HATODIK FEJEZET

Hibakeresés és -elhárítás

A fejezet tartalma:

Ami elromolhat, az el is romlik, egyáltalán nem mindegy azonban, hogy a hibaelhárítás két percig, vagy két hónapig tart – sajnos, akár azonos hiba esetén is előfordulhat mindkét véglet, a dolog egyszerűen azon múlik, hogy ki az, aki a hibaelhárítással próbálkozik, és milyen eszközök állnak rendelkezésre a probléma megkereséséhez és elhárításához. Bár a hibaelhárítás természeténél fogva nem sablonművelet, vagyis nem lehet minden helyzetben használható receptet adni, ebben a fejezetben megpróbálkozunk az alapelvek, és felhasználásra érdemes alapeszközök bemutatásával.

A hibák elhárításához általában a programok felhasználói felülete mögé kell merészkednünk, így mindenképpen indokolt az óvatosság; nem számíthatunk a megszokott „bolondbiztos” viselkedésre, vagyis egy meggondolatlan mozdulattal az eredetinél akár sokkal nagyobb bajt is okozhatunk. Egy fontos szabályt tehát mindig célszerű betartani: Ha nem **tudod**, hogy mit csinálsz, és pontosan mit akarsz vele elérni, akkor inkább ne csináld!

A fejezetben a következő témákkal fogunk megismerkedni:

- **Hibakeresés és javítás mélyebben** – elsőként azokkal a hibákkal foglalkozunk, amelyek megakadályozzák az operációs rendszer szokásos módon való indítását, illetve a rendszer leállásával járnak, vagyis kezelésükhöz speciális, általában grafikus felület nélküli eszközökre van szükség.
    - **A rendszerindítás folyamata és az indítómenü elemei** – ebben a részben részletesen megismerkedünk a Windows-rendszerek indítási folyamatának lépéseivel, és a hibakeresésre szolgáló üzemmódokat lehetővé tevő indítómenüvel.

    - **A helyreállítási konzol** *(Recovery Console)* – áttekintjük a Windows telepítőlemezéről indítható Recovery Console lehetőségeit. Az eszköz segítségével hozzáférhetünk a más módon már nem indítható operációs rendszer fájljaihoz és más beállításaihoz.
- **A „kék halál"** – megismerkedünk a Windows-rendszerek leállását kísérő hírhedt kék képernyő kiváltó okaival, és a megjelenő adatok jelentésével.
- **Grafikus ellenőrző- javító eszközök** – a sikeres rendszerindítás után rendelkezésünkre áll a Windows valamennyi beépített hibakereső-, javító és ellenőrző eszköze. Ebben a részben ezek közül fogunk a legfontosabbakkal megismerkedni.
- **Adataink biztonsága** – Ha már minden más módszer csődöt mondott, akkor a biztonsági mentésből való visszaállításhoz kell folyamodnunk. Ebben a részben a mentési rendszer megtervezéséről és használatáról lesz szó.
- **Külső eszközök** – a Windows beépített eszközein kívül számos külső programot is igénybe vehetünk a hibakereséshez. Ebben a részben a Sysinternals cég által készített eszközök közül ismerkedünk meg a legfontosabbakkal.

Bár témánk alapvetően a Windows Server 2003 R2, a fejezetben leírtak gyakorlatilag teljes mértékben érvényesek a régebbi kiszolgálórendszerekre (Windows 2000 Server) és az ügyfélrendszerekre is (Windows 2000 és XP). A Windows Vista esetén természetesen vannak bizonyos (esetenként jelentős) különbségek és újdonságok is, de ezek legnagyobb részéről a könyv első részében már szót ejtettünk.

Hogyan lehet észlelni a hibákat?

A hibák kezelésével kapcsolatban rendkívül fontos kérdés, hogy milyen módon szerzünk tudomást arról, hogy valamiféle hiba történt a rendszer, vagy egy számítógép működésében. Természetesen, ha elég sokáig várunk, akkor egészen nyilvánvaló jelek is várhatók (például sűrű fekete füst a szerverszobában☺), de sokkal jobban járunk, ha elébe megyünk az ilyen helyzeteknek és rendszeresen ellenőrizzük például az eseménynaplót és az egyes komponensek önálló naplófájljait is. A legjobb persze az (és a különféle rendszerfelügyeleti szoftverek, például a System Center Essentials, vagy a System Center Operations Manager használatával ez meg is valósítható), ha kiszolgálóink és az ügyfélgépek is önállóan jelzik, ha valamiféle probléma miatt beavatkozást igényelnek.

A legnehezebben felderíthető hibák azok, melyek nem járnak konkrét, jól beazonosítható jelenséggel (például hibaüzenet), nincs nyomuk az eseménynaplóban, csak bizonyos homályos, nehezen, vagy egyáltalán nem reprodukálható tünetek utalnak arra, hogy valami nincs teljesen rendben a kiszolgálóval. A következő jelenségekre érdemes figyelmet fordítani:

- A kiszolgáló a szokásosnál lassabban működik, esetleg néha minden különösebb látható ok nélkül újraindul.
- Az ügyfelek a szokásosnál lassabban érik el a kiszolgálót, esetleg bizonyos műveletek (például névfeloldás) elvégzésére sokat kell várakozni.
- Különféle hálózati szolgáltatások elérése bizonytalan, néha gond nélkül működik, máskor egyáltalán nem érhető el.
- Rejtélyesnek tűnő hardverproblémák jelentkeznek (melegedés, hangok stb.)

Ha a megfigyelt jelenségek alapján már biztosak vagyunk benne, hogy valami probléma lehet a kiszolgálóval, akkor az alábbi eszközöket vethetjük be a konkrét hibajelenség azonosításához:

- Task Manager *(Feladatkezelő)* – a futó (vagy nem futó) folyamatok azonosítására és az erőforrások foglaltságának ellenőrzésére
- Services *(Szolgáltatások)* MMC – a rendszerszolgáltatások állapotának ellenőrzéséhez
- Event Viewer *(Eseménynapló)*
- Alkalmazás- és rendszernaplófájlok (AD, IIS, ISA, SQL stb.)
- System Information eszköz (Msinfo32)
- Külső (pl. Sysinternals) eszközök

Hibakeresés és javítás mélyebben

Ebben a részben olyan hibákkal foglalkozunk, amelyek megakadályozzák az operációs rendszer megszokott módon való indítását. Az ilyen hibák kezelése azért nehezebb a szokásosnál, mert nem használhatjuk a jól ismert és rendszeresen alkalmazott eszközöket, minden műveletet egy kevésbé komfortos és általában kevésbé ismert környezetben kell elvégeznünk.

A rendszerindítás folyamata és az indítómenü elemei

A következőkben megismerkedünk a Windows-rendszerek indítási folyamatával, hogy a folyamat közben keletkező hibák hatékonyabban felderíthetők és elháríthatók legyenek. Hogy megtalálhassuk a hibák valódi okait, ismernünk kell az adott folyamat végrehajtásának részleteit, mivel egy tetszőleges rendszer vagy program hibájának elhárításához pontosan kell tudnunk, mi történik akkor, ha a rendszer vagy program hibátlanul működik.

Hogyan indul az operációs rendszer?

A számítógép bekapcsolása után az alaplapon lévő flash memóriában tárolt program betöltődik a memóriába, és nekikezd a POST (Power-on Self Test) nevű művelet végrehajtásának. A POST által elvégzett konkrét műveletek teljes mértékben az adott hardver gyártójának hatáskörébe tartoznak, de a legtöbb esetben ilyenkor történik meg a különféle feszültségszintek ellenőrzése, a RAM, a grafikus kártya, a különféle bővítőkártyák és a legfontosabb perifériák működőképességének vizsgálata. A BIOS Setup program segítségével általában bizonyos mértékig befolyásolhatjuk a POST futását, kérhetünk további teszteket (például a memóriára vonatkozóan), és szabályozhatjuk a képernyőn megjelenő üzenetek mennyiségét.

Szintén a BIOS Setupban határozhatjuk meg, hogy mi történjen a POST után, vagyis milyen sorrendben próbálkozzon a számítógép a különféle eszközökről (merevlemez, CD-ROM, hajlékonylemez, hálózat stb.) történő rendszerindítással. Ha a számítógép a merevlemezről indul, akkor a sikeres POST után a BIOS ellenőrzi a fő rendszertöltő rekordot (*Master Boot Record, MBR).*

Az MBR minden particionált merevlemezen megtalálható (a particionáláskor kerül rá), mégpedig a lemez legelső fizikai szektorában (vagyis a teljes mérete 512 bájt). Az MBR tartalmaz némi végrehajtható kódot *(Master Boot Code),* az adott lemez egyedi azonosítóját *(Disk Signature)* és a négyszer 16 bájt méretű partíciós táblát. Az MBR végén található partíciós tábla tehát négy bejegyzést tartalmazhat. Az egyes bejegyzésekben szerepel az adott partíció első és utolsó szektorának azonosítója, a partíció szektorainak száma, és a fájlrendszerre utaló érték. Ha a bejegyzés utolsó két bájtjának értéke 0x8001, akkor aktív partícióról van szó. Az MBR utolsó két bájtja egy speciális érték (0x55AA), amely a szektor végét jelzi, és amelynek hiánya komoly problémákat okozhat.

Ha az MBR utolsó két bájtja nem 55AA, akkor a BIOS azt feltételezi, hogy az MBR sérült, vagy a lemez egyáltalán nincsen particionálva. Ekkor általában (bár a pontos szöveg BIOS-függő) az *Operating system not found* üzenet jelenik meg, a számítógép pedig természetesen nem folytatja az indítást. Ha a

BIOS megfelelőnek ítéli az MBR-t, akkor betölti és elindítja a benne található programot. Az MBR programja végigolvassa a partíciós táblát, és kiválasztja belőle az aktívként megjelölt partíciót. Ha ez valami miatt nem sikerül (például egyáltalán nincs aktív partíció) akkor az *Operating System not found*, vagy az *Invalid partition table* üzenet jelenik meg. Ha sikerült megtalálni az aktív partíciót, akkor az MBR-kód betölti az adott partíció boot-szektorát a memóriába és ellenőrzi azt.

A bootszektor az egyes partíciók első szektora, amely az adott partícióra telepített operációs rendszer indítását lehetővé tevő programkódot, és a partícióra vonatkozó különféle információkat tartalmazza. A bootszektor a partíció formázásakor jön létre, tartalma pedig a fájlrendszer típusától függ. Az MBR-hez hasonlóan a bootszektor végét is az 0x55AA érték jelzi.

Ha a bootszektort nem sikerül betölteni (például, mert a partíció nincs formázva), akkor az *Error loading operating system* üzenet jelenik meg és a betöltés leáll. Amennyiben a bootszektor végén nincs ott a mágikus 55AA érték, a *Missing operating system* üzenet jelenik meg, és a betöltés természetesen ebben az esetben sem folytatódik. Ha minden rendben van, akkor az MBR-kódtól a vezérlés a boot szektor kódjához kerül, és folytatódik a rendszerindítás.

A bootszektor programjának feladata az, hogy megkeresse és elindítsa a Windows betöltő programját az NTLDR-t, amelynek az indító partíció gyökerében kell lennie. Ha ez valamilyen ok miatt nem sikerül, akkor ezen a ponton kaphatjuk a *Missing NTLDR* hibaüzenetet (NTFS fájlrendszer esetén). Ha sikerült elindítani az NTLDR-t, akkor az első lépésként 32-bites védett módba kapcsolja a processzort és engedélyezi a memórialapozást, így ezután már rendelkezésre áll a teljes 4 GB-os címezhető tartomány (32-bites processzor esetén).

