

# Széchenyi István Egyetem Távközlési Tanszék

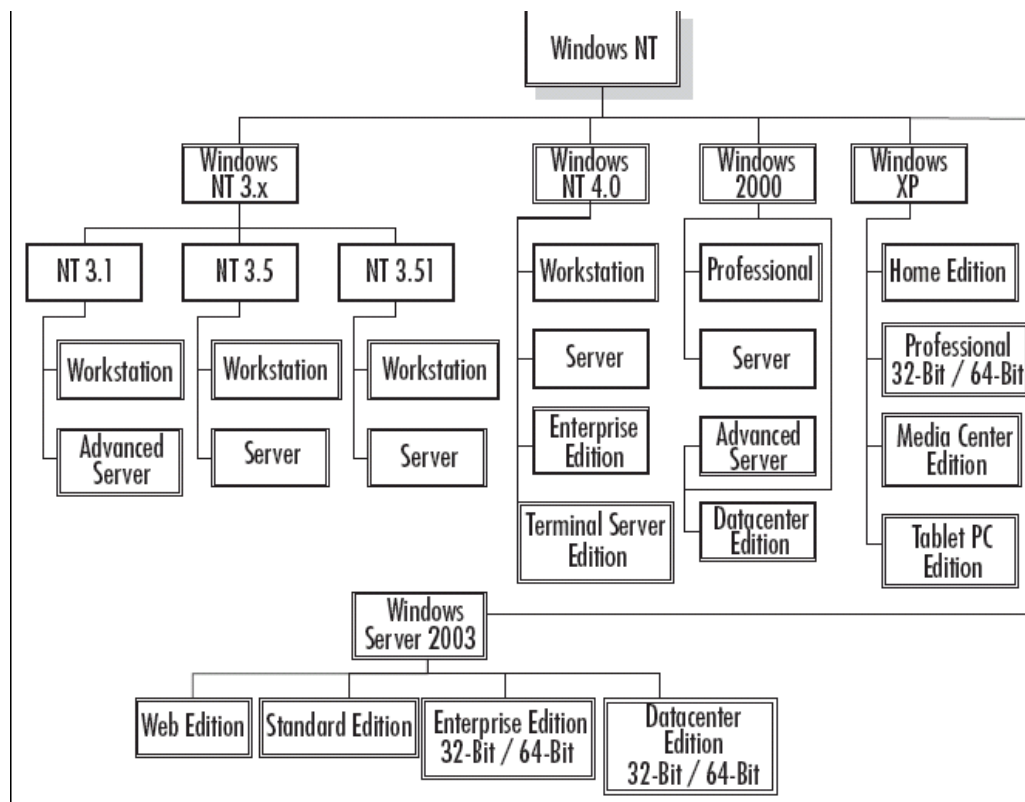
Hálózati operációs rendszerek III.

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.

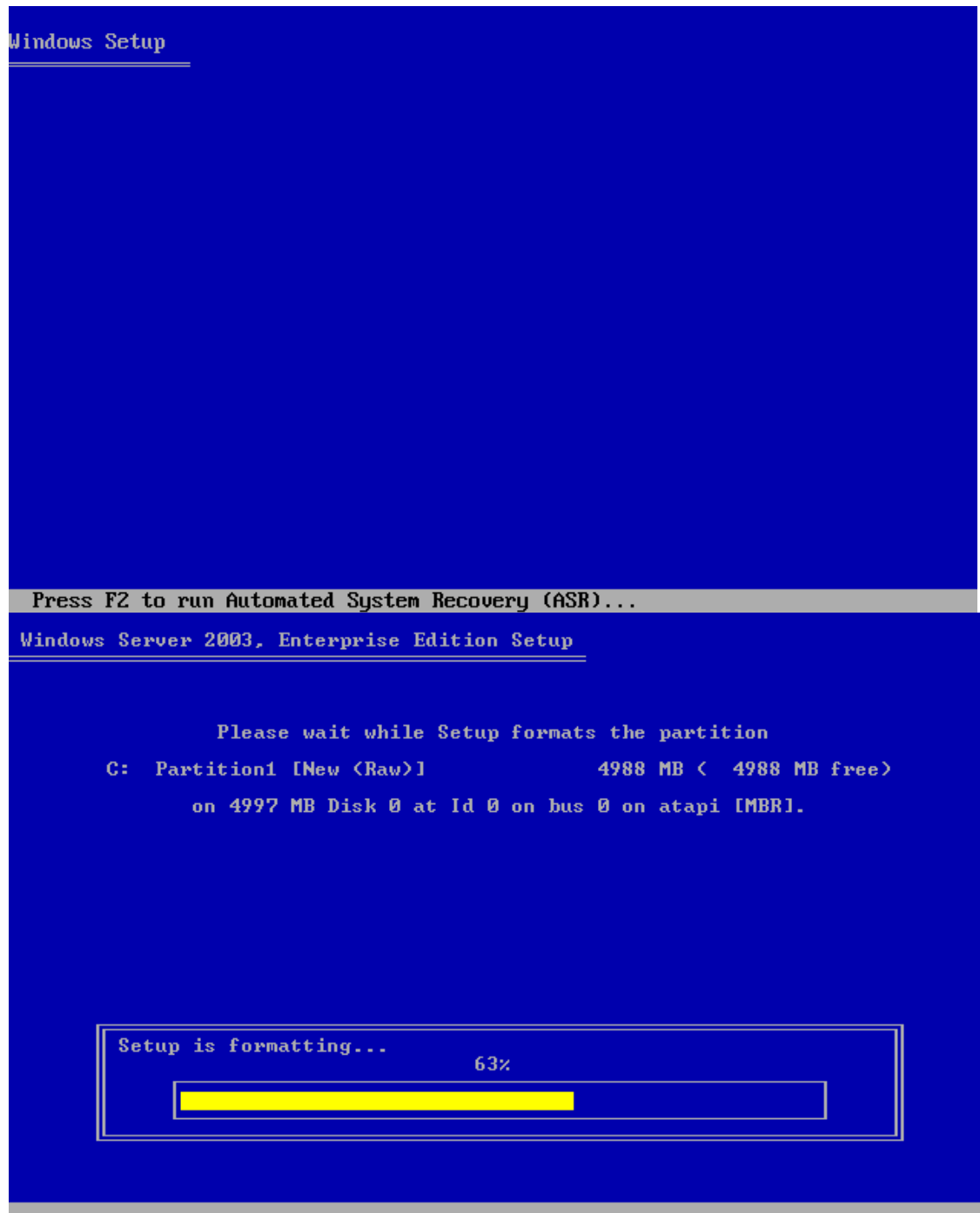
32 bites verzió: 8 CPUt támogat és 32 GB RAM-ot

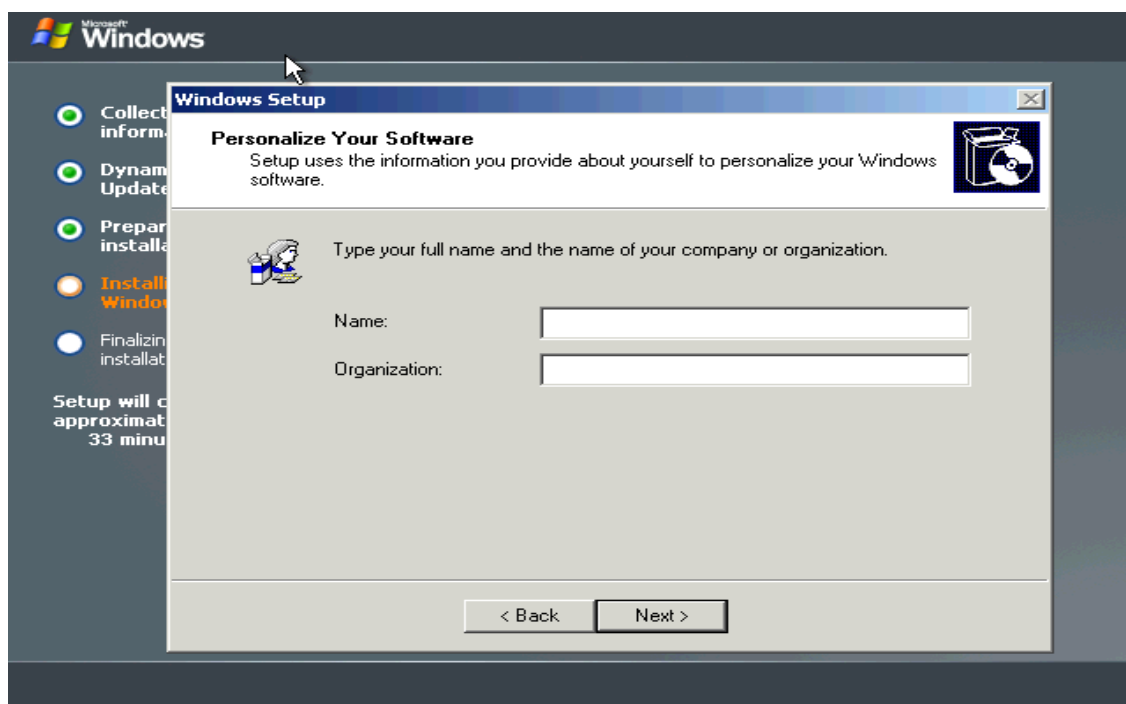
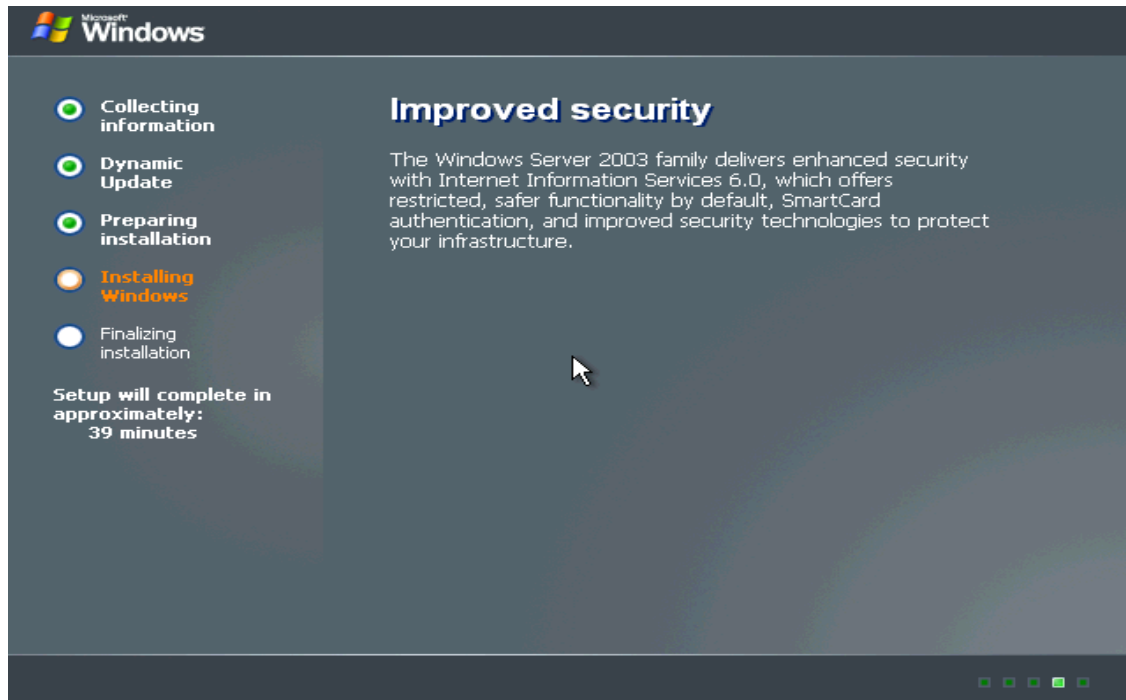
64bites: 8 CPU és 1 TB RAM.

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.





### Installálás során beállítandók:

1. Regional & Language option (regionális és nyelvi opciók)  
Dátum, idő, pénznem, szám formátum  
Billentyűzet beállítások
2. Név beállítások (saját adatok beállítása)  
Name  
Organization
3. Produkt Key (licenz kulcs)
4. Licenzelés  
Per Server (konkurens hozzáférések száma alapján)  
Per Device, Per User: Minden usernek saját kliens licenz 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: (policytól 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 installálása

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

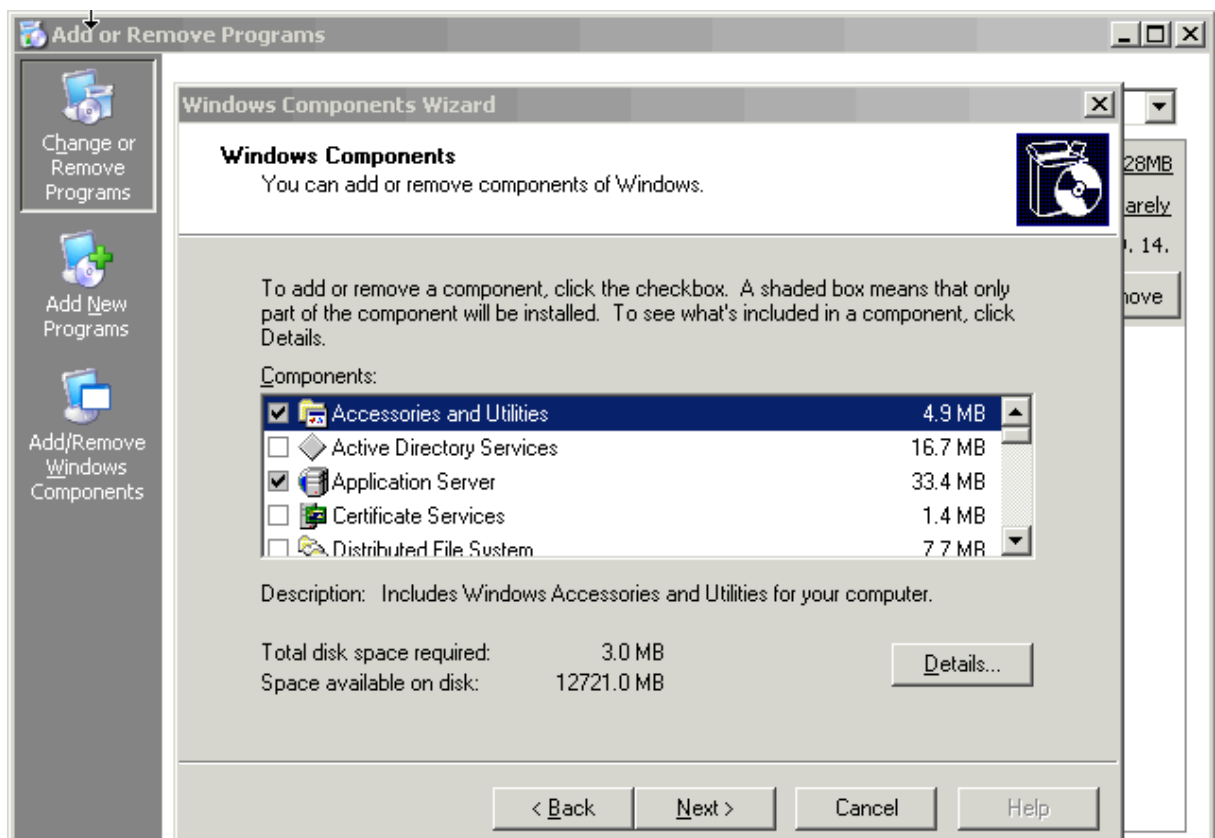
A minta szerveren installálásra került:

### Application Server

- IIS
- FTP
- SMTP

### Management & Monitoring Tools

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



Jellemzően nem installálunk minden alkalommal külön szerveret. 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).

