint ezek után van lehetőségünk létrehozni erőforrásrekordokat.

Néhány példa erőforrásrekordra:

192.168.100.123 amd ΙN Α (IPv4 cím hozzárendelése domainnamehez) 2001:db8:85a3::8a2e:370:7334 ΤN AAAA amd (*IPv6 cím hozzárendelése domainnamehez*) amd ΙN CNAME feher4 ("ALIAS" erőforrásrekord hozzárendelésre egy, már létező domainhez) 192.168.100.123 ΙN SRV amd (tartományvezérlő kijelölése a zónában)

A DNS szerver a telepítés után két tárolót tartalmaz:

Forward Lookup Zones – Címkeresési zónák Reserve Lookup Zones – Névkeresési zónák

A DNS kiszolgálók főbb beállításai:

Interfaces – Kapcsolatok: Megadhatjuk mely hálózati csatolóktól fogadjon el kéréseket a DNS szerverünk.

Forwarders – Továbbítók: Itt lehet beállítani mely DNS szerverekhez fordulhat kéréssel a saját szerverünk.

Root Hints – Gyökérmutató: A Root DNS szerverek beállítási lehetősége.

Lehetőségünk van zóna nélkül is üzemeltetni DNS szervert, ilyenkor gyorsító kiszolgálót (Caching Only Name Server) kapunk. Az ilyen kiszolgáló csak és kizárólag rekurziv kéréseket továbbít a zónával rendelkező DNS szerverekhez, esetleg a Root DNS szerverekhez. Egy ilyen kérés után a kiszolgáló eltárolja a kapott választ, majd ha az élettartam alatt (TTL) még egy ilyen kérést kap, nem kell lekérdezni, hisz a gyorsító tárban bent van a bejegyzés.

Dinamikus erőforrásrekordok

A Dinamikus erőforrás rekordok, működéséhez a klienseknek is támogatniuk kell ezt a szolgáltatást. Ilyenkor a DHCP-vel kiosztott névkiszolgálóhoz "bejelentkezik" a kliens, majd a saját magának beállított számítógépnév és a DHCP-től kapott IP címet bejegyezteti a DNS szerverbe. Ezzel az erőforrásrekordokat nem kell kézzel megadnunk automatikusan bejegyződnek.

Ehhez azonban működnie kell egy frissítés/törlés funkciónak, hogy ne legyen tele "szeméttel" a zónafájlunk.

Minden dinamikusan bejegyzett rekord "öregszik" Ha letelik a frissítéshez rendelkezésre álló idő, az erőforrásrekord elavulttá válik, és a DNS-kiszolgáló automatikusan törli a zónaadatbázisból. Ez z idő alapértelmezetten 7 nap.

A DHCP szolgáltatás Windows 2003 Server alatt

A DHCP kiszolgálók az ügyfelek dinamikus IP címzését oldják meg központilag. Ennek követelménye, hogy a DHCP szervernek az adott hálózatban statikus IP címmel kell rendelkezniük. DHCP használatával az elgépelt IP címek és az IP cím ütközés is elkerülhető, hisz amit a DHCP egyszer már kiosztott utána már nem fogja azt még egyszer kiajánlatni.

A DHCP ügyfél kezdetben nem rendelkezik IP címmel, ezért a hálózat üzenetszórás címére (broadcast – hisz nem tudja mely gép a DHCP szerver) küld egy kérést (DHCPDISCOVER) majd erre válaszolt a DHCP szerver egy ajánlással (DHCPOFFER) mely tartalmazza a következő adatokat:

- DHCP kiszolgáló IP címe
- Az ügyfélnek felajánlott IP címet és alhálózati maszkot
- Az ügyfél hardvercímét (MAC) ezzel csak ő fogja a kérést elfogadni
- Az időtartamot melyre a kiszolgáló az ügyfélnek adja az IP címet (lease time)

<u>APIPA</u>

Microsoft rendszerekben amennyiben nincs statikus IP cím beállítva és a DHCPDISCOVER-re sem kap választ az ügyfél, úgy az APIPA lép életbe. (Automatic Private IP Addressing). Ez Microsoft specialitás, hisz a Microsoftnak a tulajdonában volt egy B osztályú IP tartomány, melyet később használaton kívül helyezett ezen rendszer működéséhez. Tehát ha nem kap IP

címet úgy a windows automatikusan kioszt magának egy IP címet a 169.254.0.0/16-os tartományból. Azért, hogy ilyen esetben se forduljon elő IP cím ütközés az ügyfél 10 ping-kérést küld az adott címre, majd ha egyre sem érkezik válasz használatba veszi a címet.

Ha a bérleti idő lejár, az ügyfél küld a DHCP kiszolgálónak (mivel van érvényes IP címe, nem kell broadcast üzenetet használnia, közvetlen a kiszolgálóhoz fordul) melyben kéri a bérleti idő meghosszabbítását. Ezt általában a DHCP kiszolgáló nyugtázza, majd bejegyzi az adatbázisba a hosszabítást.

Járulékos paraméterek DHCP kiosztása:

- 003 router 003 útválasztó: alapértelmezett átjáró megadása
- 004 time server 004 Időkiszolgáló: Az ügyfélgépek óráinak szinkronizálása
- 006 DNS servers 006 DNS-kiszolgálók: A DNS szerverek IP címei
- 015 DNS domain name 015 A domain név: a beállítandó tartománynév
- 033 Static route option 003 statikus út beállítás: akkor van rá szükség ha az alhálózatból egynél több helyen lehet kijutni.
- 044 WINS 044 Wins szerverek

A DHCP szolgáltatás telepítése szintén a Windows összetevők hozzáadásával végezhető el.

Ekkor a felügyeleti eszközöknél a DHCP bejegyzésre kattintva új hatókört hozhatunk létre, majd ezen belül van lehetőségünk IP címet lefoglalni, illetve tiltani az alhálózatban.

Az IP cím ütközések elkerülésére a DHCP modul beállításinál az Speciális beállítások alatt megadható ütközésérzékelési kísérletek opció szolgál. Ezzel megadhatjuk hányszor próbálja meg "pingelni" a kiosztandó címet a kiszolgáló mire kiadja az egy ügyfélnek.