Az NTLDR ezután a következő műveleteket végzi el [az NTLDR tartalmazza az NTFS (és FAT, illetve FAT32) fájl-rendszerrel formázott partíciók olvasásához és írásához szükséges programkódot]:

- Megvizsgálja a gyökérmappában található *hiberfil.sys* állományt, és ha talál benne alvó állapotban lévő operációs rendszert, akkor visszatölti azt a memóriába, a végrehajtás pedig folytatódik a hibernáláskor megjegyzett ponton.
- Ha nincsen alvó operációs rendszer, akkor az NTLDR beolvassa a gyökérmappában lévő *boot.ini* nevű fájl tartalmát. A *boot.*ini ARC-útvonalak *(Advanced RISC Computing)* formájában tartalmazza a számítógépen található indítható operációs rendszerek helyét. Az NTLDR a *boot.ini* alapján készíti el azt a kis menüt, amiből kiválaszthatjuk az elindítandó operációs rendszert.

A menü csak akkor jelenik meg, ha egynél több bejegyzés van a boot.ini-ben. Egy bejegyzés esetén az NTLDR azt feltételezi (milyen intelligens, nem?), hogy azt az egyet szeretnénk elindítani. Ha egyáltalán nincsen *boot.ini,* akkor az NTLDR azt feltételezi, hogy az operációs rendszer az adott partíció alapértelmezett mappájába *(c:\windows)* van telepítve. Ha ez a mappa nincs a helyén, akkor a következő üzenet jelenik meg: *Windows could not start because the following file is missing or corrupt: \winnt root\system32\ntoskrnl.exe*.

- Miután valamilyen módon sikerült tisztázni, hogy melyik operációs rendszert is kell elindítani (kiválasztottuk a menüből, vagy sikerült az alapértelmezés alapján megtalálni), az NTLDR elindítja az ntdetect.com programot (az ntdetect.com szintén a gyökérmappában található). Az ntdetect listát készít a számítógép hardverkomponenseiről (busztípusok és eszközök, lemezmeghajtók, grafikus kártya, billentyűzet, soros és párhuzamos portok, egér stb.) és az eredményt átadja az NTLDR-nek.

Ezen a ponton, vagyis az indítandó rendszer kiválasztása (automatikusan, vagy a menüből) után az NTLDR törli a képernyőt, és megjelenít egy karakteres „folyamatjelzőt". Sajnos (vagy szerencsére) ez többnyire szinte láthatatlan a gyors betöltődés miatt. A különféle indítási opciók (csökkentett mód, DSRM stb.) elérésére szolgáló indítómenü megjelenítéséhez viszont pontosan akkor kell megnyomnunk az F8 billentyűt, amikor ez a folyamatjelző látható, (illetve nem látható).

- Ezután az NTLDR sorban elkezdi betölteni a memóriába rendszer különböző részeit (de csak betölti, még nem inicializálja, illetve nem indítja el őket). Elsőként betöltődik az *ntoskernel.exe* és a *hal.dll* (mindkét fájlnak a *%systemroot%\System32* mappában kell lennie), majd a registry *HKLM\SYSTEM* ága (a *%systemroot%\System32\Config\System* fájlból, és az ebben tárolt adatok alapján valamennyi szükséges eszközvezérlő. Az eszközvezérlőket tartalmazó fájlok a *%systemroot%\System32\Drivers* mappában találhatók. Az NTLDR a registryben tárolt adatok alapján határozza meg, hogy a betöltődés további részét meghatározó úgynevezett Control Setek közül melyiket kell felhasználnia. Ezen a ponton történik a Last Known Good Configuration *(legutolsó helyes konfiguráció)* betöltése (lásd később), ebben az esetben egy korábban elmentett, a legutolsó módosításokat még nem tartalmazó Control Setet fog felhasználni az NTLDR.
- Utolsó tevékenységeként az NTLDR elindítja a már korábban betöltött ntoskernel.exe programot, a betöltődés további részét már az *ntoskernel.exe* vezérli.

- Az *ntoskernel* indulásakor a képernyő grafikus üzemmódban vált, és a színes Windows logó alatt megjelenik a dísz folyamatjelző, ami nem jelzi ugyan semmiféle folyamat előrehaladását, de legalább kellemes, megnyugtató látványt nyújt. Közben azért fontosabb dolgok is történek, az *ntoskernel* memóriastruktúrákat hoz létre, inicializálja a megszakításkezelőket, elindítja a folyamatkezelőt és létrehozza a System folyamatot. Ezután kerül sor az NTLDR által betöltött eszközkezelők inicializálására. Következő lépésként az *ntoskernel* elindítja a Session Managert (smss.exe), majd a winlogon.exe indításakor megjelenik a Windows bejelentkező ablaka.

Az indítómenü

A Windows indítómenüje lehetővé teszi azt, hogy az operációs rendszert különféle speciális üzemmódokban indítsuk el. A speciális üzemmódokra általában hibakeresés, illetve elhárítás céljából van szükség. Az indítómenüt az NTLDR futása közben lenyomott F8 billentyű segítségével érhetjük el. A következőkben áttekintjük az egyes menüpontok szerepét, és felsorolunk néhány tipikus problémát, amelyek az indítómenü használatával oldhatók meg.

Az indítómenü használata
Ebben a screencastban az operációs rendszer indítómenüjének különféle lehetőségeivel ismerkedhetünk meg.
Fájlnév: II-3-1a-Boot-Menu.avi

Csökkentett módok

Ha a számítógép a szokásos módon nem indítható, illetve a szokásos indításkor olyasmi is elindul, amire egyáltalán nincsen szükség (például különféle kedves spyware programok, vagy egyéb férgek), akkor érdemes megpróbálkozni valamelyik csökkentett módban történő rendszerindítással. Természetesen bármelyik csökkentett módot is választjuk, valamelyik helyi felhasználói fiók használatával be kell jelentkeznünk a rendszerbe.

- **Safe Mode** *(Csökkentett mód)* – Csökkentett módban a Windows az alapértelmezett beállításokat használja (hálózati szolgáltatások betöltésére nem kerül sor). Ebben az esetben az operációs rendszer csak a működéséhez nélkülözhetetlen eszközmeghajtókat (VGA monitorvezérlő, a tárolóeszközök (IDE, SCSI, CD-ROM stb.) kezelőprogramjai, egér és billentyűzet) és a legszükségesebb szolgáltatásokat (Logical Disk Manager, Plug and Play, RPC stb.) indítja el. Nincsen hálózat, nem használhatóak a különféle extra eszközök (USB-memóriák, hangkártya

stb.), és nem indulnak el a szokásos rendszerindításkor automatikusan induló programok sem. Ha a számítógépet ilyen módon sikerül elindítani, akkor megkereshetjük és letilthatjuk, illetve eltávolíthatjuk a problémát okozó eszközillesztőt, szolgáltatást, vagy programot.

- **Safe Mode with Networking** *(Csökkentett mód hálózattal)* – Ez az indítási mód megegyezik a csökkentett móddal, de betöltődnek a hálózati alapszolgáltatások is (DHCP- és DNS-ügyfél, Server, Workstation stb.) vagyis elérhetjük és felhasználhatjuk a hálózati erőforrásokat is. Ebben az esetben használhatunk tartományi felhasználónevet is a bejelentkezéshez.
- **Safe Mode with Command Prompt** *(Csökkentett mód parancssorral)* – ebben az esetben nem indul el a Windows grafikus felhasználói felületét biztosító Windows Explorer (explorer.exe), hanem helyette csak egy parancssort (cmd.exe) kapunk. Akkor lehet szükség erre az indítási módra, ha a számítógép normál módú indítását lehetetlenné tevő problémát maga a Windows Explorer okozza (például hiányzik, vagy sérült az explorer.exe fájl).

A csökkentett módokban elinduló eszközillesztőket és szolgáltatásokat a *HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot* registrykulcs alatt található értékek határozzák meg, a Minimal szakasz mindhárom esetben, a Network szakasz pedig a *Csökkentett mód hálózattal* menüpont választása esetén töltődik be.

Az indítómenü további lehetőségei

A menü további elemei bizonyos speciális problémák esetén használható hibakeresési, illetve helyreállítási lehetőségeket kínálnak:

- **Enable Boot Logging** *(Rendszertöltés naplózásának engedélyezése)* – ha ezt a menüpontot választjuk, akkor indításkor naplófájl készül a betöltött (és a valami miatt be nem töltött) eszközillesztőkről és szolgáltatásokról. A fájl ntbtlog.txt néven a *%systemroot%* mappában található. A rendszer indítása ebben az esetben normál módban történik, de alapértelmezés szerint valamennyi csökkentett mód használata esetén is készül naplófájl. A napló segítségünkre lehet a rendszerindítási hibák pontos okának meghatározásában.
- **Enable VGA Mode** *(VGA mód engedélyezése)* – A számítógép ebben az esetben a grafikus kártya telepített illesztőprogramjának betöltésével, de a lehető legkisebb képernyőfelbontással (640×480) indul. (A csökkentett módokban a rendszer a grafikus kártya illesztőprogramja helyet a Windows beépített VGA-eszközillesztőjét használja.)

- **Last Known Good Configuration** *(Legutolsó helyes konfiguráció)* – A rendszer minden indításkor mentést készít a registrynek a betöltődési folyamatot meghatározó részéről (Control Set). A menüpont kiválasztásakor a rendszer indítása a Windows legutóbbi indításakor elmentett registryadatok alapján történik, vagyis az utolsó bejelentkezés óta módosított illesztőprogram- és rendszerbeállítások el fognak veszni. A Control Set „jó" készletként való megjelölése, a bejelentkezéskor történik, vagyis ekkor az aktuális és a legutolsó helyes Control Set megegyezik. A munkamenet során elvégzett változtatások csak az aktuális registryadatokat érintik, a bejelentkezéskor létrehozott példány megmarad eredeti állapotában, erre térhetünk később vissza (a csökkentett módban való bejelentkezés **nem** szinkronizálja a Control Seteket, vagyis ekkor megmarad a korábbi konfiguráció is). A menüpontot tehát közvetlenül a hibát okozó változtatás után érdemes használni (a következő bejelentkezés előtt), segítségével részlegesen visszaállíthatjuk a registryt (az eszközmeghajtók és szolgáltatások beállításait), de sérült vagy hiányzó fájlok pótlására nem használható.
- **Directory Services Restore Mode** *(Címtárszolgáltatások visszaállítása)* – Az elmentett Active Directory adatbázis mentésből való helyreállításakor van szükség a DSRM üzemmódban történő rendszerindítás használatára (csak tartományvezérlőkön). A DSRM-üzemmód részletei az előző, „Tartományi környezet" című fejezetben találhatók.
- **Debugging mode** *(Hibakeresési mód)* – A rendszer indításkor a soros (COM2), illetve firewire portra küld különféle hibakeresési adatokat.
- **Disable automatic restart on system failure** *(Automatikus újraindítás letiltása rendszerhiba esetén)* – Alapértelmezés szerint rendszerleállás („kék halál") után a számítógép automatikusan újraindul, így nem tudjuk megnézni és felírni a képernyőn látható hibaüzenetet, ami pedig igen fontos lenne a hiba okának megállapításához. Természetesen az alapértelmezett viselkedés a működő rendszer grafikus felületén megváltoztatható, de ha a leállás a Windows indítása közben történik, akkor ez a lehetőség már nem érhető el. A menüpont használatával nem induló rendszer esetében is megváltoztathatjuk ezt a fontos beállítást.