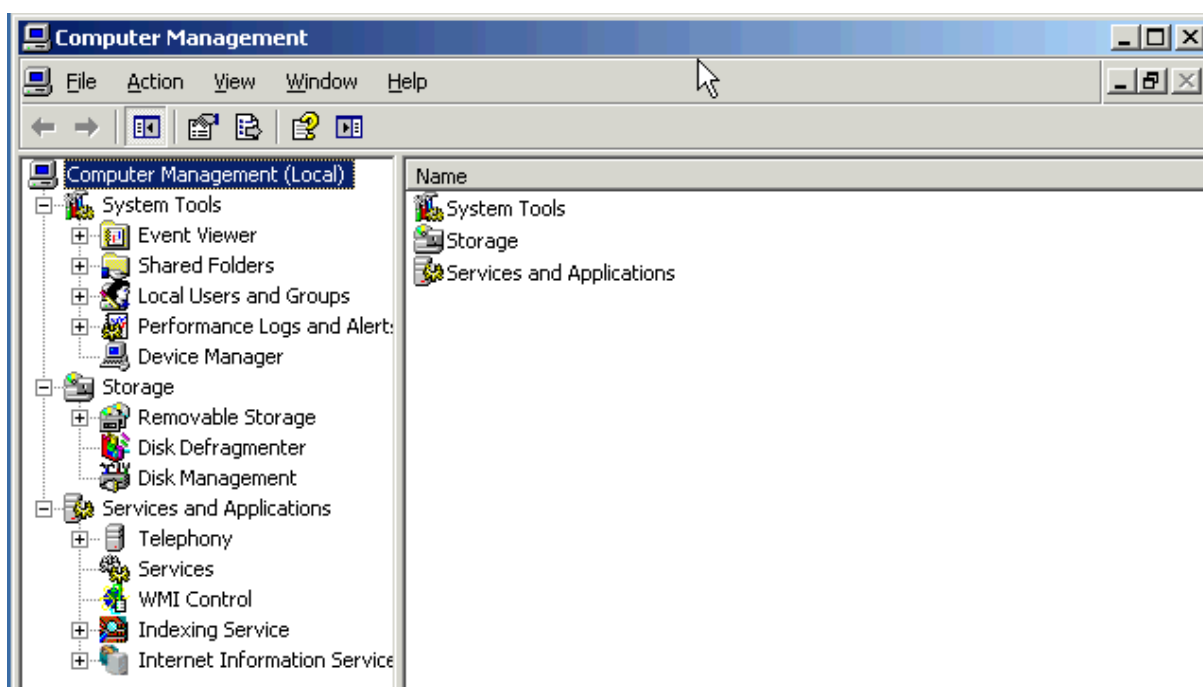
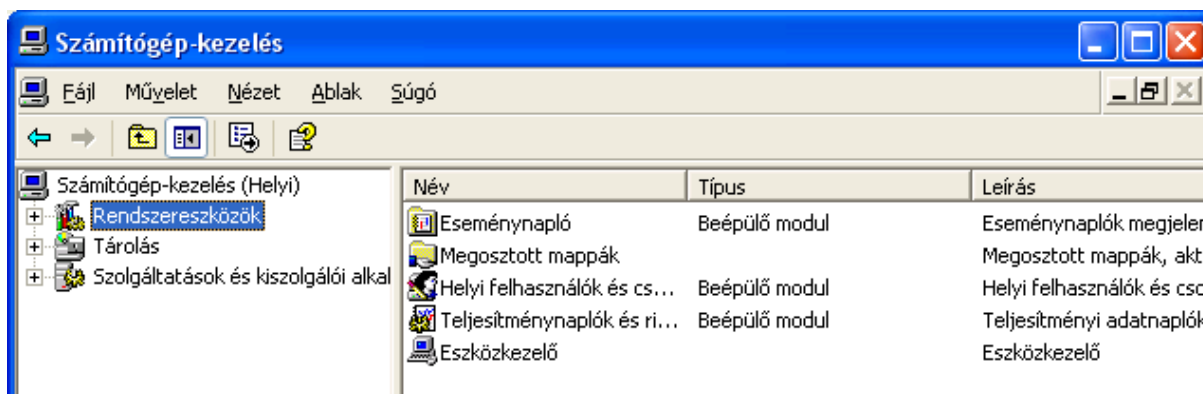
## Domain fogalmának tisztázása

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



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

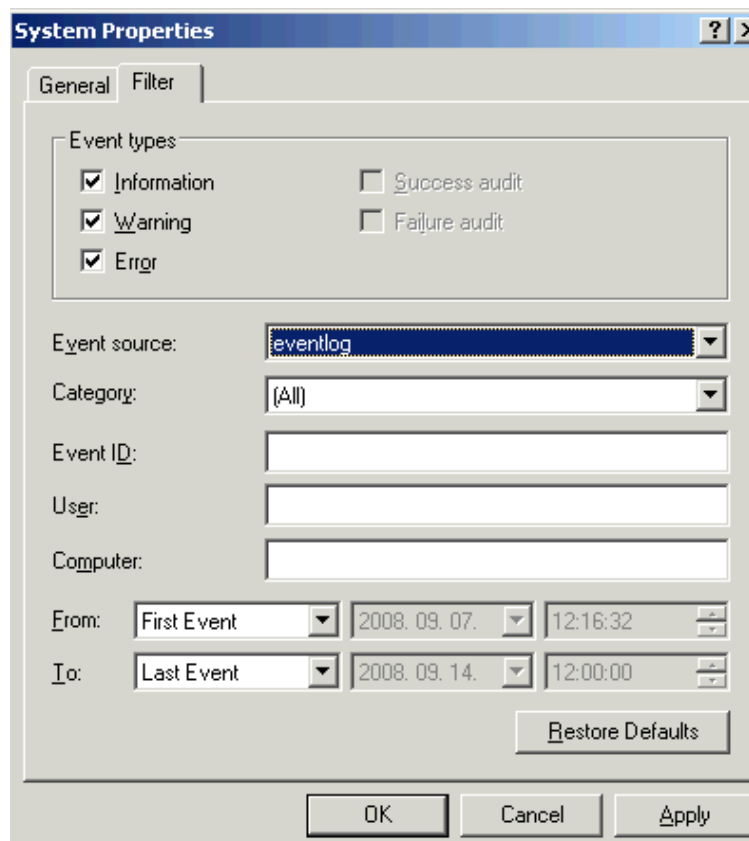
*Biztonsági-napló:* a sikeres és sikertelen események kerülnek ide.

*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.



Egyéb műveletek:

- Megnyitás.
- Mentés
- Export
- Logolás beállítása.
  - 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 felhasználók 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 hozzáféréseivel, 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.

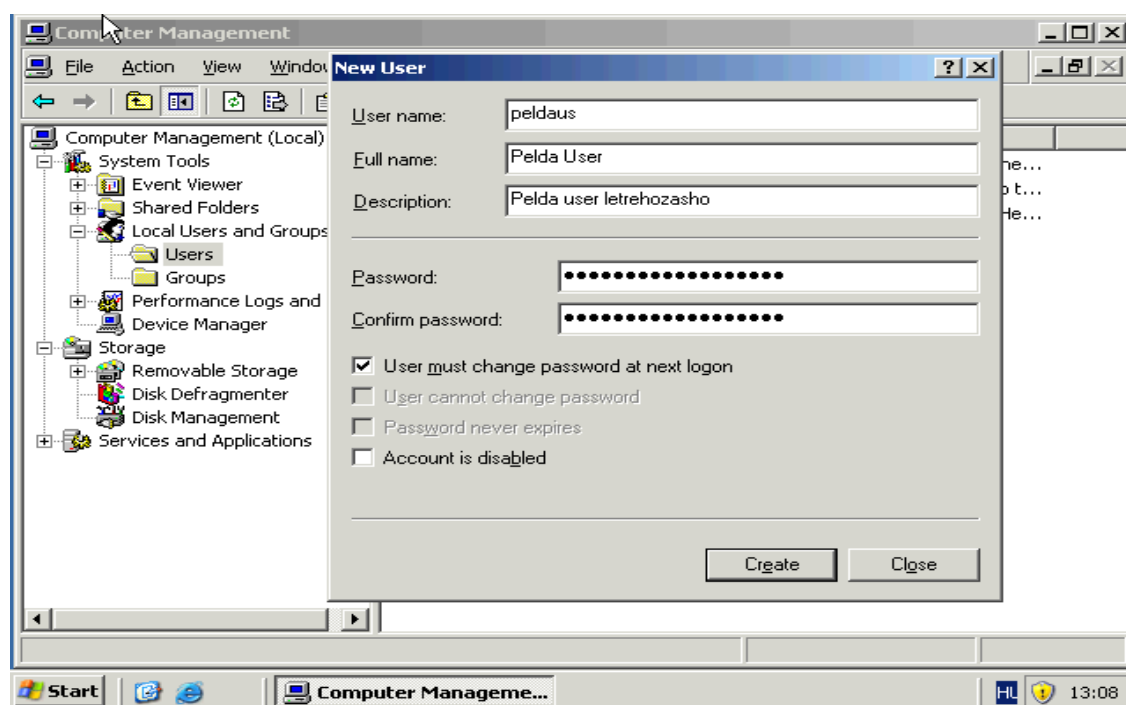
Nincs engedélyük ahhoz, hogy felvegyék magukat a Rendszergazdák csoportba, és nem férhetnek hozzá más felhasználók NTFS-köteten levő adataihoz, kivéve, ha ehhez megfelelő jogosultságot kaptak az adott felhasználótól.

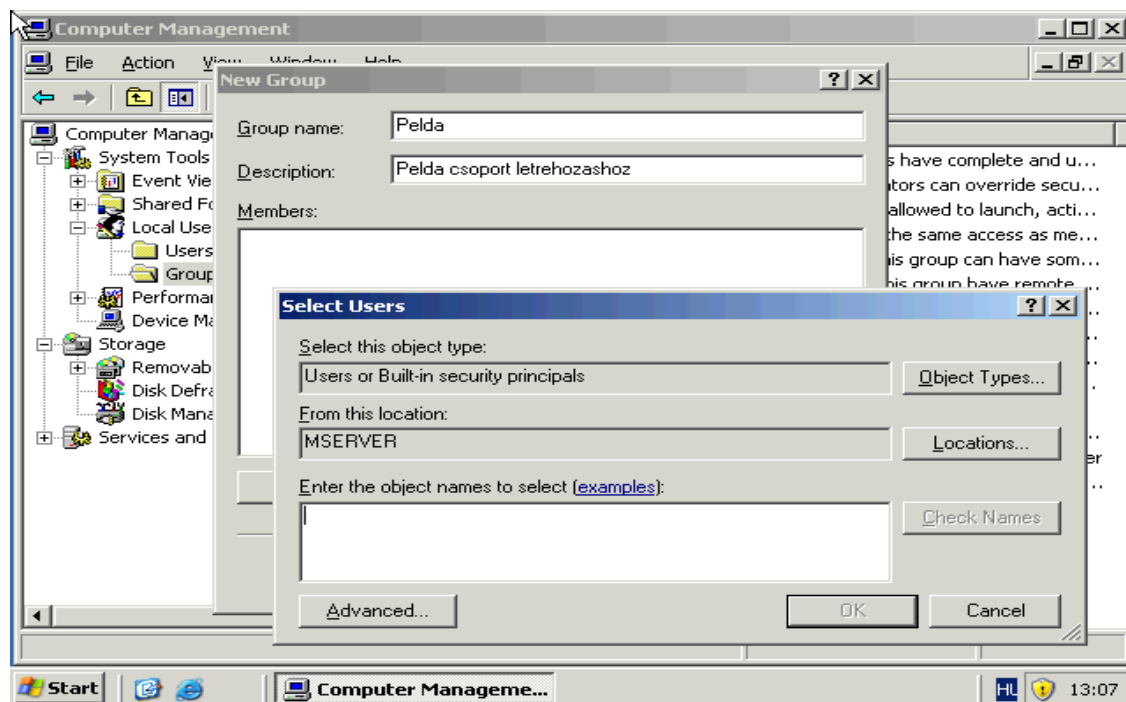
*Print Operators:* Kezelhetik a nyomtatók beállításait, illetve hozzáférési jogukat, de újat nem telepíthetnek.

*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.

Feladat: Példa felhasználók és csoportok létrehozására.