Példák az indítómenü lehetőségeinek használatára

A következőkben felsorolunk néhány, az indítómenü felhasználásával könnyen megoldható tipikus problémát:

- Telepítettünk egy olyan programot a számítógépre, ami hozott magával egy új rendszerszolgáltatást vagy eszközmeghajtót, és beállította ennek automatikus indítását is. Újraindításakor azonban az induló szolgáltatás hibája miatt nem indul el a számítógép („kék halál"). Ebben az esetben csökkentett módban valószínűleg probléma nélkül elindítható a rendszer, és letilthatjuk az újonnan telepített szolgáltatás vagy eszközmeghajtó automatikus indulását, illetve eltávolíthatjuk a programot.
- Telepítettük gépünkre az internetről letöltött rendszerkarbantartó és kávéfőző csodaprogram legfrissebb, 2.43.5f verzióját. Mégsem tetszik azonban a programba integrált e-mailküldési funkció, ami folyamatosan különféle reklámokkal bombázza ismerőseinket, ezért megpróbálunk megszabadulni tőle. Szomorúan tapasztaljuk, hogy a Feladatkezelővel sajnos nem lehet leállítani a folyamatot. Sebaj, töröljük le magát a programfájlt! Amíg azonban a folyamat fut, sajnos a fájlt sem lehet letörölni. Következő lépésként megpróbálhatjuk megkeresni és törölni a registry megfelelő bugyrában *(HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run)* a program automatikus indítását végző bejegyzést. Újraindítás után azonban a csodaprogram.exe újra ott figyel a futó folyamatok között, sőt visszaírta magát a registrybe is. Ekkor következik a csökkentett módban történő indítás, ami már valódi megoldást jelenthet. Csökkentett módban nem indulnak el az egyébként automatikusan induló (csoda)programok, így már törölhetőek a fölösleges fájlok, és véglegesen törölhető a registrybejegyzés is.
- Az egyik számítógéphez új monitort csatlakoztatunk. A gép látszólag elindul, de aztán már csak nem látszólag működik, mivel a bejelentkező ablak helyén csak egy fekete képernyő fogad minket. Ebben az esetben az a helyzet, hogy az új monitor nem képes a régi monitor számára beállított 1746x1398 képpontos felbontás (esetleg a 168 Hz képfrissítési frekvencia) megjelenítésére. Csökkentett, vagy VGA-módban történő indítás esetén a grafikus felület olyan felbontással indul, amelyet minden monitor biztosan meg tud jeleníteni, így már be tudunk jelentkezni, és tetszés szerint átállíthatjuk a képernyő paramétereit.

Helyreállítási konzol

A Helyreállítási konzol *(Recovery Console)* használatára akkor van szükség, ha semmilyen más módon nem tudjuk elindítani a gépre telepített operációs rendszert (csökkentett módban sem). A Helyreállítási konzol teljesen önállóan indítható, használatához nincsen feltétlenül szükség a merevlemezen tárolt információkra.

A Helyreállítási konzolnak nincsen grafikus felülete, ez tulajdonképpen egy korlátozott parancskészlettel rendelkező önálló mini operációs rendszer, amelynek használatával hozzáférhetünk a merevlemezeken tárolt adatokhoz, pótolhatunk, kicserélhetünk, vagy lementhetünk fájlokat (NTFS fájlrendszer esetén is). Lehetőségünk van diagnosztikai eszközök futtatására (például *chkdsk* a fájlrendszer ellenőrzéséhez és javításához), és bizonyos mértékig hozzáférhetünk a registryhez is: engedélyezhetjük, illetve letilthatjuk az egyes eszközmeghajtók és rendszerszolgáltatások indítását. További fontos lehetőség a fő rendszertöltő rekord (MBR) és a bootszektor javítása (újraírása) is.

A Helyreállítási konzolt telepíthetjük a gép merevlemezére (de a telepített változat a rendszerindítás korai fázisának hibája esetén nem érhető el), illetve elindíthatjuk közvetlenül az operációs rendszer telepítőlemezéről is. A konzol lefelé kompatibilis, vagyis például a Windows Server 2003 telepítőlemeze használható a Windows 2000, XP stb. rendszerek javításához is.

A Recovery Console telepítése a merevlemezre
Ebben a screencastban feltelepítjük a kiszolgáló merevlemezére a Recovery Console-t.
Fájlnév: *Fájlnév*: *II-3-1b-RC-telepites.avi*

A konzol indítása

A Helyreállítási konzol indításához a számítógépet a Windows telepítő CD-ről kell elindítanunk (mintha csak az operációs rendszert telepítenénk). A merevlemezek eléréséhez esetleg szükséges SCSI- vagy RAID-vezérlőket az F6 billentyű megnyomása után floppyról adagolhatjuk be (éppen úgy, mint telepítés közben).

Lehetőség van arra is, hogy a Helyreállítási konzolt a merevlemezre telepítsük. Ebben az esetben a konzol indításához már nincs szükség a telepítő CD-re, mivel a telepítés során a futtatáshoz szükséges minden fájl a rendszerkötet gyökerében létrejövő *cmdcons* nevű rejtett mappába kerül, a rendszerindításkor megjelenő menübe pedig *(boot.ini)* bekerül a *Windows Server 2003 Recovery Console* sor. A telepítéshez azonban szükség van a Windows CD-re, a következő parancsot kell kiadnunk: *x:\i386\winnt32/cmdcons*, ahol *x* a telepítőlemezt tartalmazó CD-meghajtó betűjele.

6.1. ábra: *Telepítés helyett válasszuk a Recovery Console indítását*

Az eszközmeghajtók betöltése után a telepítés helyett válasszuk a rendszer javítását, majd a telepített operációs rendszerek listája alapján (a szám beírásával) ki kell választanunk azt a Windows példányt, amelyikbe be szeretnénk jelentkezni, és meg kell adnunk a helyi Administrator *(Rendszergazda)* fiókhoz tartozó jelszót (ha a fiók nevét megváltoztattuk, akkor sincs szükség felhasználónévre, mivel azt a biztonsági azonosító (SID) helyettesíti).

```
Microsoft Windows(R) Recovery Console.
The Recovery Console provides system repair and recovery functionality.
Type EXIT to quit the Recovery Console and restart the computer.

1: C:\WINDOWS

Which Windows installation would you like to log onto
(To cancel, press ENTER)? 1
```

6.2. ábra: *A Recovery Console egyetlen lehetőség esetén is kérdez…*

Tartományvezérlő esetén a DSRM-mód jelszavát kell begépelnünk, amelyet a tartományvezérlővé való előléptetéskor állítottunk be. (Ez a jelszó utólag az *ntdsutil* program használatával módosítható, de természetesen csak a működő rendszerben, a helyreállítási konzolban nem.) A jelszó megadásával háromszor próbálkozhatunk, ha a harmadik tipp is helytelen, a számítógépet már csak újraindítani lehet. Ha a helyreállítási konzol nem talált a lemezen telepített Windows-rendszert, akkor természetesen nincs hova bejelentkezni, és a parancssor minden további nélkül megjelenik.

Ha sikerült megadnunk a megfelelő jelszót, akkor a kiválasztott példány *%systemroot%* mappájában (például *c:\windows)* találjuk magunkat, és kezdődhet a küzdelem.

A Helyreállítási konzol parancsai

A Recovery Console indítása és használata
Ebben a screencastban elindítjuk, illetve megmutatjuk a Recovery Console számos lehetőségei közül a legérdekesebbeket, illetve a leghasznosabbakat.
Fájlnév: Fájlnév: II-3-1c-RC-hasznalat.avi

A következőkben áttekintjük a helyreállítási konzol legfontosabb, leggyakrabban használt parancsait, és a parancsok használatával kapcsolatos tudnivalókat.

A konzol indítása után kilistázhatjuk a használható parancsokat a help parancs használatával, illetve egyes parancsokhoz is kérhetünk segítséget, ha begépeljük a help <parancsnév> utasítást.

- **Chkdsk** – a parancs segítségével lemezellenőrzést végezhetünk, és kérhetjük a talált hibák automatikus javítását. Ha az ellenőrzendő lemez nincsen inkonzisztensként megjelölve, akkor a *chkdsk* csak a */p* kapcsoló használata esetén végzi el annak ellenőrzését. Ha megadjuk a */r* kapcsolót is, akkor a *chkdsk* megkísérli a hibás szektorokban található adatok helyreállítását. A *chkdsk* működéséhez szükség van az *autocheck.exe* programra, ha nem sikerül automatikusan megtalálnia (a merevlemezen vagy a telepítő CD-n), akkor a *chkdsk* rákérdez annak helyére.
- **Fixmbr** – a parancs újraírja a fő rendszertöltő rekord (MBR) első 446 bájtját, vagyis az MBR-ben található programkódot, de (általában) érintetlenül hagyja a partíciós táblát.

Más a helyzet azonban hibás partíciós tábla (például két aktívként megjelölt partíció) vagy az MBR-t lezáró 0x55AA érték hiánya esetén. Ekkor a *fixmbr* teljesen, és visszavonhatatlanul letörli a partíciós táblánkat. Nem szabad tehát a *fixmbr* parancsot használni, ha az *Operating system not found* vagy az *Invalid partition table* hibaüzenetet látjuk (legalábbis, ha még szükségünk van a lemez partíciós táblájára). Ilyen esetben sajnos az automatizált megoldásokban már nem bízhatunk, vagyis csak a nehéz út járható: a merevlemezt átszereljük egy működő gépbe, és a Resource Kit-ben található *DskProbe.exe* nevű program segítségével manuálisan kijavítjuk a partíciós tábla hibáját (csak erős idegzetűeknek!). Ugyancsak fölösleges a *fixmbr*-rel próbálkozni, ha egyáltalán nincs aktívként megjelölt partíciónk, mivel ekkor a partíciós tábla megmarad ugyan, de aktív partíció továbbra sem lesz benne.

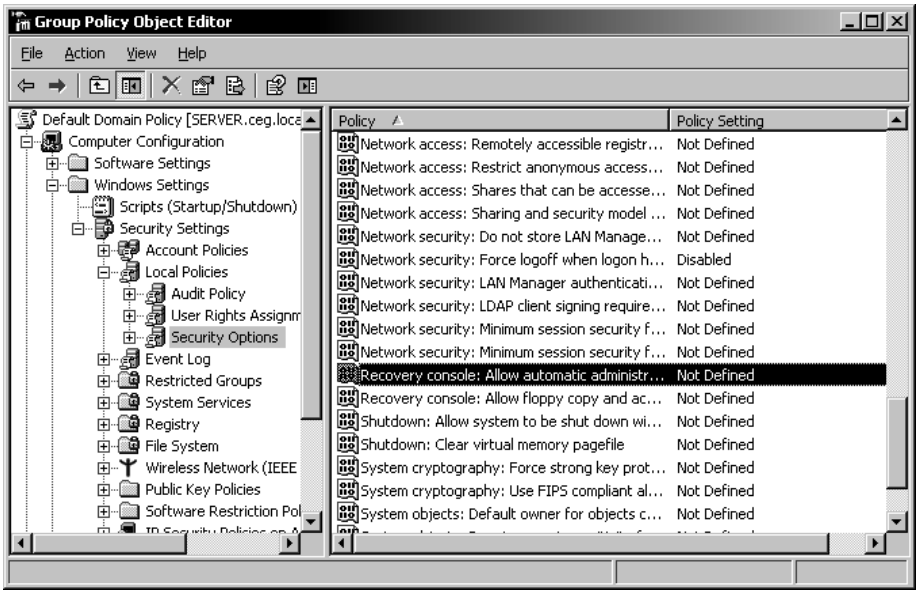
- **Fixboot** – a rendszerpartícióra új bootszektort ír. Ez a művelet nem jár különösebb kockázattal, rontani biztosan nem ront a helyzetünkön.
- **Diskpart** – egyszerű, karakteres felületű partícionálóprogram, megegyezik azzal (csak a színösszeállítás más egy kicsit), amivel a Windows-telepítés elején találkozhatunk. Elsődleges és kiterjesztett partíciók, illetve logikai kötetek létrehozását és törlését végezhetjük el segítségével, illetve meg is formázhatjuk a létrehozott meghajtókat.
- **Map** – a parancs megjeleníti a meghajtó betűjelek és a fizikai eszköznevek összerendeléseit. Erre az információra például a *fixboot* és a *fixmbr* futtatásakor lehet szükség, mivel ekkor a fizikai eszközneveket (például *\Device\HardDisk0\Partition1)* kell megadnunk paraméterként. Az *arc* paraméter használatával a parancs ARC (Advanced RISC Computing) formátumban írja ki az eszközneveket (például *multi(0)disk(0)rdisk(0)partition(1)),* ezeket az értékeket a *boot.ini* szerkesztésekor használhatjuk fel.

- **Set** – a parancs segítségével megjeleníthetjük és beállíthatjuk a konzol környezeti változóit. Mindössze négy környezeti változónk van (értékük *true* vagy *false* lehet), amelyekkel tiltható, illetve engedélyezhető különféle műveletek végrehajtása. Alapértelmezés szerint mind a négy változó értéke *false*, vagyis a hozzájuk tartozó műveletek tiltottak. Sőt alapértelmezés szerint csak akkor állíthatjuk át a változók értékét, ha ezt a számítógép helyi házirendjében (vagy a csoportházirendben) már korábban engedélyeztük (lásd később). A négy változó a következő:
    - **AllowAllPaths** – a változó segítségével engedélyezhetjük a merevlemezeken található valamennyi kötet és mappa elérését. (Alapértelmezés szerint csak a Windows-mappa és a gyökér érhető el.)
    - **AllowRemovableMedia** – engedélyezhetjük az adatok cserélhető meghajtóra való kimásolását. (Alapértelmezés szerint csak befelé másolhatunk.)
    - **AllowWildCards** – engedélyezhetjük a helyettesítő karakterek használatát a fájl és mappakezelő parancsokban (például *copy *.*).*
    - **NoCopyPrompt** – *true* érték esetén a konzol nem kér megerősítést a meglévő fájlok felülírása előtt.
- **Batch** – a parancs paramétereként tetszőleges nevű, a Helyreállítási konzol utasításait tartalmazó szövegfájl nevét adhatjuk meg. A fájlban szereplő utasításokat a konzol úgy hajtja végre, mintha egyesével gépeltük volna be azokat. Második paraméterként megadhatjuk a parancsok kimenetét fogadó fájl nevét is, de ha nem adunk meg nevet, akkor a kimenet a szokásos módon a konzolra kerül.
- **Bootcfg** – a parancs segítségével módosíthatjuk a *boot.ini* tartalmát, megkereshetjük például a lemezre telepített Windows-példányokat és hozzáadhatjuk a megfelelő bejegyzéseket a *boot.ini*-hez.
- **Listsvc** – a parancs megjeleníti a számítógépen elérhető valamennyi eszközillesztő és szolgáltatás listáját.
- **Enable** – a parancsot a paraméterként megadott eszközillesztő vagy szolgáltatás engedélyezésére használhatjuk. Második paraméterként megadható az engedélyezet szolgáltatás indítási típusa is. Az indítási típus a következő értékek valamelyike lehet:
    - SERVICE_BOOT_START
    - SERVICE_SYSTEM_START
    - SERVICE_AUTO_START
    - SERVICE_DEMAND_START

- **Disable** – a parancs letiltja a paraméterként megadott szolgáltatás, vagy eszközillesztő indítását.
- **Logon** – a parancs segítségével átjelentkezhetünk a lemezre telepített másik operációs rendszerbe.
- Használhatók a fájl és mappaműveletekkel kapcsolatos szokásos parancssori utasítások *(cd, dir, copy, delete, md, rd, rename, type).* Ha a Windows telepítőlemezről másolunk fájlokat a merevlemezre, akkor nincs szükség külön kitömörítésre *(expand),* a *copy* parancs ezt elintézi helyettünk.
- **Exit** – kilépés a konzolból és a számítógép újraindítása.

Biztonsági beállítások

A Helyreállítási konzol két biztonsági beállítását még a számítógép működőképes állapotában a helyi-, illetve a csoportházirendben kell megadnunk. Tartományhoz nem tartozó számítógépek esetén csak a helyi házirend áll rendelkezésre. A két beállítást ebben az esetben a *gpedit.msc* (vagy a *secpol.msc)* konzolban adhatjuk meg (Security Settings -> Security Options). Természetesen a fenti módszer tartományi számítógépek esetén is működik, de ekkor a csoportházirend esetleges beállításai felülírhatják a helyi házirendet. Tartományi számítógépek esetén célszerű a fenti beállításokat központilag, a csoportházirendben szabályozni.



6.3. ábra: *Recovery Console opciók a csoportházirendben*

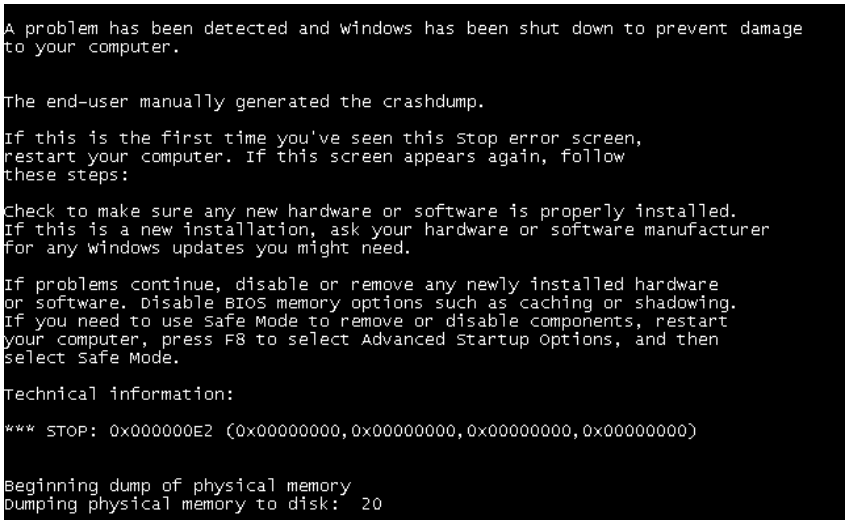
A két opció jelentése a következő:

- **Allow floppy copy and access to all drives and folders** *(Hajlékonylemez másolása és hozzáférés minden meghajtóhoz és mappához)* – ha engedélyezzük ezt az értéket, akkor a korábban említett *set* parancs használatával átállíthatjuk a konzol négy környezeti változóját.
- **Allow automatic administrative logon** *(Automatikus rendszergazdai bejelentkezés)* – ha engedélyezzük az értéket, akkor a konzol indításakor nem kell megadnunk a rendszergazda jelszavát, a bejelentkezés automatikusan megtörténik.

A „kék halál”

Ha a Windows indítása vagy futása során kezelhetetlen hibába ütközik, az adatok megóvásának érdekében leáll, és megjeleníti a hírhedt kék képernyőt (a jelenség neve Blue Screen of Death, vagyis a halál kék képernyője). A kék halál tehát egy megoldhatatlan szituációnak a lehetőségekhez képest korrekt lezárását jelenti.

A kék képernyős rendszerleállásokat az esetek nagyon jelentős részében nem maga az operációs rendszer, hanem valamelyik kernel módban futó eszközmeghajtó, illetve a hardver hibája okozza. A hiba okától függetlenül az információs képernyő megjelenítését, és a rendszer leállítását a *KeBugCheckEx* nevű rendszerfüggvény hajtja végre.

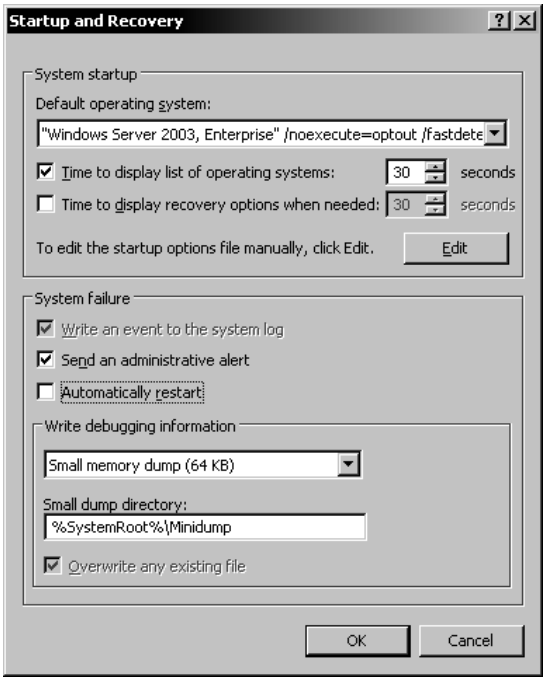


6.4. ábra: *Ha valaki még nem látott volna ilyet…*

A kék képernyő a következő esetekben jelenhet meg:

- Egy eszközmeghajtó, vagy kernel módban futó operációs rendszer függvény kezelhetetlen kivételt generál (például írni próbál a memória írásvédett területére)
- Egy eszközmeghajtó vagy operációs rendszer függvény kifejezetten meghívja a *KeBugCheckEx* függvényt, mert olyan körülményeket észlelt, amelyek lehetetlenné teszik a rendszer további működését.
- Hardver hiba, vagyis nem maszkolható megszakítás *(Non maskable Interrupt, NMI)* esetén.

Természetesen az is megoldható lenne, hogy az operációs rendszer egyszerűen nem vesz tudomást a fenti jelenségekről, és fut tovább, mintha mi sem történt volna, de ebben az esetben később valószínűleg még rosszabb körülmények között kényszerülne leállni a rendszer. A „kék halál" tehát nem feltétlen kényszer, hanem a későbbi súlyosabb problémák megelőzésére szolgáló óvintézkedés, ha nem lenne, ki kellene találni ☺.



6.5. ábra: *Beállíthatjuk, hogy mi történjen rendszerhiba esetén*

A megjelenő információk igen fontosak lehetnek a hiba okának megtalálásához, szerepel köztük egy hibakód, és annak emberi nyelvű megfelelője is (például *IRQ_NOT_LESS_OR_EQUAL).* Bár száznál is több különböző hibakód létezik, a legtöbb közülük csak nagyon ritkán fordul elő. Ha nem vagyunk biztosak a hiba okában és a lehetséges megoldásban, akkor a hibakód alapján további információkat találhatunk a Microsoft Tudásbázisban (http://support. microsoft.com).

Ha a képernyőre kiírt információk alapján nem sikerül azonosítani a hibát, akkor hasznos lehet a rendszerleállás közben fájlba mentett memóriatartalom *(crash dump)* tanulmányozása. Erre a célra számos különféle többékevésbé automatizált analizáló eszköz létezik.

A rendszerhibák kezelésének beállításai
Ebben a screencastban áttekintjük a Startup and Recovery lap beállítási lehetőségeit.
Fájlnév: II-3-1d-Startup-and-Recovery.avi

A rendszerhibák kezelésének különféle paramétereit a Control Panel -> System -> Advanced -> Startup and Recovery lapon (6.6.5. ábra) adhatjuk meg. Talán a legfontosabb beállítás az automatikus újraindítás engedélyezése, illetve tiltása. Alapértelmezés szerint a számítógép újraindul a leállások után, ami nagyon jól jöhet például egy csendes hétvégén, mivel ha a kiszolgáló egyáltalán képes az újraindulásra, akkor a rendszergazda jó esetben hétfőn csak az eseménynaplóból értesül a történtekről. Ha azonban szeretnénk látni a hibaüzenetet, akkor feltétlenül ki kell kapcsolnunk az automatikus újraindítást. Ha ezt elmulasztjuk, akkor – ahogyan már korábban említettük –, az indítómenü használatával utólag is megváltoztatható ezt a beállítás *(Disable automatic restart on system failure).*

A „kék halál" mesterségesen is előidézhető több módon is. Leállíthatunk például olyan szolgáltatásokat, amelyek nélkül a rendszer működésképtelen, illetve használható a „hivatalos", valószínűleg tesztelés céljára szolgáló módszer is. Létre kell hoznunk a *CrashOnCtrlScroll DWord* értéket (1) a *HKLM\System\CurrentControlSet\i8042prt\Parameters* kulcs alatt. Újraindítás után a jobb oldali *Ctrl* nyomva tartása mellett üssük le kétszer a *Scroll Lock* billentyűt…

Grafikus ellenőrző-javító eszközök

Ha sikerült elindítanunk az operációs rendszert (akár csökkentett módban is), akkor a különféle hibák felderítéséhez és elhárításához számos beépített, grafikus felülettel rendelkező eszköz áll rendelkezésünkre, a következőkben ezek közül ismerkedünk meg a legfontosabbakkal.