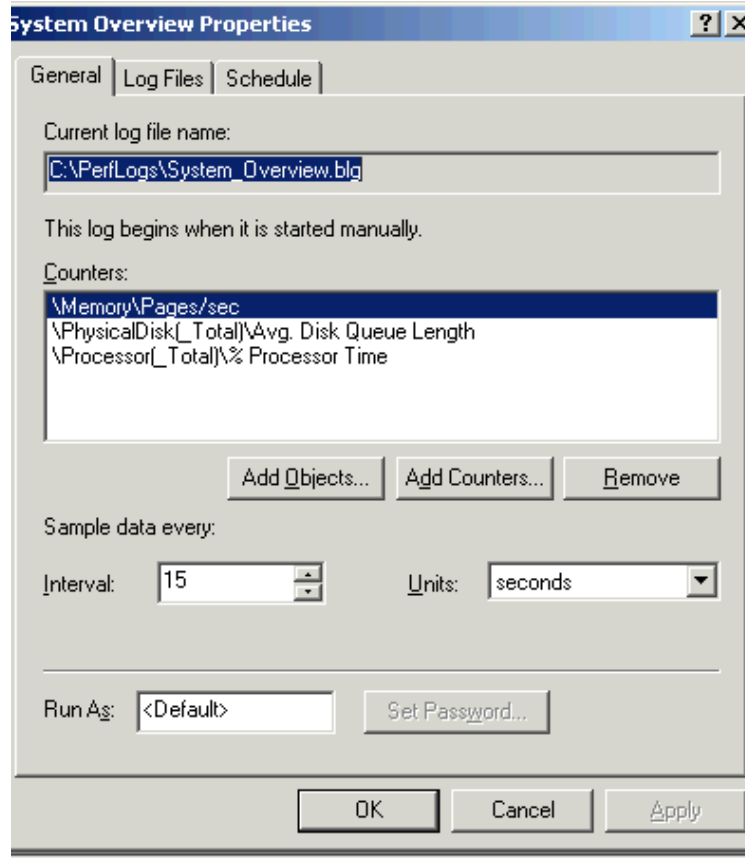


#### 4. Teljesítmény naplók és riasztások (performance logs & alerts)

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 grafikusán megjeleníteni.



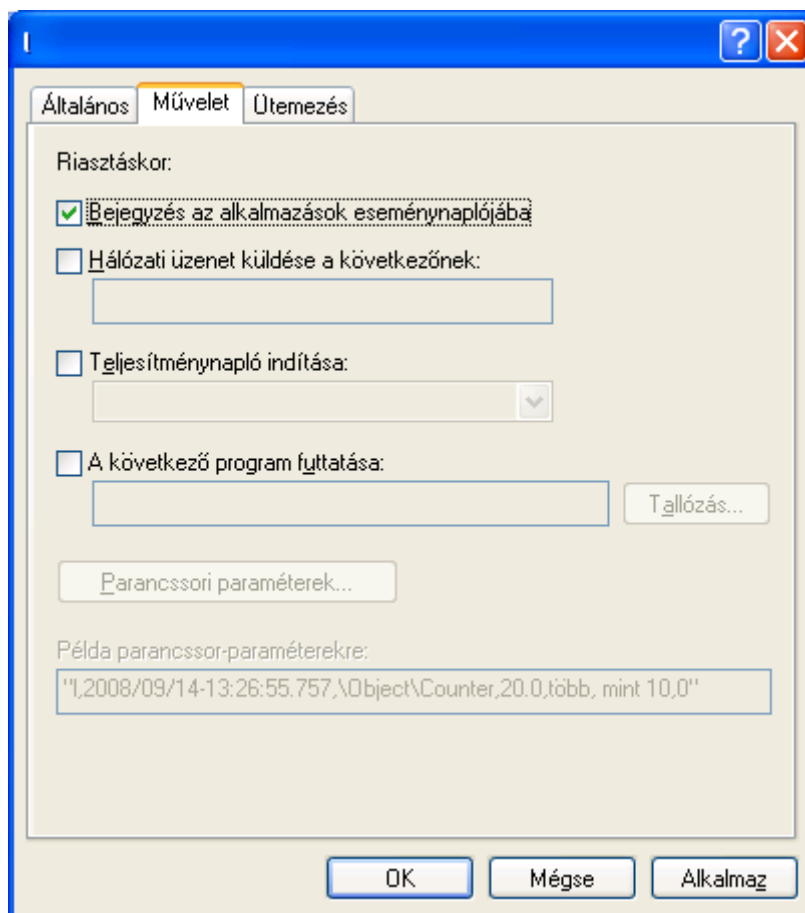
### *Nyomkövetési naplók (trace logs)*

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

### *Riasztások (alerts)*

Beállítható, hogy bizonyos esemény bekövetkezésekor riasztás „hajtódjon” végre.

Az esemény bekövetkezésekor a következő műveletek hajthatók végre.



## 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

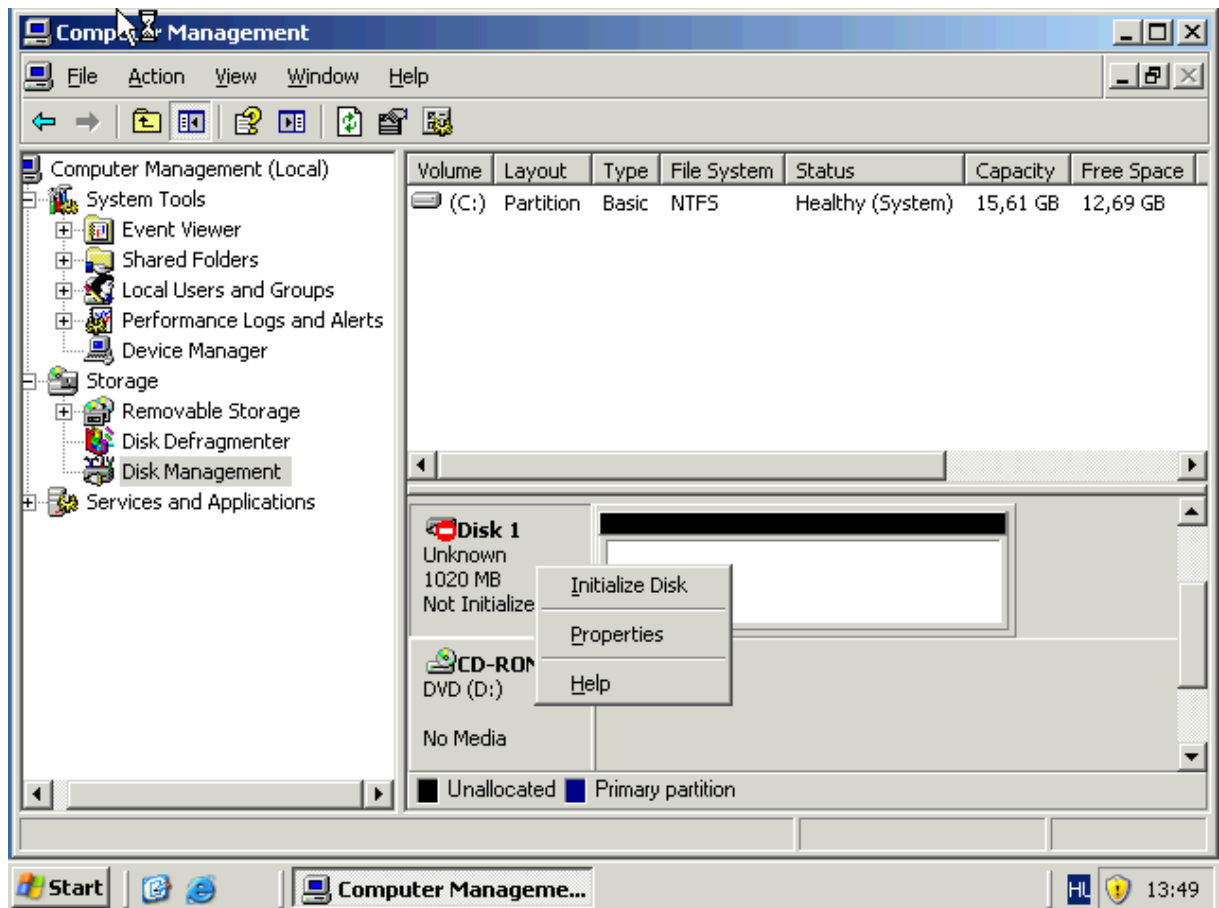
A Lemeztöredezettség-mentesítő egységesíti a számítógép merevlemezén talált töredezett fájlokat és mappákat, így minden fájl és mappa egyetlen összefüggő helyet foglal el a kötetben. Ennek eredményeként a rendszer hatékonyabban éri el a meglévő fájlokat és mappákat, és hatékonyabban



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.



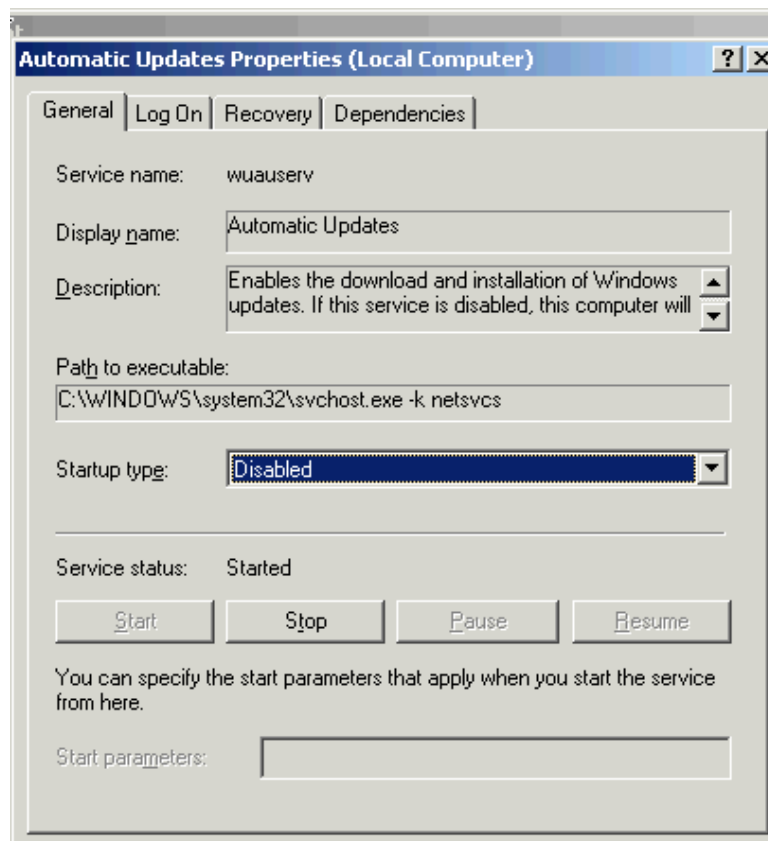
### III. Szolgáltatások és kiszolgálói

#### 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.



#### 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.

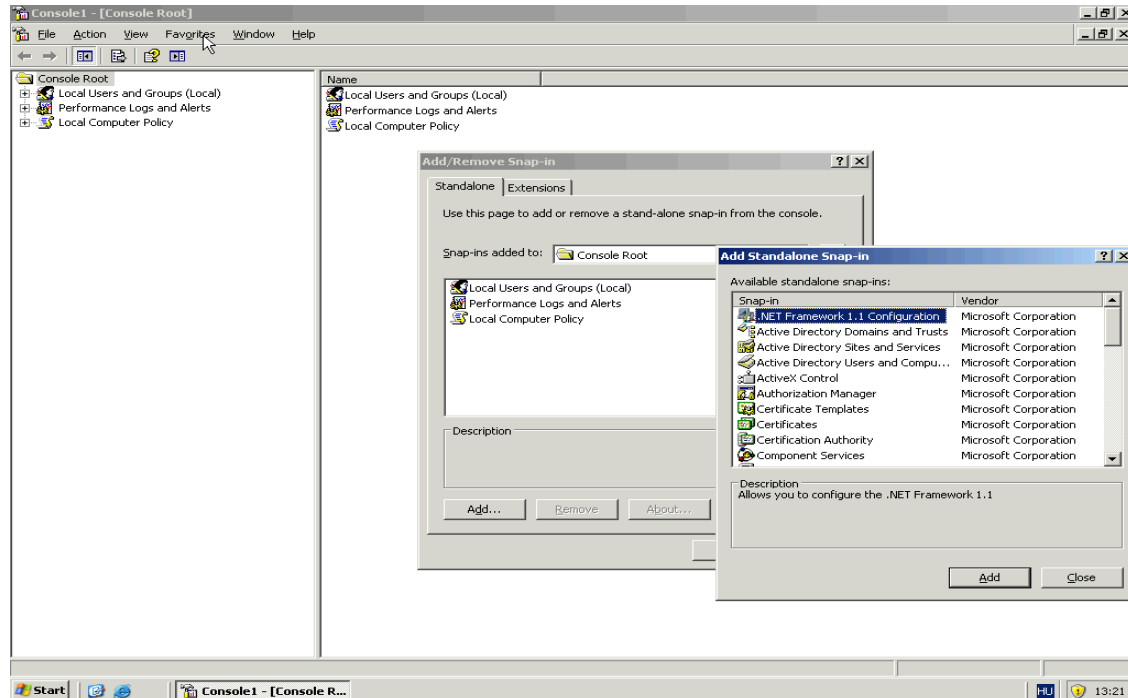
## A Microsoft Management Console használata

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 meglévő 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.



## 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:

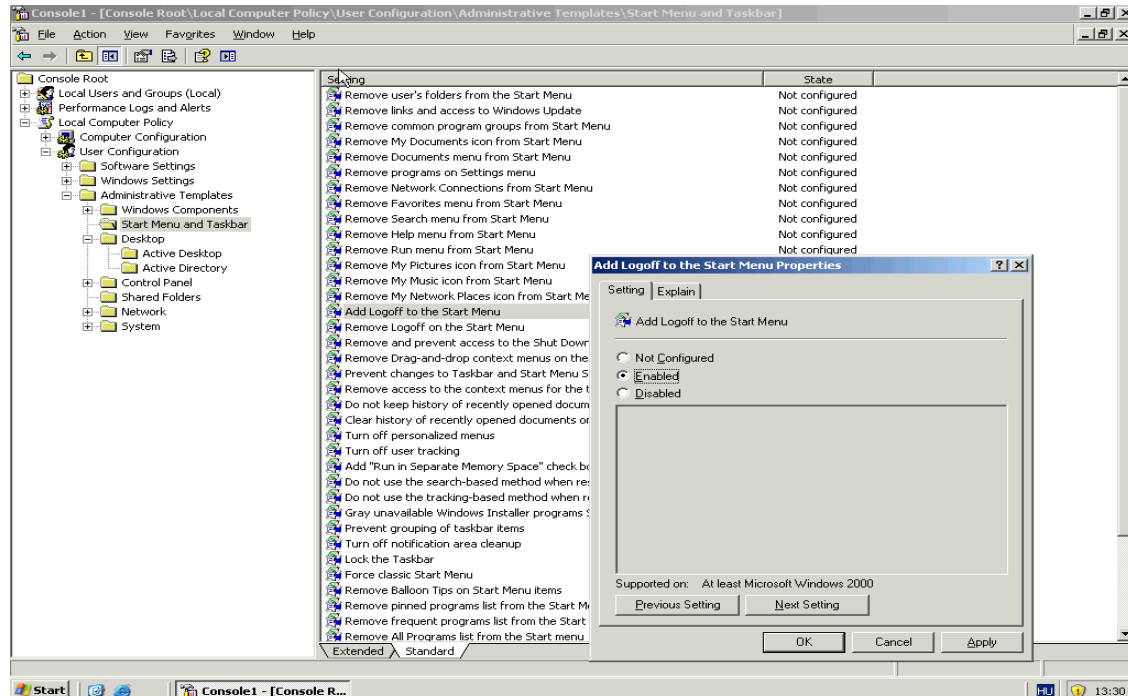
Startmenüből eltüntetni a shut down parancsot és megjeleníteni a logoff parancsot.