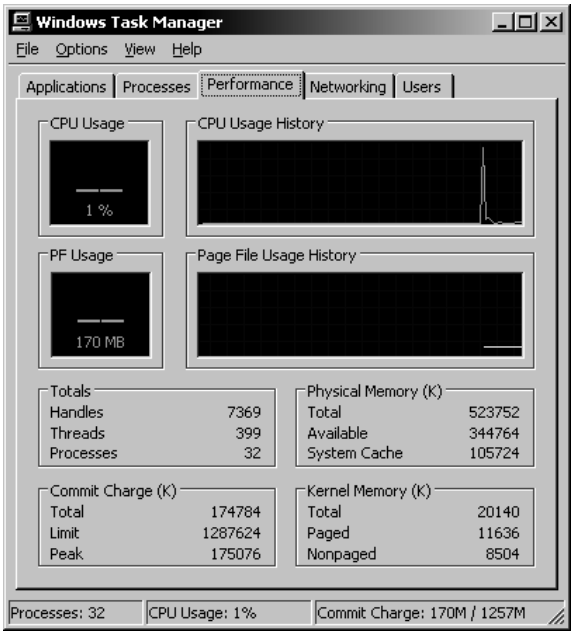
A grafikus felülettel rendelkező ellenőrző- javító eszközök használata
Ebben a screencastban kipróbáljuk a Windows rendszerek beépített ellenőrző és hibajavító eszközei küzöl a legsűrűbben használtakat.
Fájlnév: II-3-2a-GUI-eszkozok.avi

Feladatkezelő *(Task Manager)*

A Windows-rendszerek talán legtöbbet használt ellenőrző eszköze a Feladatkezelő *(Taskmgr.exe)*. Segítségével gyors, de viszonylag átfogó pillanatképet kaphatunk a rendszerben futó alkalmazásokról és folyamatokról, ellenőrizhetjük a számítógép legfontosabb terhelési adatait és megjeleníthetjük a bejelentkezett felhasználókat. Ismerkedjünk meg a Feladatkezelő egyes lapjairól leolvasható adatokkal, illetve az ott elvégezhető műveletekkel:

- **Applications** *(Alkalmazások)* – a lap elnevezése talán kissé félrevezető lehet, mivel a lapon nem a rendszerben futó alkalmazásokat, hanem az adott felhasználó munkaasztalán lévő, látható állapotú ablakok címsorait találhatjuk meg. Egy alkalmazáshoz több megnyitott ablak is tartozhat (tipikusan ilyen például a Windows Explorer), illetve számos olyan alkalmazás is futhat a gépünkön, amelyikhez egyáltalán nem tartozik látható ablak – ezek nem fognak megjelenni az Alkalmazások lapon sem. Szintén nem egészen egyértelműek az egyes ablakok állapotaként megjelenített értékek. Ha az ablak állapota *Fut (Running)*, az azt jelenti, hogy az ablak üzenetkezelő ciklusa (ez fogadja a leütött billentyűket, egérműveleteket, más folyamatoktól érkező üzeneteket stb.) késlekedés nélkül válaszol a kérésekre, vagyis az ablak mögött található alkalmazás üzenetre (bevitelre) vár, tehát nem csinál semmit. Ha az ablak állapota *Not responding (Nem válaszol)*, az jelentheti persze azt is, hogy az ablak mögött álló alkalmazás leállt (lefagyott), de az is lehetséges, hogy csak egyéb sürgős elfoglaltságai miatt éppen nem jut ideje az üzenetkezelő ciklusra. Az egyes „alkalmazásokhoz" (például a jobb gombos helyi menüből) a szokásos ablakkezelő parancsok kiadására van lehetőség [Bring to Front *(Előtérbe hozás)*, Minimize *(Kis méret)*, Maximize *(Teljes méret)* stb.]. Az End Task *(Feladat befejezése)* menüpont szintén nem az alkalmazásra, hanem az ablakra vonatkozik, a kérést első körben az üzenetkezelő ciklusnak kell(ene) fogadnia (ha ez nem sikerül, akkor komolyabb eszközökkel is próbálkozik a Feladatkezelő). Nagyon fontos a Go To Process (*Ugrás folyamatra)* menüpont, ezzel a Feladatkezelő következő lapjára kerülünk, és kijelölhetjük azt a rendszerfolyamatot, amelyikhez az adott ablak tartozik.

- **Processes** *(Folyamatok)* – ezen a lapon már a számítógépen futó összes folyamat látható, megtalálhatjuk köztük az előző oldalon felsorolt alkalmazásokhoz, a többi alkalmazáshoz és az összes rendszerszolgáltatáshoz tartozó folyamatot is. Alapértelmezés szerint itt láthatjuk a folyamathoz tartozó végrehajtható állomány nevét, a futtató felhasználót, valamint itt követhetjük nyomon a pillanatnyi memória- és processzoridő felhasználást. Itt kereshetjük meg például azt a rendszerfolyamatot, amelyik valami miatt túl sok erőforrást használ, és lelassítja a rendszert. Számos más adatot is megjeleníthetünk, ha a View *(Nézet)* menü Select Columns *(Oszlopok kiválasztása)* pontjára kattintunk. Fontos információ lehet például a folyamat azonosítója *(Process Identifier, PID)*, ezt a hibakeresés során, több helyen is felhasználhatjuk majd. A jobb gombos helyi menüben beállíthatjuk az egyes folyamatok prioritását (de csak óvatosan, mert ha egy processzt nagyon „kiemelünk" pl. a Realtime lehetőséget választva, akkor minden más folyamat iszonyúan lelassulhat), és itt közvetlenül is leállíthatjuk a nem válaszoló alkalmazásokhoz tartozó folyamatokat.
- **Performance** *(Teljesítmény)* – a Teljesítmény lapon a számítógép teljesítményével, vagyis a processzor(ok) és a memória kihasználtságával kapcsolatos információk jelennek meg. A memória kihasználtságával kapcsolatos adatok között is találhatunk néhány félreérthető nevű mezőt, így tekintsük át egyenként az adatok tartalmát.



6.6. ábra: *Az operációs rendszer legfontosabb teljesítményadatai a Feladatkezelőben*

- A **CPU Usage** *(CPU-használat)* mezővel semmi probléma nincs, százalékos érték formájában megjeleníti a processzor pillanatnyi terheltségét.
- A **PF Usage** *(Lapozófájl)* érték (és a hozzá tartozó grafikon) viszont nem a lapozófájl használatát mutatja, hanem a rendszer által lefoglalt összes memóriaterület (a fizikai memóriában és a lapozófájlban együttesen) nagyságát.
- A **Totals** *(Összesítés)* szakaszban a rendszerben futó folyamatok, programszálak és a leírók (a programok által használt erőforrások, például fájlok, registrykulcsok stb.) számát találhatjuk.
- A **Commit Charge** *(Lefoglalt memória)* szakasz három értékének jelentése a következő: a Total *(Összes)* érték a rendszer által a fizikai memóriában és a lapozófájlban lefoglalt összes memóriát jelenti (megegyezik az PF Usage kijelzőn látható értékkel). A Limit *(Korlát)* a fizikai memória és valamennyi lapozófájl összesített mérete, maximálisan ennyi memóriát foglalhatnak a folyamatok. A Peak *(Csúcsérték)* a számítógép bekapcsolása óta lefoglalt legtöbb memóriát jelenti.
- A **Physical Memory** *(Fizikai memória)* szakaszban a számítógépben lévő fizikai memória (RAM) méretét láthatjuk. Az Available *(Rendelkezésre álló)* érték a szabad memória mennyiségét jelenti, a System Cache *(Rendszergyorsítótár)* mezőről pedig a megnyitott fájlok leképezéséhez igénybe vett fizikai memória mennyiségét olvashatjuk le.
- A **Kernel Memory** *(Kernelmemória)* szakaszban az operációs rendszer magja és az eszközillesztők által használt memóriára vonatkozó adatokat találhatjuk meg. A Paged *(Lapozható)* érték a kernel által használt memória kilapozható részét jelenti, a Nonpaged *(Nem lapozható)* mező pedig az a rész, amelynek mindenképpen a fizikai memóriában kell maradnia.

- **Networking** *(Hálózat)* – ezen a lapon a számítógép engedélyezett hálózati csatolóira vonatkozó adatokat tekinthetünk meg. A grafikonok a pillanatnyi terhelés alakulását mutatják, alul pedig az alapértelmezett készleten kívül még számos további adatot is megjeleníthetünk (View menü Select Columns pontja).
- **Users** *(Felhasználók)* – a lapon láthatók a számítógépre bejelentkezett felhasználók, az egyes munkamenetek állapota és neve. A bejelentkezet felhasználóknak küldhetünk üzenetet, és szükség esetén meg is szakíthatjuk a kiválasztott munkamenetet.

Computer Management MMC

Az első fejezetben már megismerkedtünk a Vista legfontosabb MMC-alapú felügyeleti eszközeivel, és az ezzel kapcsolatos újdonságokkal, most csak azokra az elemekre fogunk koncentrálni, amelyek a Windows kiszolgálókon is megtalálhatók, és a hibakeresésben is jól felhasználhatók.

A rendszerszolgáltatások

A rendszerszolgáltatás olyan program, vagy folyamat, amely a rendszer egy meghatározott, más programok támogatására szolgáló funkcióját valósítja meg, általában alacsony, hardver közeli szinten. Minden szolgáltatás egy meghatározott felhasználói fiók használatával bejelentkezve éri el az operációs rendszer erőforrásait és objektumait. Windows Server 2003 esetén a szolgáltatások nagy többsége alapértelmezés szerint a Helyi rendszer *(Local System)* fiók használatával jelentkezik be, ami gyakorlatilag korlátlan hozzáférést biztosít a teljes rendszerhez.

A SYSTEM fiók sok esetben még az Administrators csoport tagjainál is kiterjedtebb jogokkal rendelkezik, a rendszerleíró adatbázis néhány területéhez például csak a SYSTEM fióknak van jogosultsága, az *administrator* még csak be sem nézhet oda. Bár a SYSTEM fiókkal természetesen nem lehet közvetlenül bejelentkezni, egy egyszerű trükk segítségével mégis elindíthatunk a SYSTEM nevében futó programokat; ha egy tetszőleges programot a SYSTEM fiókkal bejelentkező Feladatütemező szolgáltatás indít el, az természetesen szintén a SYSTEM fiók nevében fog futni. Ha tehát például kiadjuk a következő parancsot: *C:\>at 21:00:00 /interactive cmd*, akkor (majd este kilenckor) kapunk egy SYSTEM jogokkal futó parancssort, ahonnan már bármilyen más programot is ugyanilyen jogosultsági szinttel indíthatunk el.