Remove & Prevent access to Shut Down

Remove Logoff on the Start menu

A policyknak 3 értéke lehet:

- Not configured
- Enable
- Disable

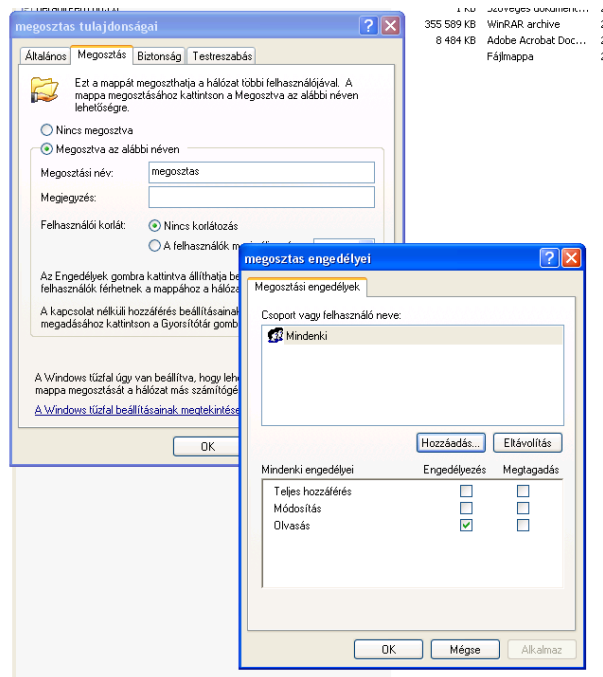


## Megosztások\Sharek létrehozása, jogosultságok beállítása:

### 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.



## Jogosultság állítások: mappákon

### Feladat: konkrét jogosultság beállítása egy felhasználónak a korábban létrehozott mappán.

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

- Share törlése.
- Mappa törlése.

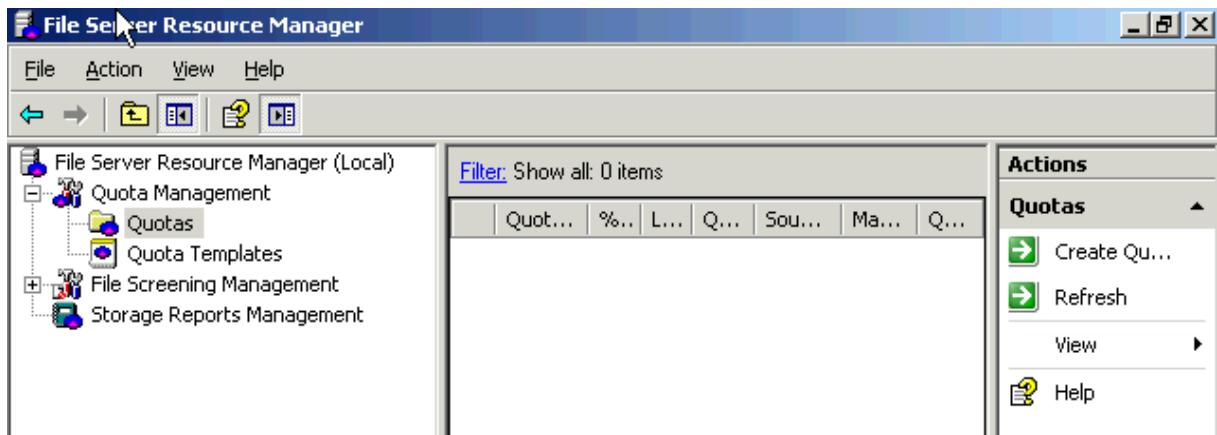
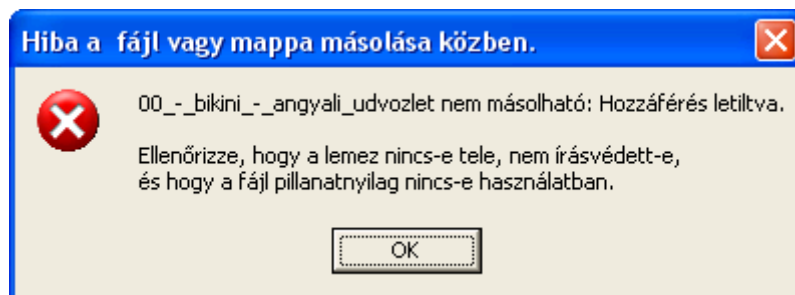
## További Management eszközök bemutatása

### 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 fájl típusokat adott mappákba nem tárolhatunk.



## **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 Properties\ Tulajdonságok**

- General: általános jellemzők
- Computer Name
  - Név megadás
  - Domainbe léptetés
  - Primary DNS suffix megadása
- Hardware
  - Device Manager
  - Drivers
    - Nem windows által tesztelt driverek
    - Mit tegyen, ha driver frissítés szükséges
- Advanced
  - Performance Option: CPU ütemezés, memória használat
  - 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 tartományi 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.

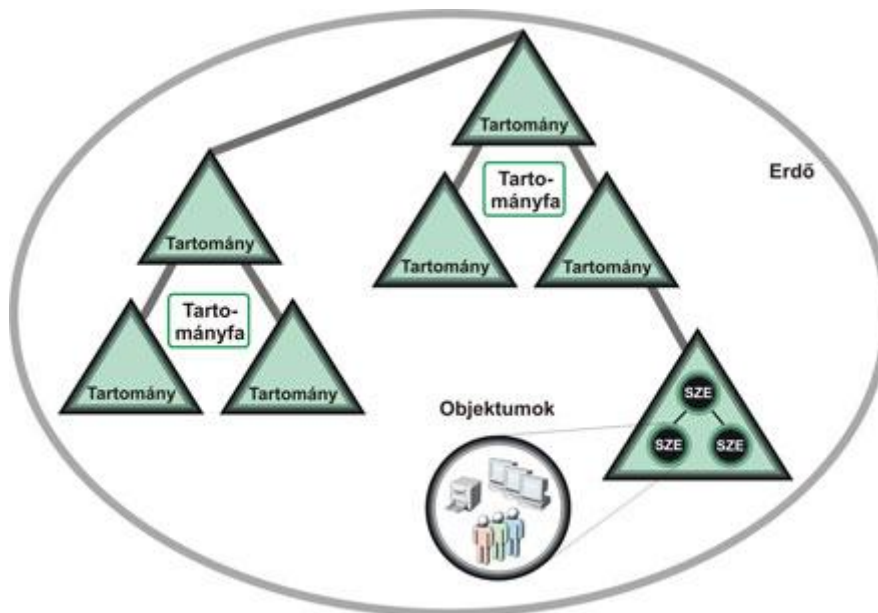


## Tree, Forest

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 katalógus nincs jelen minden tartományvezérlőn, csak néhány kitüntetetten.

### **Kitüntetett szerepkörök**

#### Tartomány feletti fő kiszolgálók:

##### 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.

##### Schema Master:

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

#### Tartományon belüli fő kiszolgálók

##### 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.

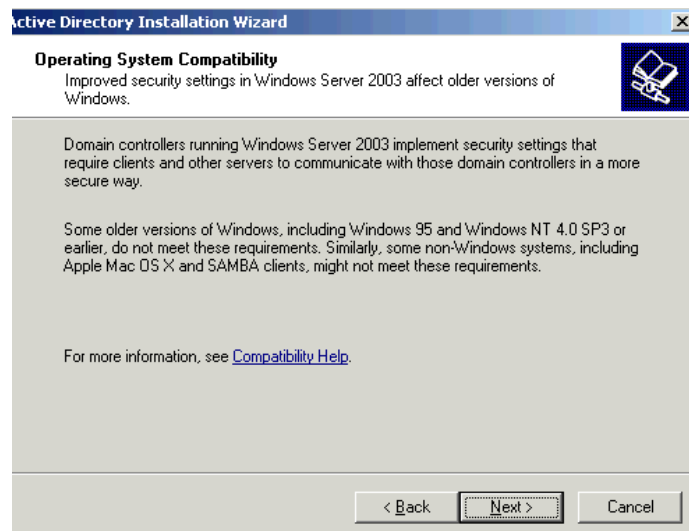
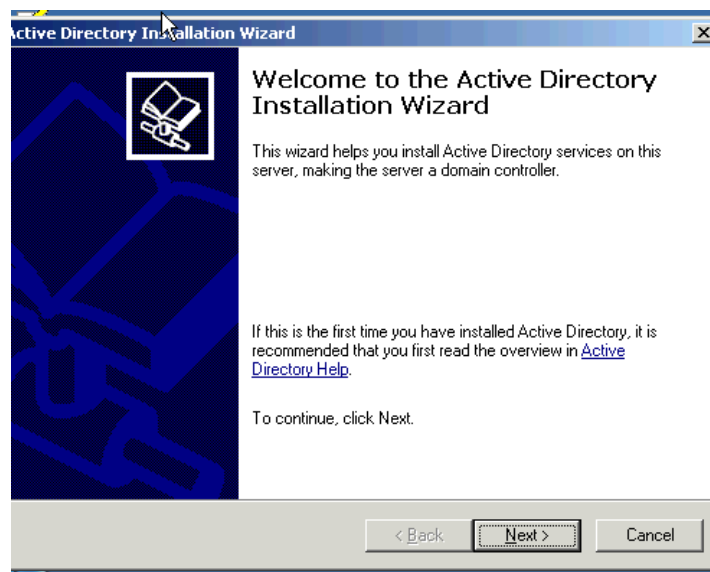
Ha nem telepítünk előre DNS-t, akkor az AD telepítésekor automatikusan települni fog egy DNS szerver is, és létrejön a DNS zóna is.

## Példa a TK-ból.

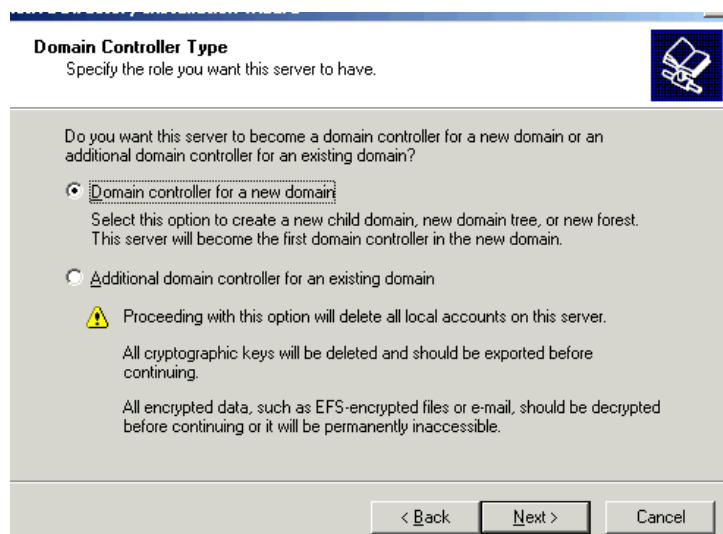
Szak.local tartomány első tartomány vezérlőjének telepítése. Ez a tartomány egy tartományfa gyökértartománya. Mivel a teljes erdőben az egyetlen tartományfa, ezért az erdő gyökértartománya is egyben.

## Telepítés menete:

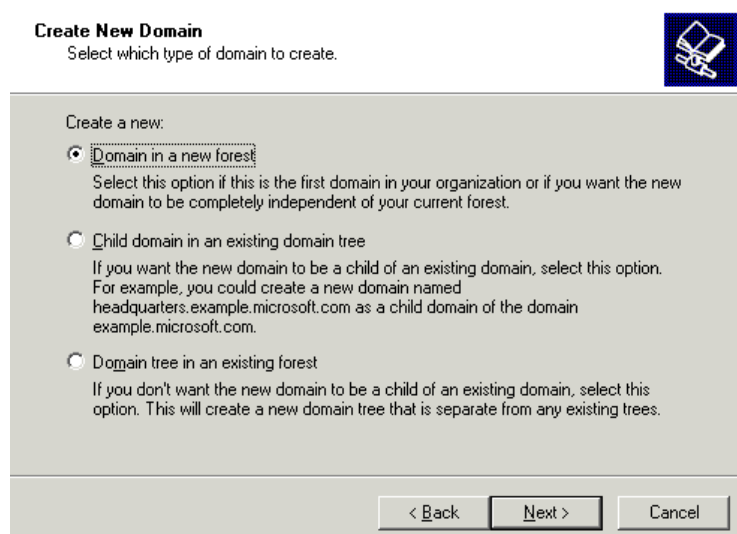
Startmenü\Run\DCPROMO: ez a program menüből nem érhető el.



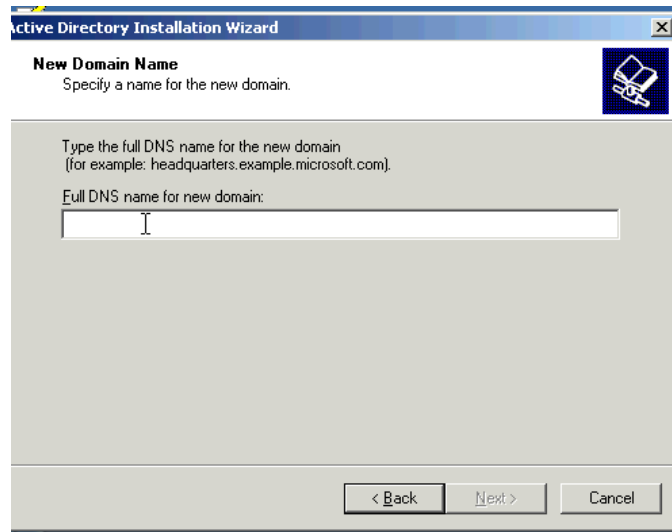
Figyelmeztetést kapunk, hogy a hálózatunkban levő Win95 és Win NT SP3 előtti kliensek nem fognak tudni bejelentkezni a hálózatba. Ennek oka az alapértelmezett biztonsági beállítások nem támogatják a nem biztonságos hitelesítést.



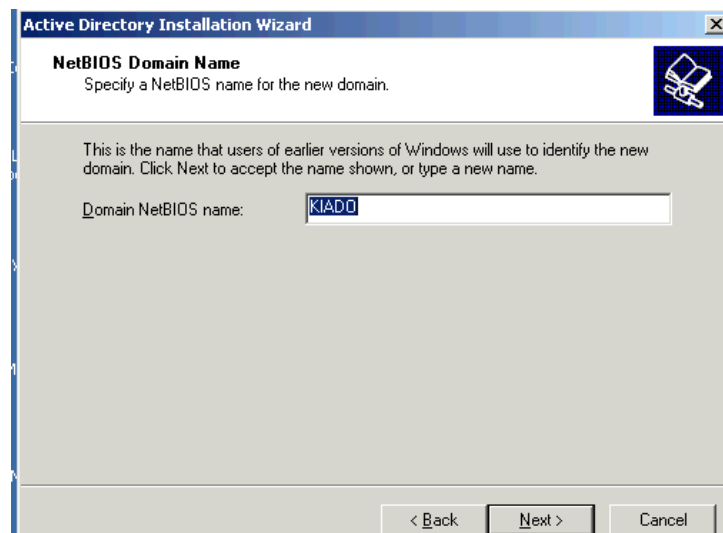
Választhatunk, hogy egy új Domain domain controllere lesz-e gépünk, vagy egy meglévő tartományba telepítünk-e tartományvezérlőt.



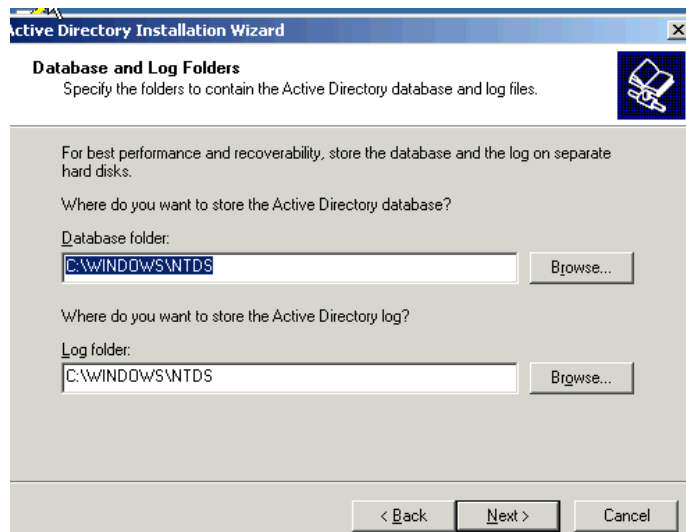
Azt is ki kell választanunk, hogy egy új tartományfát hozunk-e létre, vagy egy meglévő fa tartománya alá rendeljük.



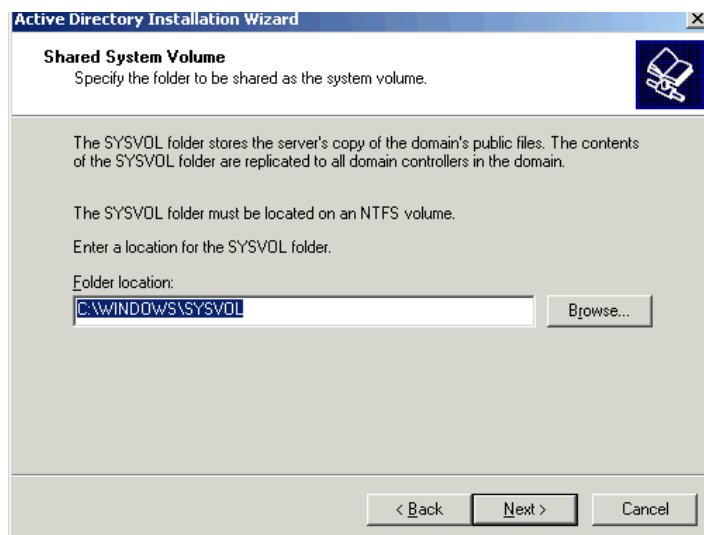
Tartomány teljes DNS nevének megadása.



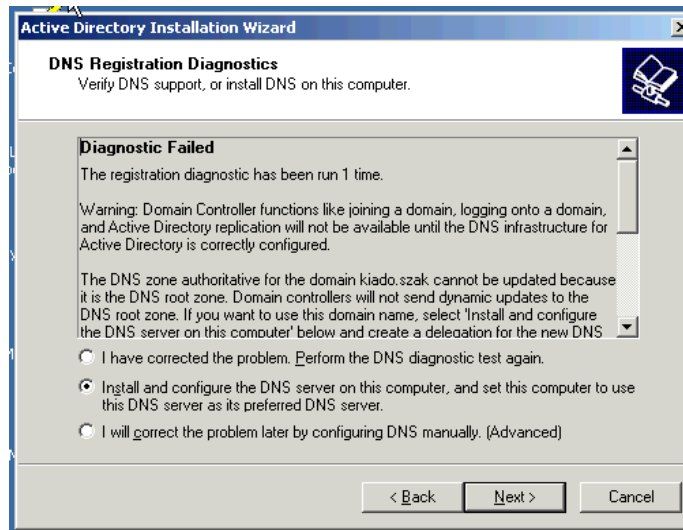
Tartomány Netbios neve: Tartomány régi típusú, NT-számára is értelmezhető név. (Max. 15 karakter hossz lehet).



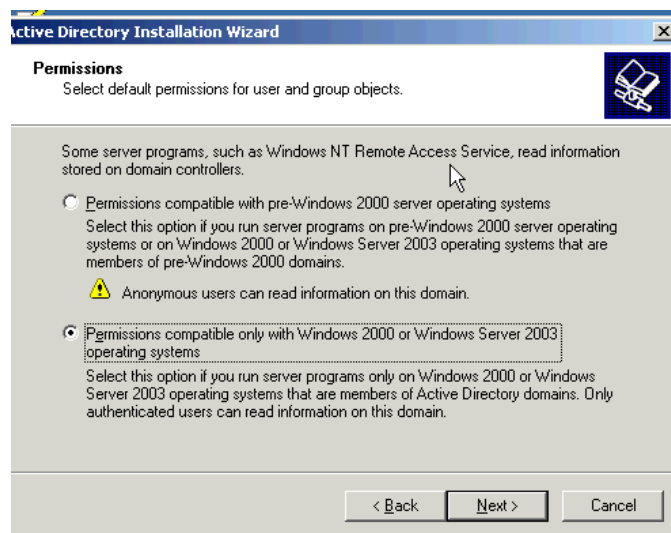
Adatbázis és a tranzakciós naplójának helye. Javasolt, nem az alapértelmezett helyen meghagyni, hanem egy másik rendszer partíciótól független partícióra tenni.



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

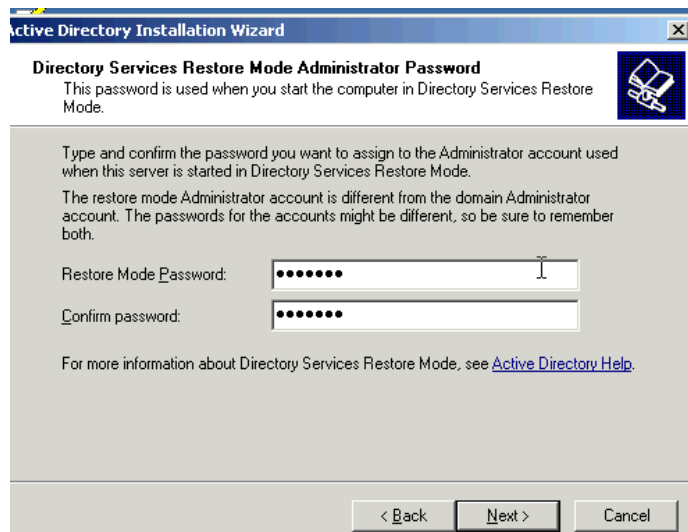


DNS kiszolgáló beállítása: Ha van DNS szerverünk, csak nem állítottuk be jól, lehetőségünk van ezt javítani. Telepíthetünk egy újat, ha nincsen.

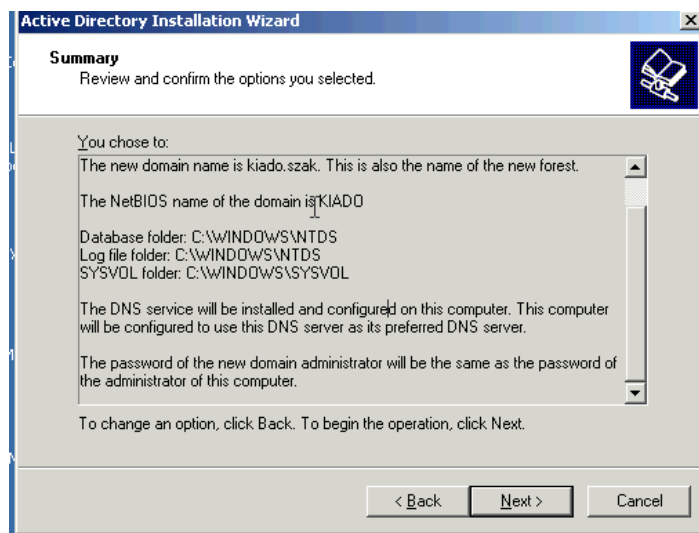


Meghatározzuk, hogy milyen hozzáférési jogok kerüljenek beállításra. Ez attól függ, van-e a tartományban W2K előtti kiszolgálók.





Rendszergazda jelszó megadása. Ez nem azonos a címtárbeli rendszergazda jelszavával. Vannak olyan karbantartási műveletek, melyek nem hajthatók végre, működő címtár mellett. 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.



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: tartományok közötti replikációk 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.

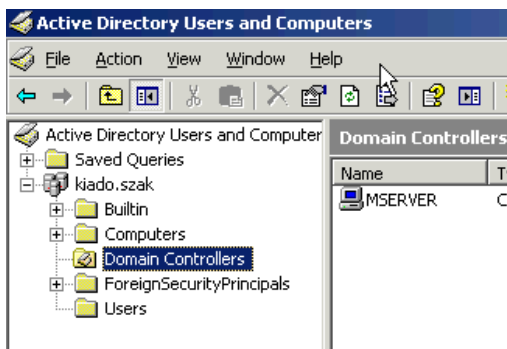
## **Active Directori Users & Computers (ADUC)**

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.

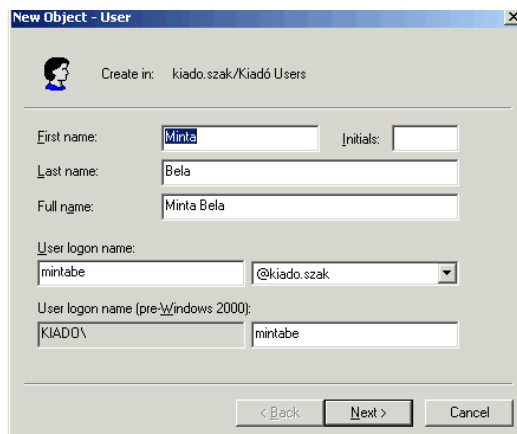
Alapértelmezett tárolók:



## Feladat: 3 OU / 2 AI OU létrehozása

Számítógépek  
Felhasználók  
Csoportok  
    Security  
    Disztribúciós

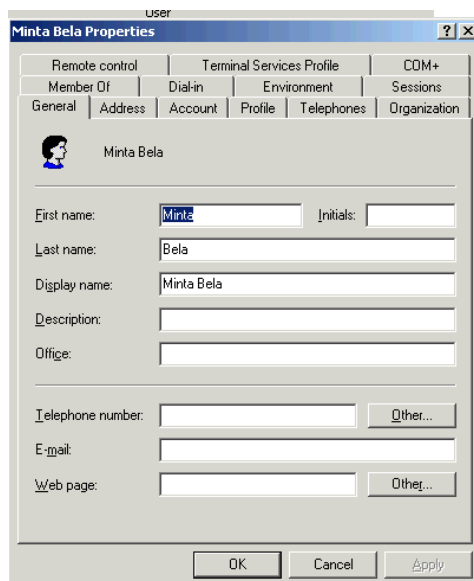
## Feladat: Felhasználó létrehozása:



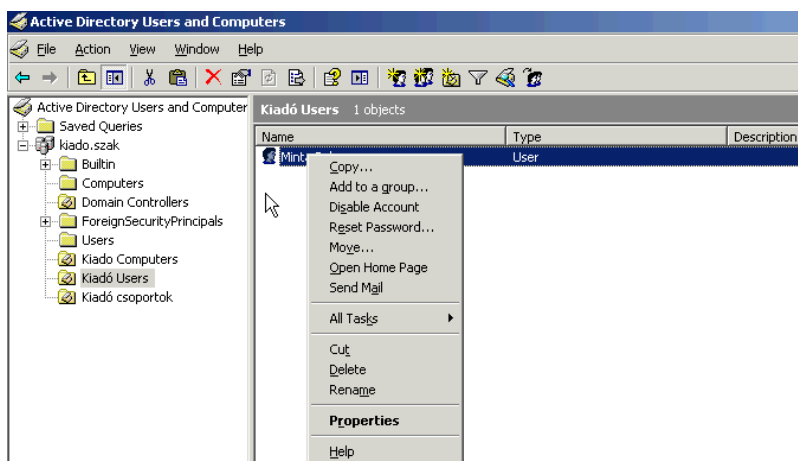
The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'kiado.szak/Kiadó Users'. The 'First name' field contains 'Minta', 'Last name' contains 'Bela', and 'Full name' contains 'Minta Bela'. The 'User logon name' field contains 'mintabe' and the domain dropdown is set to '@kiado.szak'. The 'User logon name (pre-Windows 2000)' field contains 'KIADD\mintabe'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

A felhasználó objektum legfontosabb attribútumai:

- GUID: globális egyedi azonosító
- SID: biztonsági azonosító
- Bejelentkezési név: mintabe
- Elsődleges felhasználó név: UPN: User Principal név: mintabe@kiado.szak
- Teljes név
- E-mail cím
- Jelszó
- Csoporttagság
- .
- .