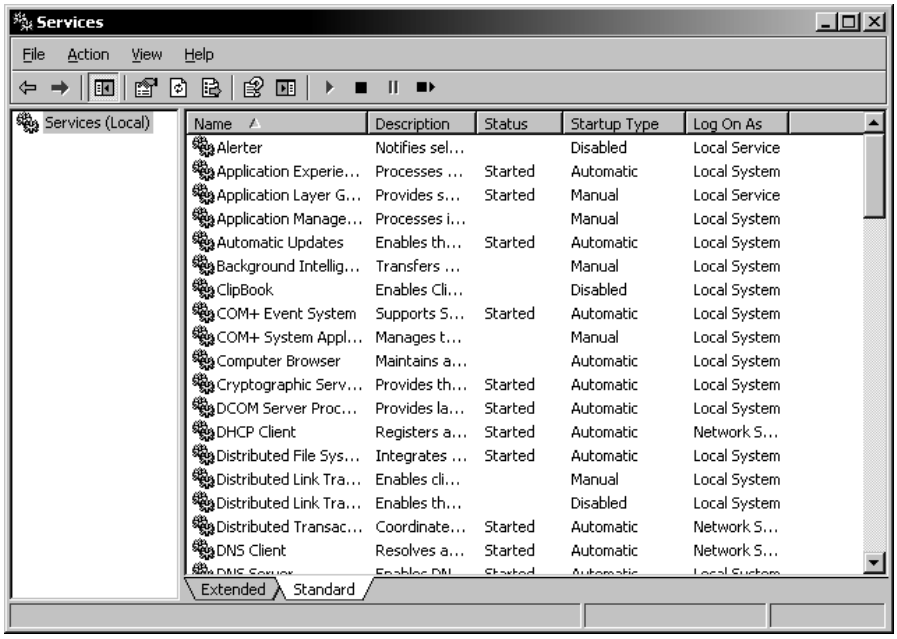
Ha a SYSTEM fiókkal bejelentkező szolgáltatás tartományvezérlőn fut, akkor nemcsak magához a számítógéphez, hanem a teljes tartományhoz is korlátlan hozzáféréssel rendelkezik.

Más, korlátozott jogosultsági szinttel is megelégedő szolgáltatások a Network Service *(Hálózati szolgáltatás),* vagy a Local Service *(Helyi szolgáltatás)* fiók használatával jelentkezhetnek be, amelyek jelentősen kevesebb jogosultsággal (és veszéllyel) járnak. Az előbbi esetben (Network Service) a szolgáltatás csak a hálózaton, míg a Local Service használata esetén csak a helyi gépen kap jogosultságokat. A szolgáltatások hozzáférési szintjének korlátozása a rendszer védelmét szolgálja az adott szolgáltatás hibás működése, vagy egy ellene irányuló külső támadás esetén. Ahogyan már korábban is említettük, a Vista operációs rendszerben drasztikusan csökkent a SYSTEM fiók nevében futó szolgáltatások száma, éppen a biztonsággal kapcsolatos megfontolások következtében.

A szolgáltatások három különböző indítási típusba tartozhatnak. Az automatikus indításúak a rendszer indításával együtt elindulnak és többségük folyamatosan aktív marad a teljes rendszer, vagy az adott szolgáltatás leállításáig. A kézi indítású szolgáltatásokat szükség esetén a felhasználó, illetve különféle programok vagy más szolgáltatások indíthatják el, a tiltott szolgáltatások pedig sem automatikusan, sem manuálisan nem indíthatók el.

A Services *(Szolgáltatások)* MMC-modul segítségével (meglepetés!) a rendszerben futó szolgáltatások állapotáról kaphatunk információt, illetve beállíthatjuk a futtatásukkal kapcsolatos különféle paramétereket. Amint a 6.7. ábrán látható, a listában megtalálhatjuk a szolgáltatások nevét, rövid leírását, aktuális állapotát, indítási típusát és azt a felhasználónevet, amelynek használatával a szolgáltatás bejelentkezik a rendszerbe.

A szolgáltatásokkal kapcsolatos hibák gyors felmérése jól felhasználható, ha a sorokat az indítási típus szerinti sorrendbe rendezzük. Ekkor az automatikus típus kerül a lista elejére, így könnyen észrevehetjük, ha egy ilyen szolgáltatás valami miatt nem indult el. (Néhány automatikusan induló szolgáltatásnak nem kell folyamatosan futnia, de ezekből meglehetősen kevés van.)



6.7. ábra: *A Szolgáltatások kezelésére szolgáló MMC-modul*

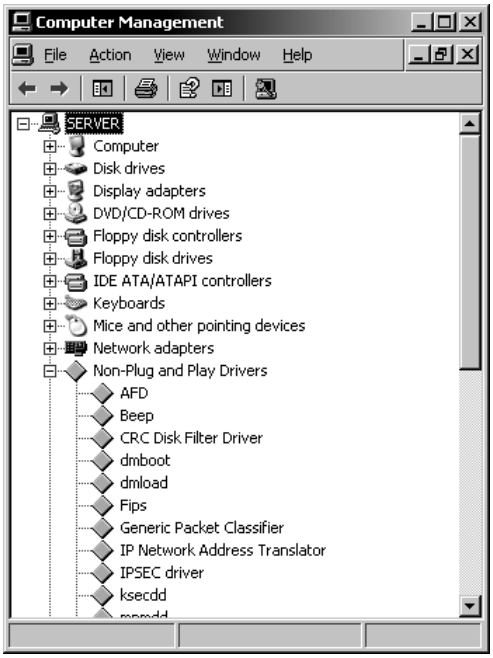
A további adatokat megjelenítő, illetve bizonyos paraméterek beállítását is lehetővé tévő párbeszédablak megjelenítéséhez duplán kell kattintanunk az adott szolgáltatást reprezentáló sorra. A párbeszédablak lapjain megadhatjuk a

szolgáltatás indítási típusát, és a futtató felhasználói fiókot (le is állíthatjuk, illetve elindíthatjuk a szolgáltatást). A Recovery *(Helyreállítás)* lapon megadhatjuk, hogy mi történjen, ha a szolgáltatás leáll az első, második, illetve harmadik alkalommal. Újraindítható az adott szolgáltatás, maga a számítógép, illetve lefuttathatunk egy tetszőleges programot is. Ezek a lehetőségek számos esetben nagyon hasznosak lehetnek, hiszen egy szolgáltatás leállása komoly problémát okozhat, de ezt a szolgáltatás, vagy a számítógép újraindítása a legtöbb esetben megoldja (hacsak nincs nagyobb baj), az elindított program pedig értesítheti például a rendszergazdát, vagy a felhasználókat.

A hibakeresés szempontjából talán a Dependencies *(Függőségek)* lap tartalma lehet a legfontosabb. Innen azt olvashatjuk le, hogy az adott szolgáltatás mely más szolgáltatásoktól függ (vagyis minek kell futnia, hogy ő elindulhasson), és mely szolgáltatások függenek tőle (vagyis mi minden fog leállni az adott szolgáltatással együtt).

Az Eszközkezelő

Az Eszközkezelő *(Device Manager)* a számítógépre telepített hardvereszközök grafikus nézetét biztosítja; segítségével frissíthetjük a hardvereszközök illesztőprogramjait, módosíthatjuk a hardverelemekkel kapcsolatos különféle beállításokat, és felderíthetjük, illetve elháríthatjuk a hibákat.



6.8. ábra: *Az Eszközkezelő a rejtett (nem Plug and Play) eszközök megjelenítésére és eltávolítására is képes*

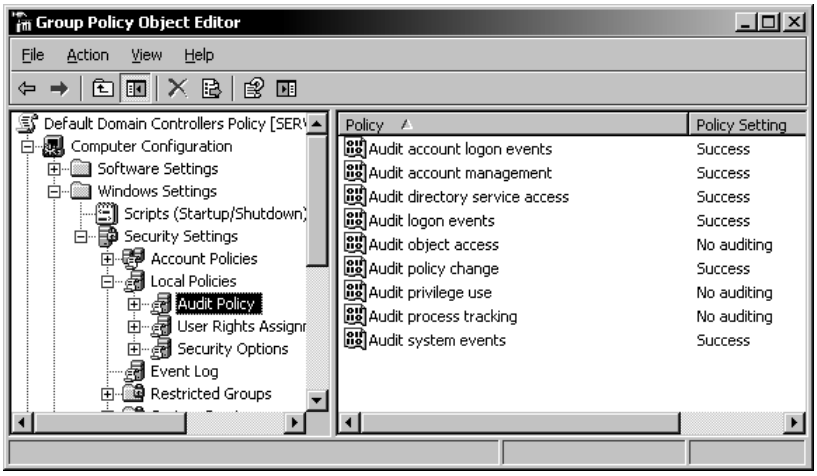
Az Eszközkezelő segítségével gyors, áttekintő képet kaphatunk a számítógép hardvereszközeiről, ellenőrizhetjük azok megfelelő működését, illetve módosíthatjuk a hardverelemek erőforrásokkal (megszakítás, I/O tartomány stb.) kapcsolatos beállításait.

Ugyancsak az Eszközkezelő ad lehetőséget a hardvereszközök illesztőprogramjainak frissítésére, illetve a korábban már megtárgyalt Árnyékmásolat szolgáltatás segítségével rosszul sikerült frissítés esetén vissza is térhetünk az előző verzióra (Driver Rollback).

Fontos lehetőség, hogy az eszközkezelő a nem Plug and Play hardvereszközök megjelenítésére (és eltávolítására) is lehetőséget ad. Az ilyen eszközök esetében ugyanis nemcsak a telepítés, hanem az eltávolítás sem mindig automatikus, ha az eltávolítást végző program nem fut le tökéletesen, akkor az illesztőprogram a hardvereszköz fizikai eltávolítása után is aktív maradhat, foglalhatja a rendszer erőforrásait, és esetleg más problémákat is okozhat. A rejtett eszközök megjelenítéséhez kapcsoljuk be a View → Show hidden devices *(Nézet → Rejtett eszközök megjelenítése)* opciót.

Az Eseménynapló

Az Eseménynapló szolgáltatás által készített naplók segítségével nyomon követhetjük a számítógép egyes komponenseinek működését, és gyorsan értesülhetünk a különféle problémákról. Természetesen lehetőségünk van az események különféle tulajdonságai (típus, forrás, dátum stb.) szerinti szűrésre és keresésre is. A Windows Server 2003 családba tartozó operációs rendszerek alapértelmezés szerint háromféle naplóban rögzítik az eseményeket:



6.9. ábra: *A tartományvezérlők naplórendje*

- Az **alkalmazásnapló** *(Application log)* a különféle alkalmazások által naplózott eseményeket tartalmazza. Ide jegyzi be a futása közben történt eseményeket valamennyi Microsoft program, de számos más forrásból származó alkalmazás üzeneteit is megtalálhatjuk itt. Az alkalmazásnaplóba kerülő üzenetek tartalma és mennyisége teljes mértékben az egyes alkalmazások fejlesztőinek hatáskörébe tartozik, bármelyik program felkészíthető az Eseménynapló használatára.
- A **biztonsági napló** *(Security log)* az érvényes és érvénytelen bejelentkezési kísérleteket, valamint a különféle erőforrások (például fájlok) létrehozását, megnyitását vagy törlését tartalmazza. A biztonsági naplóba kerülő események körét a csoportházirend, (illetve a helyi házirend) beállításai határozzák meg.
- A **rendszernapló** *(System log)* a Windows rendszerösszetevői által naplózott eseményeket tartalmazza. Ide kerülnek a különféle illesztőprogramokkal és más rendszerösszetevőkkel kapcsolatos események, például a sikertelen betöltés, leállás stb.

A tartományvezérlőkön a fentieken kívül még legalább két másik naplót is találhatunk:

- A **címtár-szolgáltatási napló** *(Directory Service log)* az Active Directory-szolgáltatás által naplózott eseményeket tartalmazza, ide kerülnek például a címtáradatbázis replikációjával kapcsolatos különféle bejegyzések.
- A **Fájlreplikációs szolgáltatás naplója** *(File Replication Service log)* a Fájlreplikációs szolgáltatása által naplózott eseményeket tartalmazza. A rendszer ebben a naplóban rögzíti például a tartományvezérlők SYSVOL-mappáinak szinkronizálásakor bekövetkező hibákat.
- Ha a tartományvezérlő egyben DNS-kiszolgáló is, akkor egy további naplót is találhatunk rajta. A **DNS-kiszolgálónapló** *(DNS Server log)* a DNS-szolgáltatás által naplózott eseményeket tartalmazza.