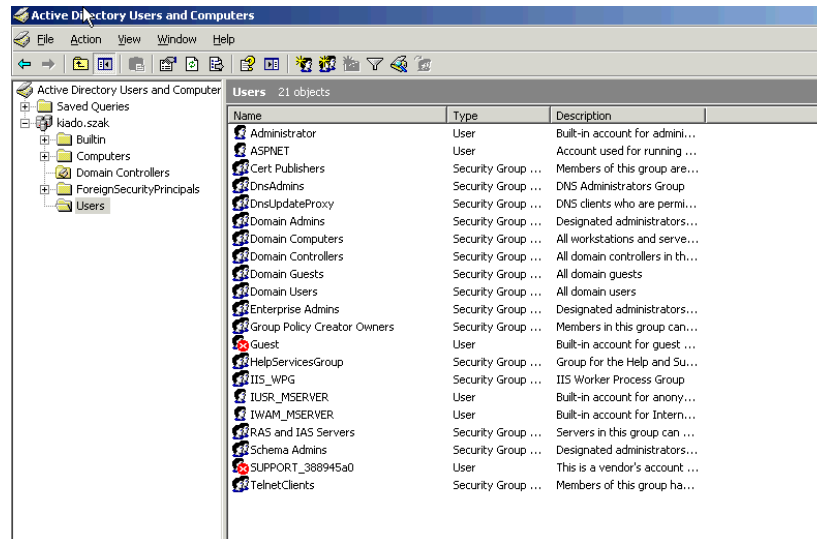


Legfontosabb műveletek felhasználókkal:



## Tartományi csoportok:

Users tároló alatt találhatóak a tartományi csoportok.



## Csoportok kezelése AD-ben:

*Type (típus)* szerint megkülönböztetett csoportok:

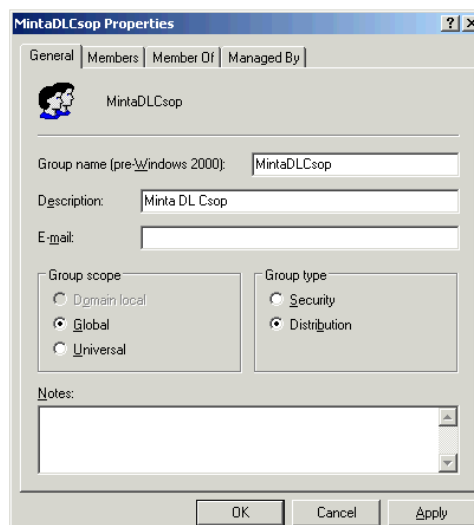
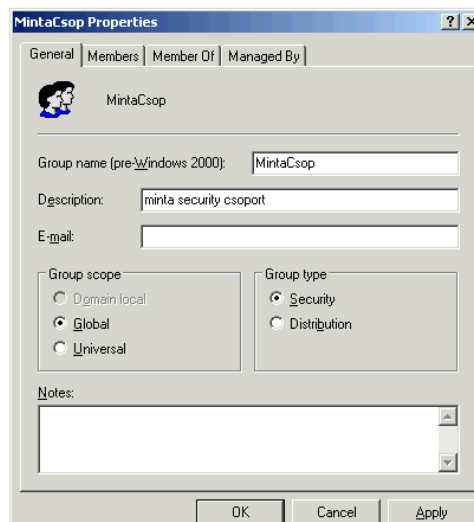
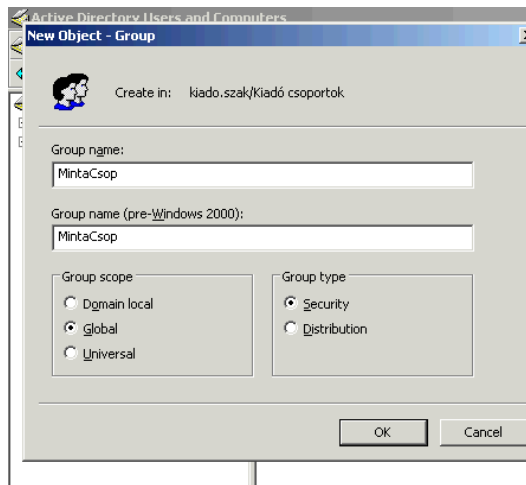
- Security (biztonsági) csoport—jogosultság állításhoz, erőforrás hozzárendeléshez
- Distribution (terjesztési) csoport—felhasználók összefogásához (csoportos levélküldéshez)

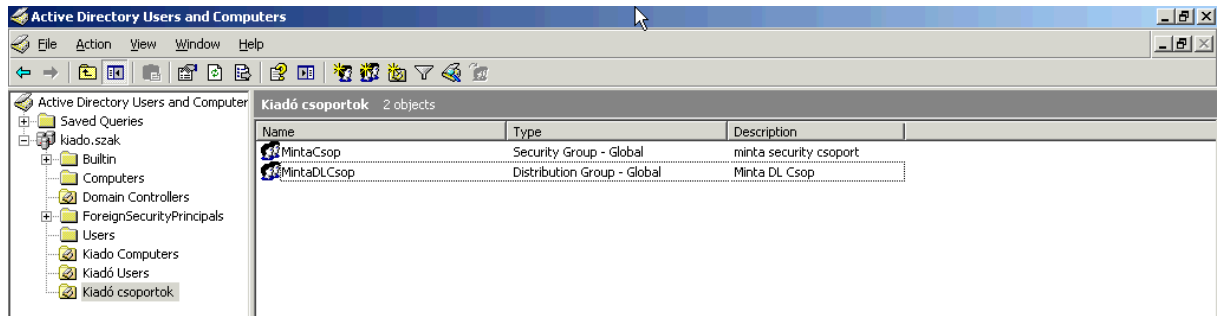
*Csoportok hatókör (scope)* szerint:

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 univerzál 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.

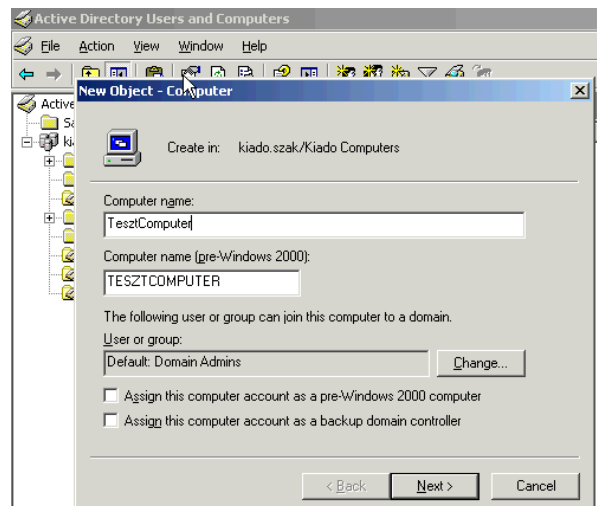




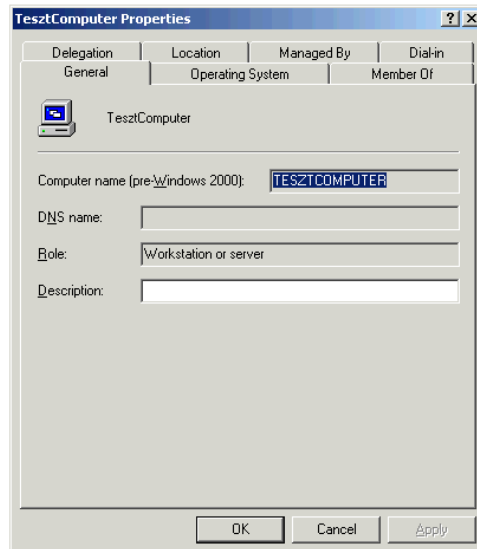
Legfontosabb tulajdonságainak ismertetése:

- Members
- Member Of
- Managed By

### Computer account létrehozása



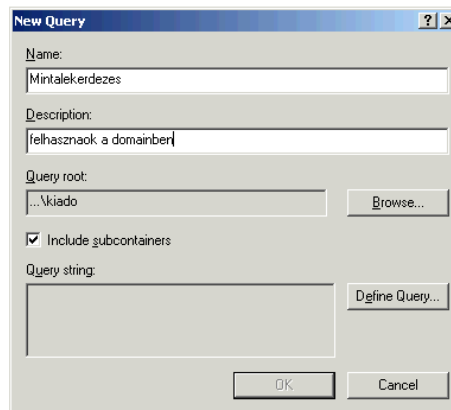


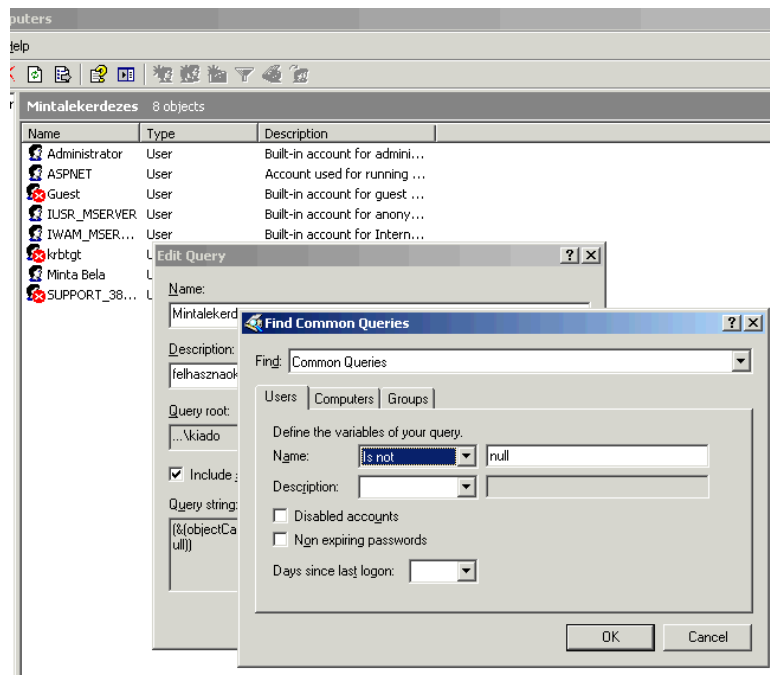


Tulajdonságai a computer tényleges domainbe léptetésével aktiválódnak. Ha nem hozom létre accountot a beléptetéskor a Computers tárolóba jön létre.

Lekérdezések:

Feladat: felhasználók listázására, lekérdezés készítése:



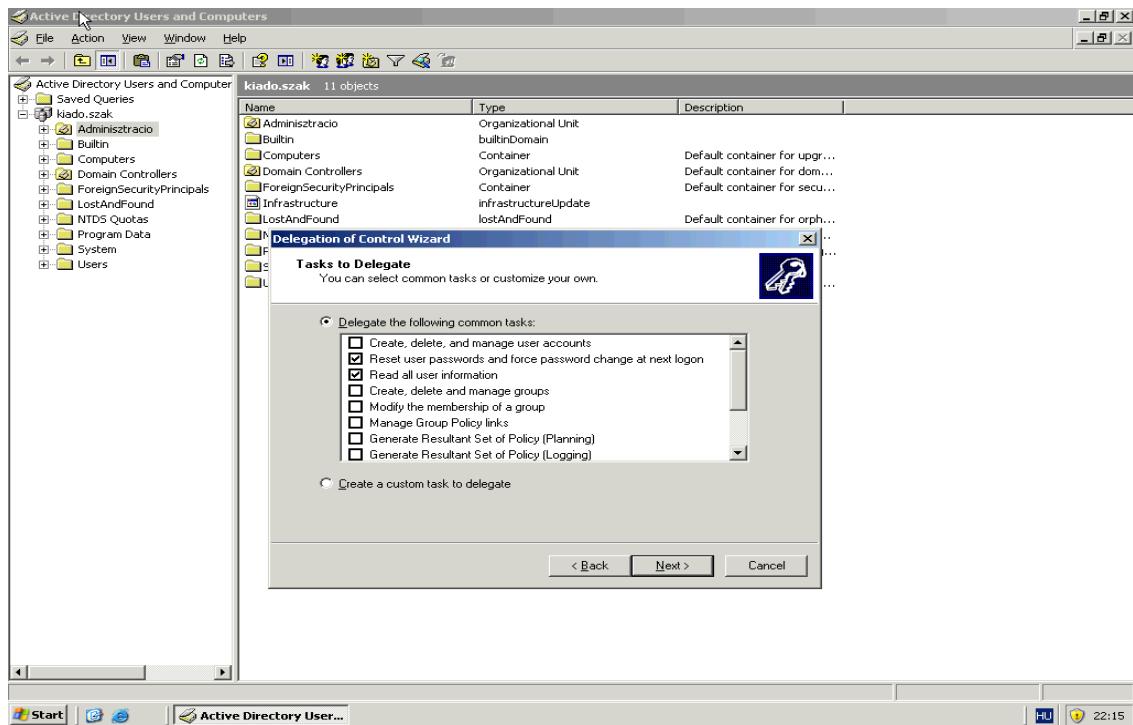


## Jogosultságok a címtár objektumokhoz

- Mindenki ahhoz férjen hozzá, amihez kell.
- Rendszergazdai feladatok megosztása lehetséges
- NTFS jogosultságokhoz hasonló jogosultság állítás
  - Felület
  - Öröklődés (kikapcsolható allow inheritable permission from)
- Minden objektumon állítható, de OUn szokás, különben átláthatatlan lesz a struktúra
- Properties\Security (speciális lehetőséget be kell kapcsolni: View\Advanced Features)
  - FC(Full Control)
  - R (Read)
  - W (Write)
- Jogok kiértékelődése
  - Összeadódnak a jogosultságok
    - Deny+Allow= Deny a tiltás mindig erősebb

## Delegálás

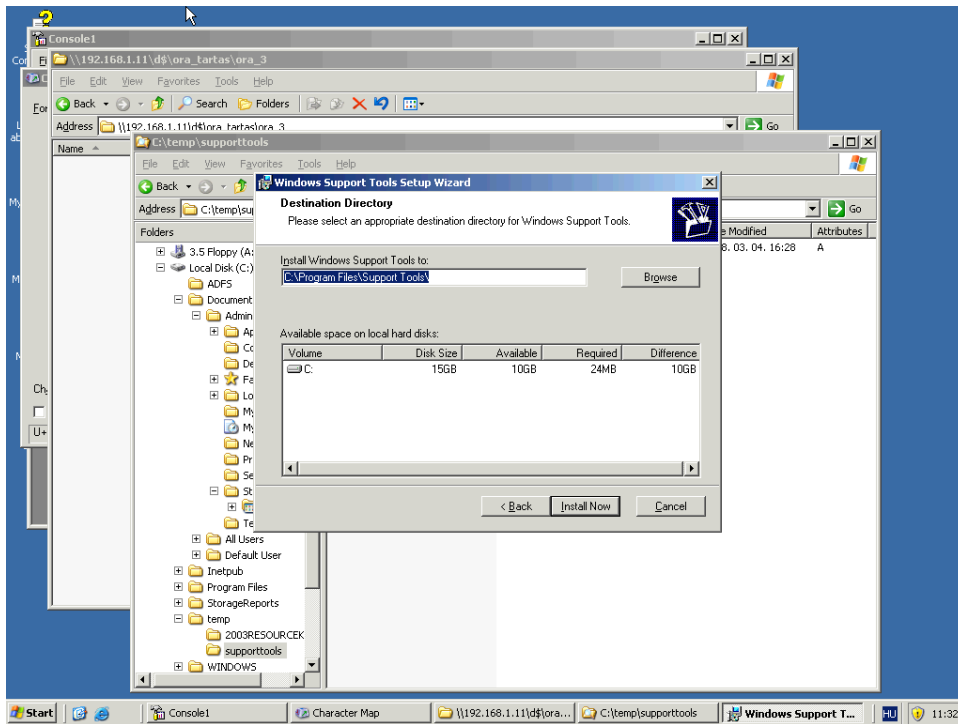
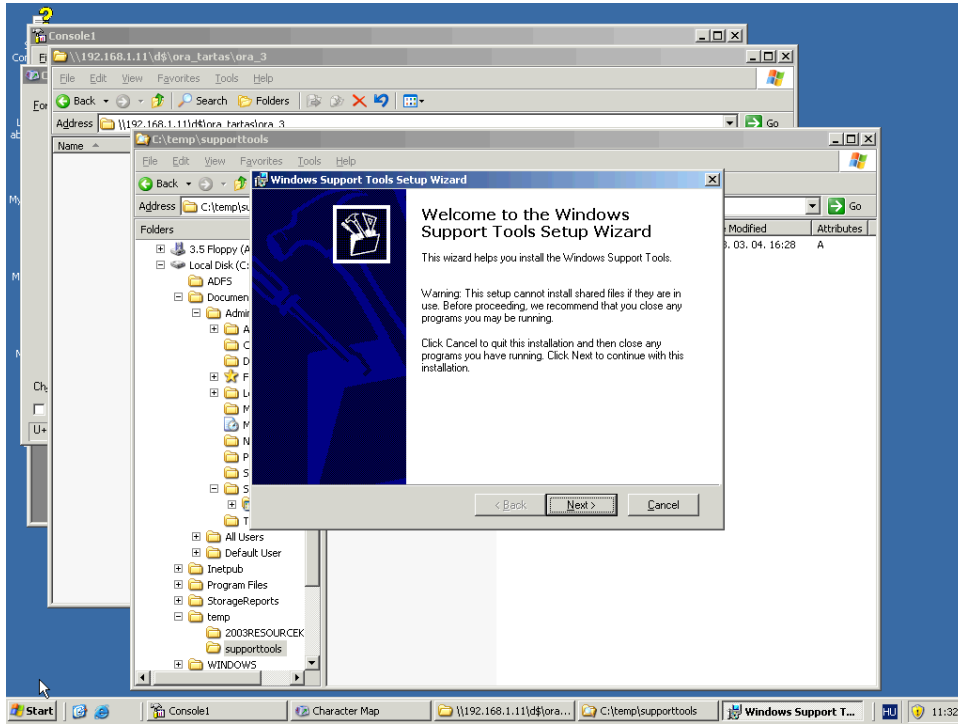
- ADUC \ OU segéd menü: Delegate Control
  - Felhasználók hozzáadása
  - Jogosultság meghatározása, mely műveletek elvégzésére jogosult
    - Delegate the following Common Task
    - Create custom task to delegate



## Support tools

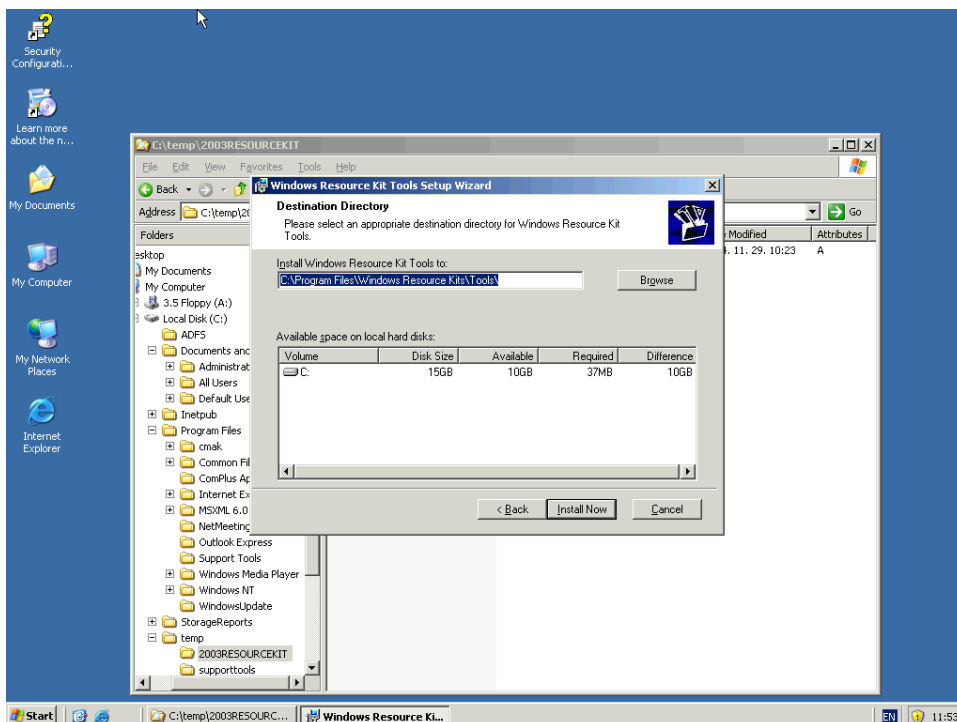
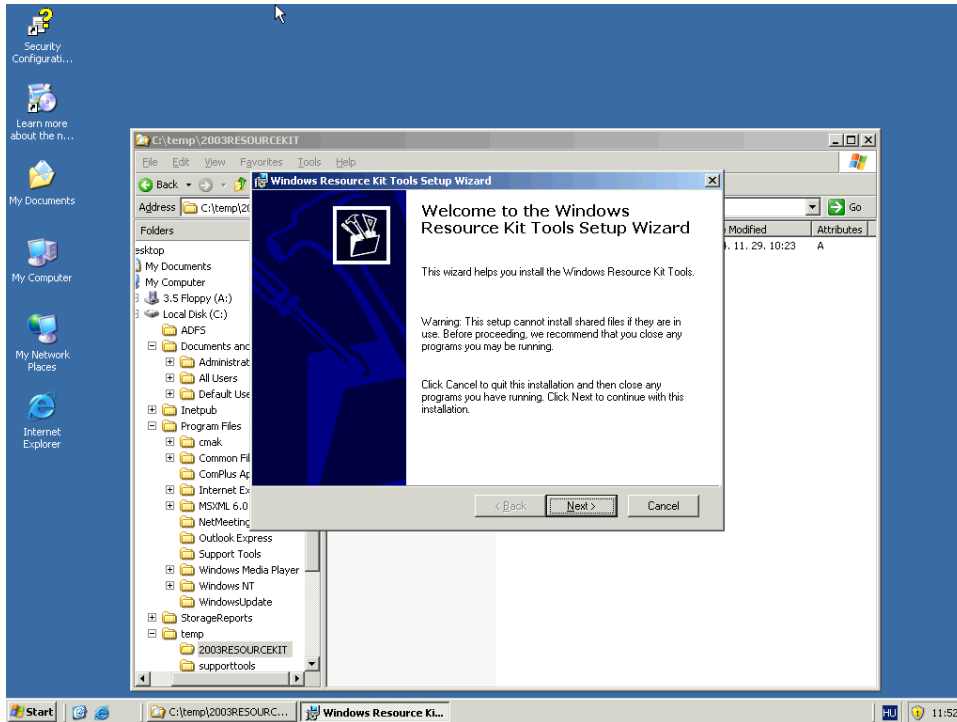
A Support Tools egy segédprogram gyűjtemény, mely megtalálható minden Windows 2000-es és XP-s telepítő lemezen. A csomag része számos diagnosztikai, biztonsági és a mindennapi munkát megkönnyítő program. Vannak köztük parancssorból elérhetőek és grafikus interfésszel rendelkezők egyaránt. A repertoárban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

# Installálása:



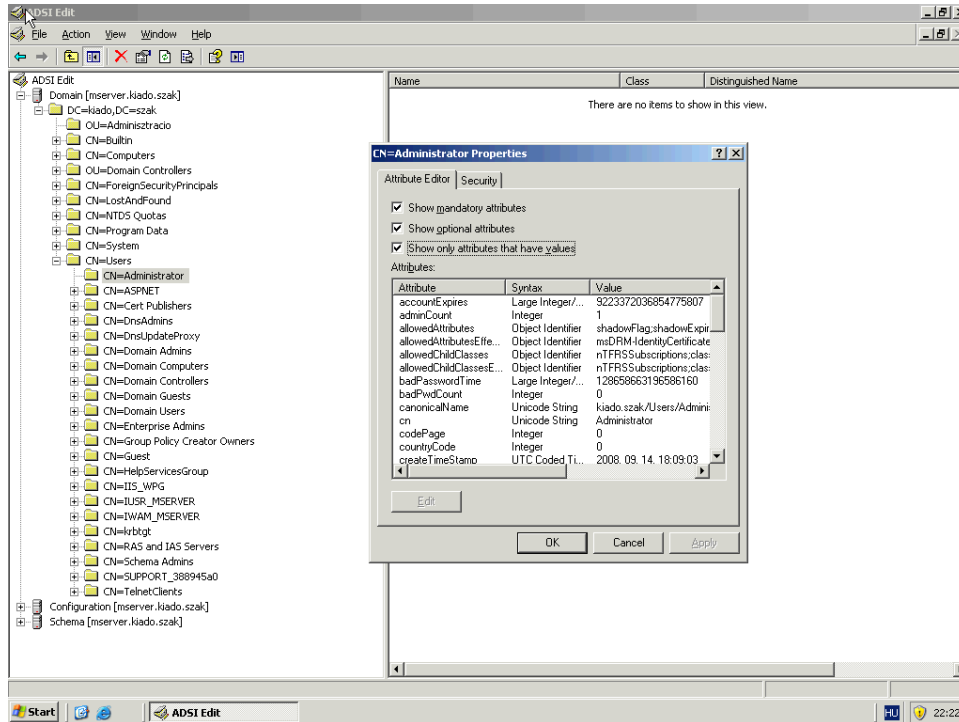
## ResourceKit

További alkalmazások, kiegészítő programok találhatóak a ResourceKit csomagban.



## ADSI Edit

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



## LDAP: Lightweight Directory Access Protocol

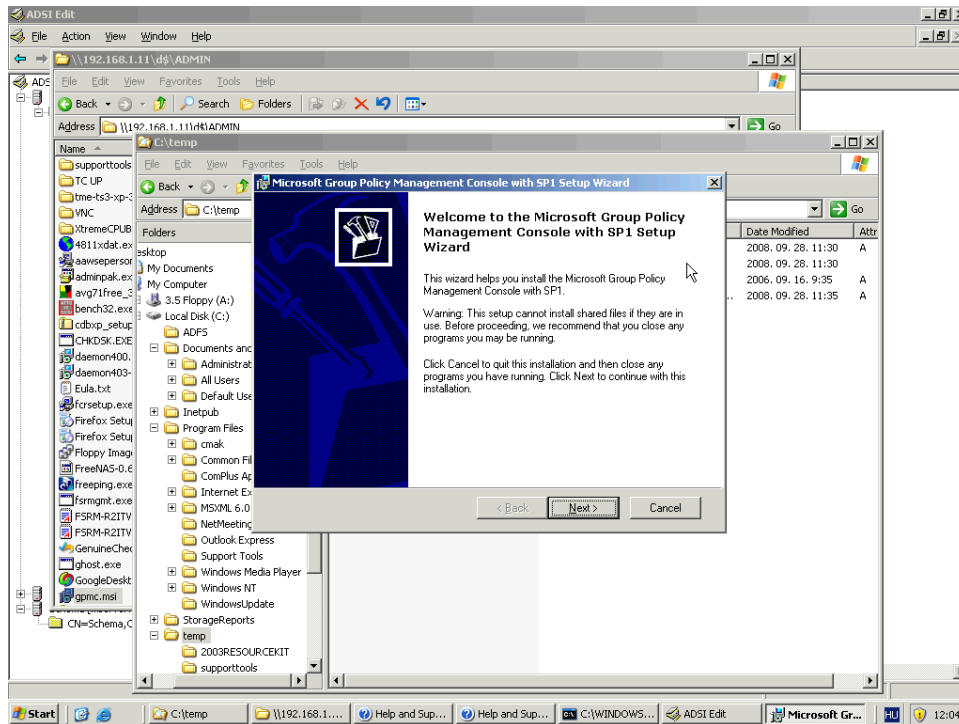
Directory szolgáltatások elérését szabályozza, ahol gyakoriak a keresések, de a struktúra változás nem gyakori.

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
  - 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 bizonyosságot 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.
2. 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 DNS-lekérdezéssel 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.



## Replikáció

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 megtalálható 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 („hídfeállítás 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.

## **Csoportházi rend**

Az Active Directory alkotta hálózatokban, Windows 2000 és XP munkaállomásokkal a Csoportházi rend (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 csoportházi rend 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 csoportházi rend akkor használható jól, ha több gépre ugyanazon beállításokat szeretnénk használni, nem pedig minden gépre sajátos beállítást alkalmazunk.

A csoportházi rend 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 Csoportházi rend, ez irányítja a programok telepítését, biztosítja a munkaállomások biztonsági és környezeti beállításait.