Az egyes naplók méretére, illetve a maximális méret elérésekor bekövetkező eseményekre vonatkozó beállításokat az egyes naplók tulajdonságlapján, illetve a csoportházirend segítségével határozhatjuk meg. Valamennyi napló esetében lehetőség van a bejegyzések fájlba mentésére, az így elkészült fájlt pedig akár egy másik számítógépen is importálhatjuk.

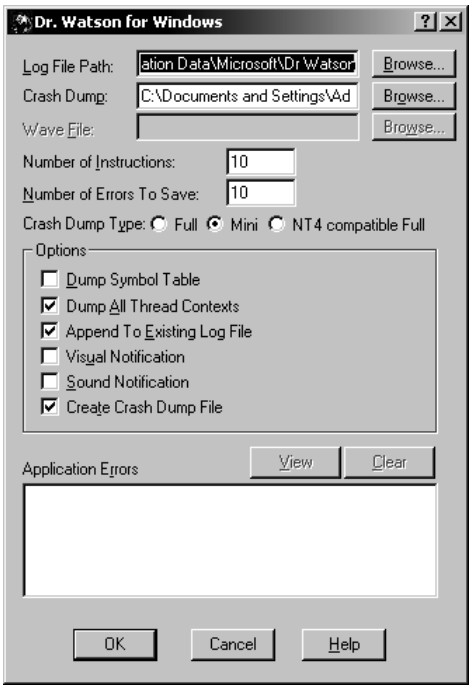
A naplókba kerülő bejegyzések a következő öt típus valamelyikébe tartoznak:

- **Hiba** *(Error)* – Jelentős, már bekövetkezett probléma, például egy szolgáltatás sikertelen indítási kísérlete, vagy leállása, egy alkalmazás „lefagyása" stb.
- **Figyelmezetés** *(Warning)* – Nem feltétlenül jelentős, de a jövőben könnyen súlyosabb problémába torkolló esemény. Figyelmeztetés kerül például a naplóba, ha a rendszerköteten (vagy máshol) lecsökken a szabad lemezterület, ha nem törődünk a figyelmeztetéssel, az a legtöbb hibánál is súlyosabb következményekkel járhat. Nem érdemes tehát csak a hibákra szűrve olvasgatni a naplókat, mert így nem kerülnek a szemünk elé azok a bejegyzések, amelyek előre jelezhetnék a későbbi komolyabb problémákat.
- **Információ** *(Information)* – Egy alkalmazás, illesztőprogram vagy szolgáltatás sikeres működését leíró esemény. Amikor például betöltődik egy hálózati csatoló illesztőprogramja a naplóba Információ típusú bejegyzés kerül.
- **Sikeres események naplózása** *(Success Audit)* – Ilyen típusú bejegyzésekkel a biztonsági naplóban találkozhatunk. Sikeres eseménynek minősül például, ha egy felhasználónak sikerül bejelentkeznie a rendszerbe.
- **Sikertelen események naplózása** *(Failure Audit)* – Szintén csak a biztonsági naplóba kerülhetnek ezek az események, ilyen bejegyzés készül például egy hálózati meghajtóhoz való sikertelen hozzáférési kísérlet esetén.

Az Eseménynaplóba kerülő hibák (és sok esetben a figyelmeztetések is) mindenképpen törődést érdemelnek, bár gyakran előfordul az is, hogy semmi különös teendőnk nincs, mert például egyszerűen a számítógép újraindítása megoldja a problémát. Ebben az esetben sem árt azonban, ha a naplóbejegyzésben található eseményazonosító alapján rákeresünk a hibaüzenetre a Microsoft Tudásbázisban *(http://support.microsoft.com),* ahol gyakorlatilag minden elképzelhető bejegyzéssel kapcsolatban részletes, megbízható forrásból származó információt kapunk (a legtöbb esetben persze angolul, bár van néhány magyarított cikk is). Megtudhatjuk, hogy mi okozhatja a jelenséget, és mi lehet a megoldás (például javítócsomag letöltése és telepítése, beállítások módosítása stb.). Szintén jól használható forrás lehet a *http://eventid.net* webhely, ahová akár mi magunk is feltölthetjük egy adott problémával kapcsolatos kérdésünket, illetve válaszolhatunk mások kérdéseire is. Természetesen sok esetben jól használhatók az általános keresők is.

Dr. Watson

Dr. Watson egy hibakereső/nyomkövető alkalmazás, ami összegyűjti a különféle programhibákkal kapcsolatos tényeket, hogy aztán ezek alapján Sherlock Holmes (a rendszergazda) rendkívül éles elméjével levonhassa a megfelelő következtetéseket.



6.10. ábra: *Dr. Watson megkapja az instrukciókat*

Programhiba, illetve kezeletlen kivétel esetén Dr. Watson automatikusan akcióba lendül, hozzákapcsolódik a hibás alkalmazáshoz vagy szolgáltatáshoz, megvizsgálja a hibát és a DRWTSN32.LOG nevű szöveges naplófájlba írja a vizsgálat eredményét (és bejegyzést készít az Eseménynaplóba is). Dr. Watson segítségével létrehozhatunk a memória tartalmát tároló bináris fájlt is, amely aztán speciális hibakereső alkalmazás segítségével elemezhető.

Dr. Watson beállításainak (például a naplófájl és a memóriakép tárolómappája) megadásához a *drwtsn32.exe* programot kell elindítanunk.

Hálózati gondok megoldása

A következőkben a hálózati hibák felderítésére szolgáló legfontosabb eszközökkel fogunk megismerkedni. Számos kisebb-nagyobb program használható erre a célra, először néhány egyszerű parancssori eszközzel, majd egy komolyabb, egészen mély vizsgálatot és elemzést is lehetővé tevő alkalmazással foglalkozunk.

A hálózat diagnosztikai eszközei
Ebben a mini bemutatóban megmutatjuk a hálózati hibák felderítéséhez használható eszközöket.
Fájlnév: II-3-2b-Halozat-eszkozok.avi

Az ***ipconfig*** parancs segítségével megjeleníthetjük a hálózati csatolókhoz tartozó TCP/IP-paramétereket, frissíthetjük a csatolók a DHCP-beállításait és bejegyeztethetjük a paramétereket a DNS-kiszolgáló adatbázisába. Ha paraméter nélkül adjuk ki az *ipconfig* parancsot, akkor megjeleníthetjük az összes adapter IPv6- vagy IPv4-címét, alhálózati maszkját és alapértelmezett átjáróját. Ha a parancsot az */all* kapcsolóval indítjuk el, akkor igen részletes adatokat kapunk valamennyi csatolóról, így könnyen áttekinthetjük a beállításokat, és gyorsan megtalálhatjuk az esetleg elgépelt, vagy más ok miatt hibás értékeket.

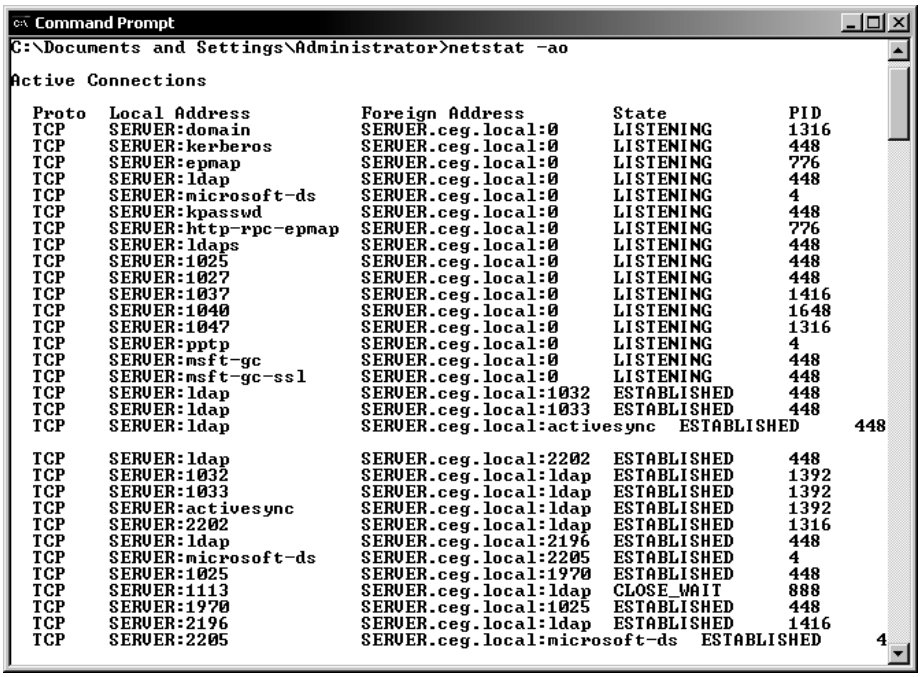
A ***NetStat*** paranccsal protokollstatisztikát és az aktív TCP/IP-kapcsolatokat jeleníthetjük meg. A *-r* kapcsoló használatával kilistázhatjuk a számítógép útválasztási táblázatát, a *-e* kapcsolóval pedig a küldött és fogadott Ethernet keretekre vonatkozó statisztikai adatokat jeleníthetjük meg. A *-s* kapcsoló segítségével protokollonkénti bontásban kapunk statisztikát a számítógép TCP/IP-forgalmáról.

A ***netstat –a*** parancs segítségével az aktív kapcsolatokat listázhatjuk ki, megjelenik használt protokoll, a nyitott port száma, és a kapcsolat állapota. Fontos információt kaphatunk a *netstat –ao* parancs használatával, mivel ekkor az előző lista kiegészül az egyes kapcsolatokat nyitva tartó folyamat azonosítójával (PID) is. A PID-et felhasználva a Feladatkezelő segítségével gyorsan beazonosítható az adott kapcsolatot nyitva tartó rendszerfolyamat.

Az ***Nbtstat*** parancs hasznos eszköz a NetBIOS-alapú név-hozzárendelési problémák hibakeresésében. Az *nbtstat* paranccsal megjeleníthetjük az aktív NetBIOS-munkamenetek listáját, azok állapotát, és a munkamenetekre vonatkozó statisztikai adatokat, illetve kilistázhatjuk vagy megújíthatjuk a gyorsítótárakban és a WINS-kiszolgálón regisztrált névhozzárendeléseket.

Az ***Arp*** parancs segítségével a címfeloldási protokoll *(Address Resolution Protocol, ARP)* által a hálózati forgalom csökkentéséhez használt címfordítási táblázat, vagyis az ARP-gyorsítótár tartalmát jeleníthetjük meg. Az ARP végzi a

kimenő Ethernet-keretekbe kerülő MAC-címek meghatározását az IP-címek alapján. Az ARP-gyorsítótár tartalmát az *arp –a* paranccsal jeleníthetjük meg, az *arp –s* használatával pedig új statikus bejegyzéseket adhatunk a táblázathoz.



6.11. ábra: *A tartományvezérlő igen sok ponton kapcsolódik a hálózathoz*

A ***NetDiag***-program a kiszolgáló operációs rendszerek telepítőlemezén, a Support Tools csomagban található, a csomag telepítésével kerül fel a gépre *(\support\tools\suptools.msi)*. A parancs segítségével a különféle hálózati komponensek részletes vizsgálatát végezhetjük el. A program megvizsgálja valamennyi fontos hálózati elem működését (TCP/IP-paraméterek, NetBIOS, tartományvezérlők, különféle szolgáltatások elérhetősége stb.).