### Csoportházi rend-objektumok

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

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

Minden csoportházi rend-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 csoportházi rend is érvényesülhet, melyeknek „összege” adja meg a tényleges beállításokat. Az összeg azt jelenti, hogy minden olyan beállításra hatással lesz a csoportházi rend, amelyek valamelyik csoportházi rend-objektumban definiálva vannak. Természetesen itt vigyázni kell az öröklődésre, hiszen egy beállításra csak egy definíció fog érvényesülni.

### **A csoportházi rend-objektumok hozzárendelése szervezeti egységekhez.**

A csoportházi rendek 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.

### **A különböző programok automatikus telepítése csoportházirend segítségével**

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 software) az IIS az egyik legjobb webkiszolgáló a Microsoft platformjára.

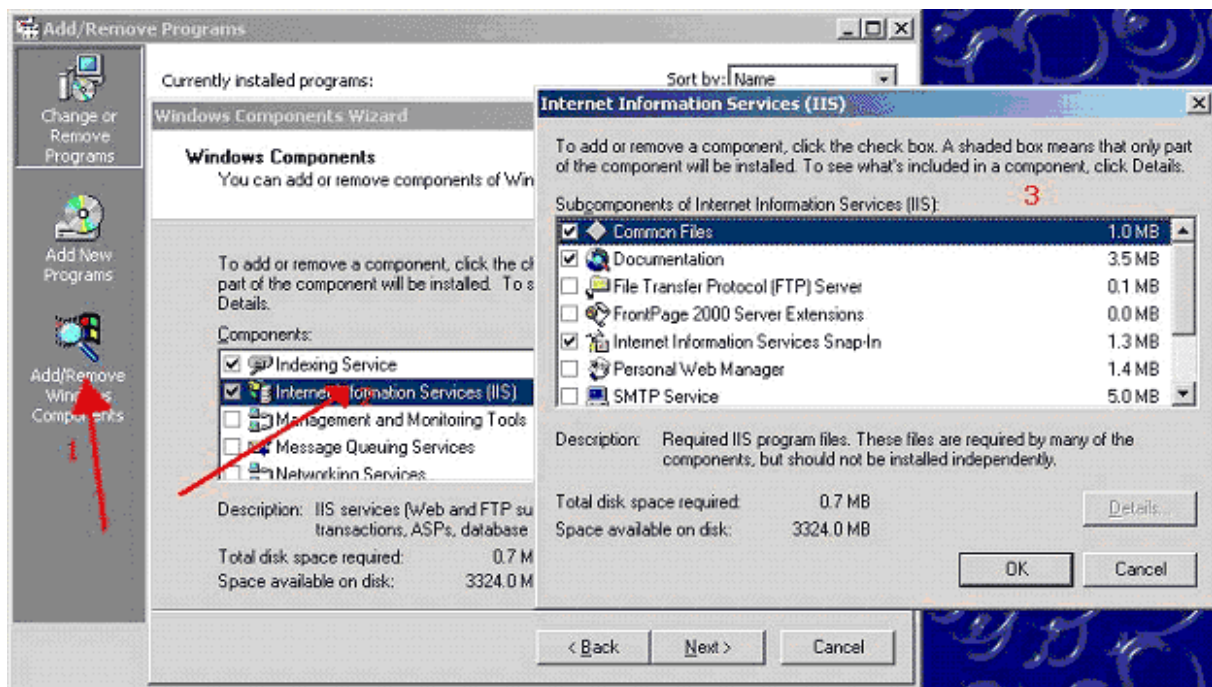
Az IIS a Windows NT, Windows 2000, és Windows XP operációs rendszerekben is megtalálható, de nem része a Windows95/98/ME, és a Windows XP Home rendszereknek.

Telepítése a következőképpen zajlik:

Programok Telepítése/törlése \ Windows összetevők \ IIS

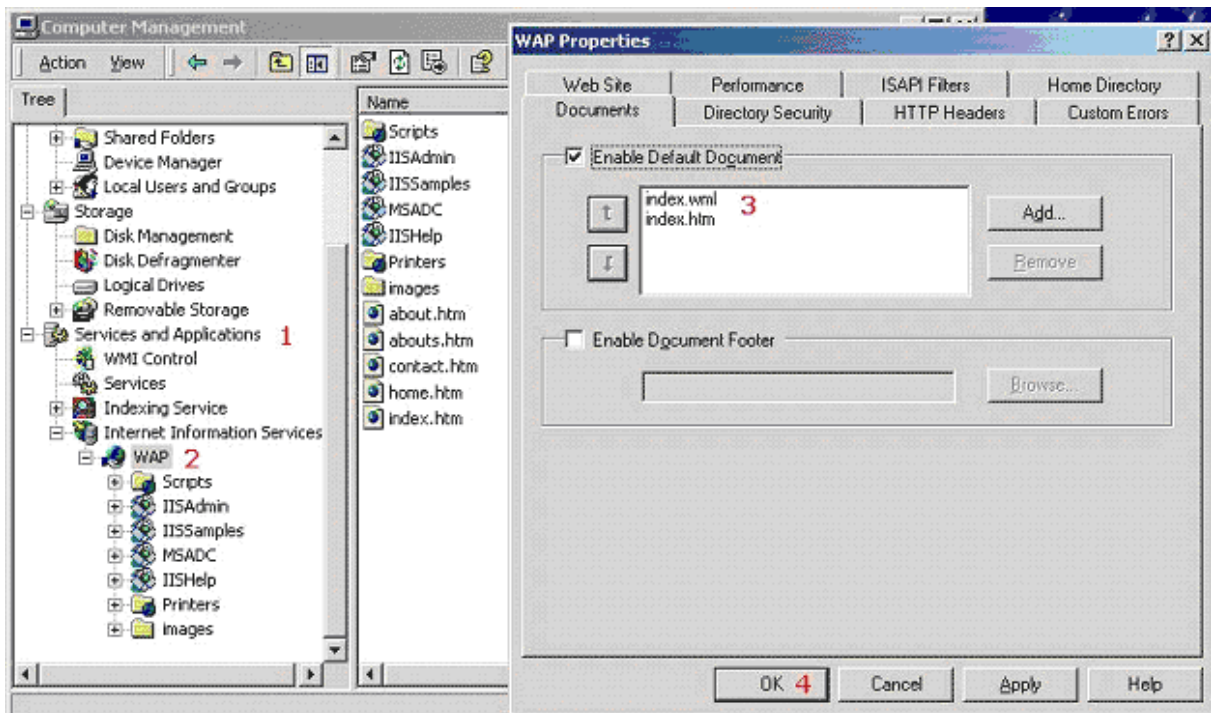
Ezen belül számtalan plusz telepíthető beépülőt találunk melyek az IIS sokoldalúságát szolgálják.

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



Az IIS a weblapokat a `c:\InetPUB\www_root` könyvtárból hoztolja alapértelmezetten, ez telepítéskor 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.



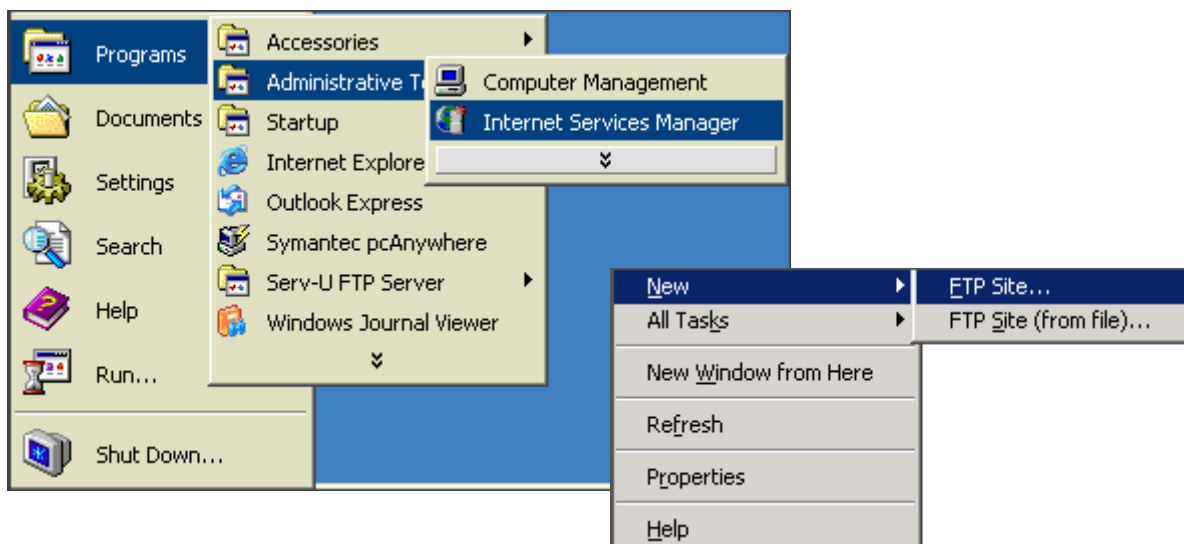
A szerver elindítását már csak a saját weblapunkra kattintva és a szolgáltatások ablakban az elindít gombot lenyomva érhetjük el.

Ellenőrzésképpen a web böngészőnkbe írjuk be:

*http://{ a gép IP címe }*

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.

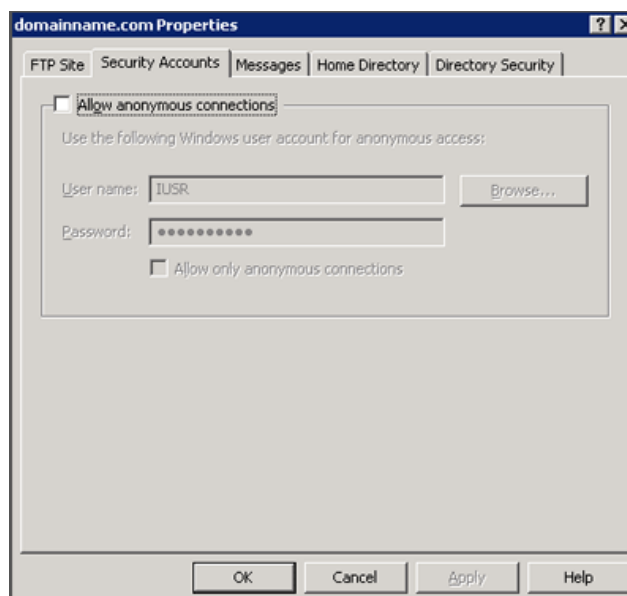


Az új FTP varázsló végigvezet bennünket azokon a lépéseken amelyek feltétlen fontosak az ftp szerver üzemeltetéséhez.

Ezek sorra a következők:

- Az FTP szerver leírása
- Az FTP szerver IP címe, és alapértelmezett portja
- A következő oldalon több választási lehetőségünk van,
  - A ftp felhasználóit el lehet különíteni a windows 2003 felhasználótól, így létre lehet hozni olyan csoportot mely használhatja az FTP szervert de nem tud belépni a 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.

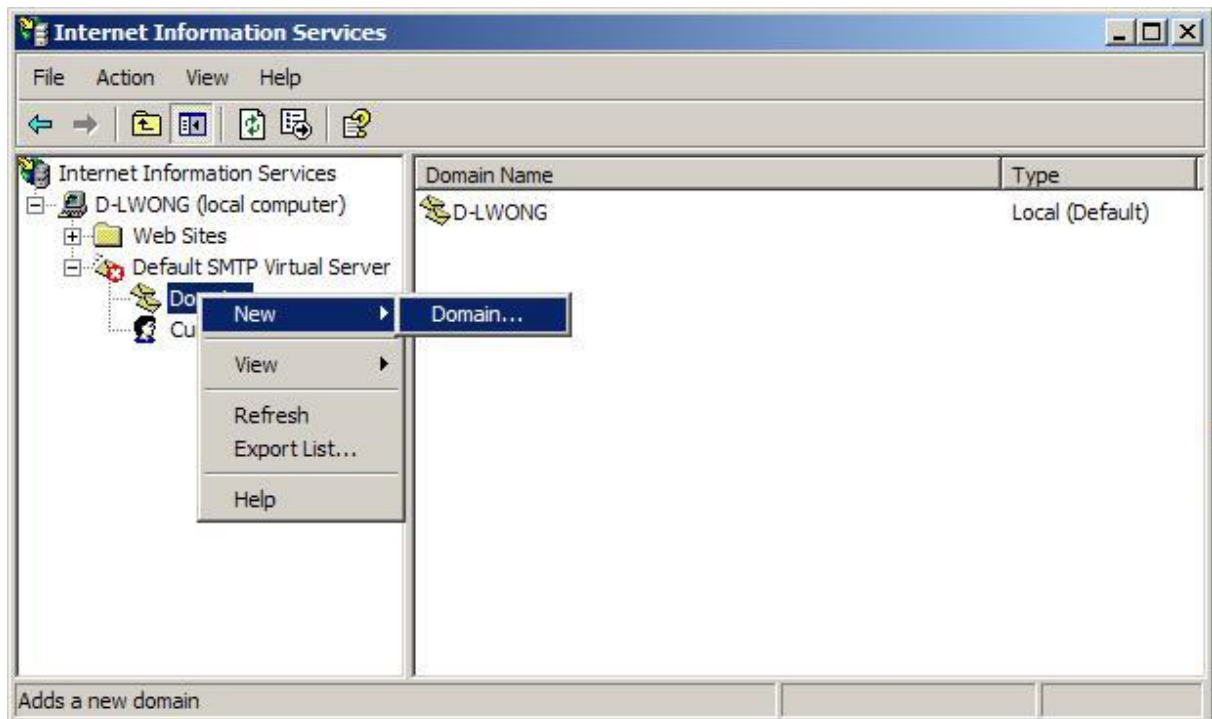


## Az IIS mail szerver szolgáltatása

Az internetes ajánlások az IIS beépített SMTP szolgáltatása helyett az EAsendmail service SMTP szerveret 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.

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 rendelték 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 beállításában 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:

```
amd          IN      A          192.168.100.123
```

*(IPv4 cím hozzárendelése domainnamehez)*

```
amd          IN      AAAA       2001:db8:85a3::8a2e:370:7334
```

*(IPv6 cím hozzárendelése domainnamehez)*

```
amd          IN      CNAME       feher4
```

*(„ALIAS” erőforrásrekord hozzárendelésre egy, már létező domainhez)*

```
amd          IN      SRV         192.168.100.123
```

*(tartományvezérlő kijelölése a zónában)*

A DNS szerver a telepítés után két tárolót tartalmaz:

Forward Lookup Zones – Címkeresési zónák

Reverse 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 rekurzív 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 elgévelt 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)

## APIPA

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 beállításánál 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.