A ***Tracert*** nevű nyomkövető segédprogram a hálózati csomagok útvonalának meghatározására használható, segítségével listát készíthetünk azokról az útválasztókról, amelyeken egy megadott cél felé tartó csomagok áthaladnak. A *tracert* a következők szerint működik: A program ICMP *Echo* üzeneteket küld a cél IP-cím felé, amelyeknek TTL (Time to Live) értéke folyamatosan növekszik. A TTL érték 1-gyel indul, vagyis az első kiküldött csomag csak az első útválasztóig jut el, itt a TTL nullára csökken. Az útválasztó ilyenkor nem küldi tovább a csomagot, hanem ICMP Time Exceeded – TTL Exceeded in Transit hibaüzenetben értesíti a küldőt az eseményről. A *Tracert*-program feljegyzi a hibaüzenetet, (amely természetesen tartalmazza a feladó, vagyis

az első útválasztó címét is) és új csomagot küld a célcím felé, egyel nagyobb TTL-értékkel. Ez a csomag a második útválasztón fog hibaüzenetet generálni, így a *tracert* már ennek a címét is feljegyezheti. Mire a csomag eljut a címzetthez, a *tracert* az összes útválasztó címét ismerni fogja, amelyeken a csomag áthaladt. Ezután a *tracert* listát készít a hibaüzenetekből kinyert útválasztó-címekből, és a címhez DNS-lekérdezés segítségével meghatározott nevekből. Ha használjuk a *-d* opciót, a program nem hajt végre DNS-lekérdezést, ilyenkor csak az útválasztók IP-címei jelennek meg. A *tracert* parancs felhasználható annak a meghatározására, hogy egy adott csomag továbbítása a hálózat mely pontján lett leállítva.

A ***ping*** parancssori segédprogram a megadott célállomás működőképességének ellenőrzésére szolgál. A ping ICMP *Echo* üzeneteket küld a megadott IP-cím felé, majd várakozni kezd a címzettől érkező ICMP *Echo Reply* üzenetekre. A program kiírja a beérkezett válaszüzenetek számát, valamint a kérés elküldése és a válasz megérkezése között eltelt időt.

A ***pathping*** nevű parancssori eszköz a *ping* és a *tracert* funkcionalitásának kombinációját nyújtja, és néhány további szolgáltatással is rendelkezik. Az útvonal feltérképezése mellett a *pathping* minden egyes útválasztót többször is pingel, és megjeleníti a késleltetéssel és elveszett csomagokkal kapcsolatos információkat. Ilyen módon felmérhetjük az útvonalon elhelyezkedő rossz átvivő képességű vonalakat és útválasztókat.

Az ***nslookup*** program a DNS-infrastruktúra hibakereséséhez használható adatok megjelenítésére alkalmas. Segítségével lekérdezhetjük a megadott DNS-kiszolgáló adatbázisában tárolt értékeket (számítógépnév megadásával IP-címet és fordítva). A parancs első paramétereként a lekérdezendő nevet, vagy IP-címet kell megadnunk, második paraméterként pedig megadhatjuk annak a DNS-kiszolgálónak a nevét (vagy IP-címét), amelynek a lekérdezését el kell küldeni. Ha nem adunk meg második paramétert, akkor a számítógépen beállított alapértelmezett DNS-kiszolgáló fog válaszolni. Az *nslookup* nagyon jól használható a névfeloldással kapcsolatos egyszerűbb hibák gyors felderítésére, ha ilyen problémára gyanakszunk érdemes mindig ezzel kezdeni a hibakeresést.

6.12. ábra: *A kiszolgáló saját magától kérdezi meg az IP-címét*

Network Monitor

Az eddigiekkel szemben a Network Monitor már egyáltalán nem nevezhető egyszerű eszköznek, de szakértő kézben gyakorlatilag bármire képes; segítségével a hálózati működés legmélyebb rétegeibe is betekintést nyerhetünk. A program segítségével rögzíthetjük és megvizsgálhatjuk a gépünkhöz érkező vagy kimenő valamennyi hálózati csomagot, ezeket a Network Monitor a hálózati architektúra NDIS rétegének megcsapolásával gyűjti össze számunkra. Mivel az NDIS meghajtó a hierarchia legalacsonyabb szoftveres rétege (alatta már csak a hálózati adapter hardvere található), a Network Monitor segítségével minden olyan csomagot láthatunk, amit a hálózati adapter továbbküld az operációs rendszer felé.

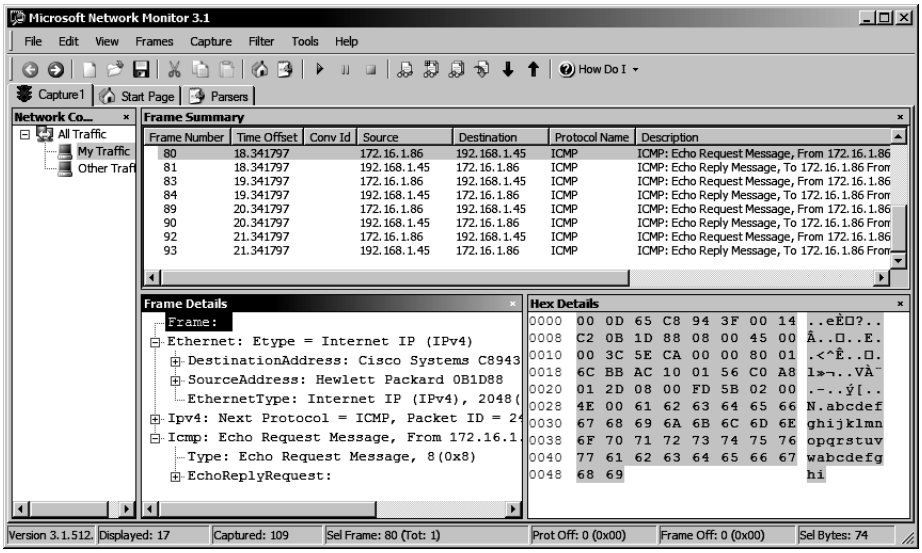
Az üzenetszórásos hálózat működési elve szerint (a switchekkel összekapcsolt hálózattal most nem foglalkozunk), minden egyes csomagot a hálózatra kapcsolt valamennyi gép megkap. Ezután a hálózati adapter hardveresen összehasonlítja az Ethernet csomagban lévő cél MAC-címet a sajátjával, és csak a neki szánt csomagokat küldi tovább a feljebb lévő szoftveres rétegek felé. A Network Monitor driver ezt a hardveres szűrést kapcsolja ki (promiszkusz mód), így megjelenítheti a hálózaton elérhető valamennyi csomag tartalmát.

A promiszkusz mód korábban csak a SMS részeként beszerezhető Network Monitor Gold verzióban volt használható (a kiszolgáló operációs rendszerek részeként kapott alapváltozatban nem), de a legújabb, 3.1-es verzióban már nincs ilyen megkülönböztetés, a p-módnak elnevezett üzemmód egyszerűen ki- és bekapcsolható a grafikus felületen.

Egyetlen esetben nem jelenik meg a hálózati csomag a Network Monitorban; ha az Ethernet keret CRC-je hibás, a hálózati adapter semmiképpen nem küldi tovább a csomagot. A Network Monitor használatával összegyűjthetjük azokat az információkat, amelyek segítségünkre lehetnek a hálózat hibátlan működésének fenntartásában, és az esetleges hibák gyors kiküszöbölésében.

A Network Monitor programot beállíthatjuk úgy, hogy csak azokat az adatokat jelenítse meg, amelyekre az adott helyzetben éppen szükségünk van. Szűrők segítségével szabályozhatjuk a csomagok megjelenítését és elrejtését, például a csomag típusa (protokoll), vagy forrás-, illetve célcíme alapján. Beállíthatjuk azt is, hogy a Network Monitor bizonyos feltétel, vagy feltételek teljesülése esetén automatikusan elindítsa, vagy leállítsa a csomagok gyűjtését. Természetesen lehetőségünk van a megjelenítés paramétereinek beállítására is, például a különböző csomagtípusokat különböző színnel jeleníthetjük meg.

A Network Monitor segítségével az összegyűjtött adatokat fájlba is menthetjük későbbi vizsgálat és elemzés céljából.

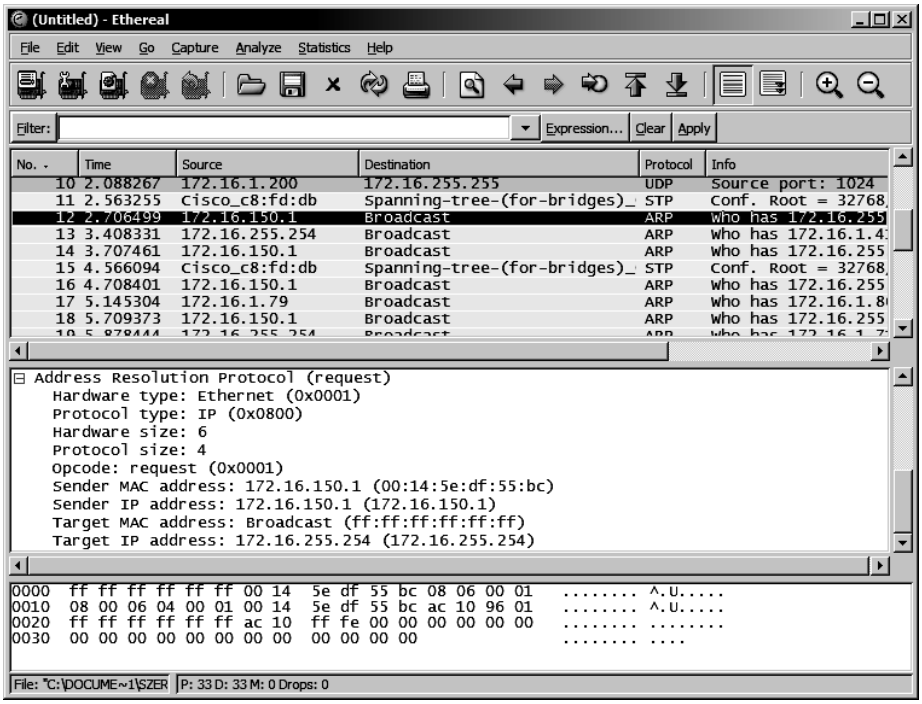


6.13. ábra: *A ping program hálózati forgalma a Network Monitorban*

A Network Monitor régebbi verzióit a Windows kiszolgáló operációs rendszerek beépítetten tartalmazzák (az Add or Remove Programs *(Programok telepítése és törlése)* segítségével telepíthető), a legújabb, 3.1-es verzió pedig szabadon letölthető a Microsoft webhelyről. Az új verzió számos új funkcióval rendelkezik, képes például a vezeték nélküli hálózatok forgalmának megfigyelésére, a Vista RAS-kapcsolatainak (beleértve a VPN-kapcsolatokat is) ellenőrzésére. Az új Network Monitor a szokásos módon a Microsoft Update, (illetve a vállalat saját WSUS-kiszolgálója) segítségével frissíthető.

Ethereal

Az Ethereal egy másik hálózatmonitorozó program, amelynek funkciói nagyjából megegyeznek a Network Monitor lehetőségeivel, de számos beállítása valamivel egyszerűbben adható meg, ezért kezdésnek talán jobban ajánlható. Az Ethereal számos platformra (Windows, MAC, különféle Linux és UNIX verziók) ingyenesen letölthető a *http://www.ethereal.com/download.html* címről.



6.14. ábra: *Broadcast ARP-lekérdezés megjelenítése az Ethereal programban*

Adataink biztonsága

A biztonsági mentés és visszaállítás beállításai és időzítése
Ebben a screencastban az NTBackup programé a főszerep, megmutatjuk a különféle beállítási lehetőségeit, biztonsági mentést készítünk néhány fájlról, majd visszaállítjuk azokat.
Fájlnév: II-3-3a-NTBackup.avi

A biztonsági mentés a hibaelhárítás utolsó védelmi vonala, segítségével még a legsúlyosabb esetekben is elkerülhető értékes adataink teljes elvesztése. Természetesen csak akkor szabad ehhez az eszközhöz nyúlnunk (persze nem a mentésről, hanem a helyreállításról van szó), ha más módszertől már nem remélhetünk eredményt, hiszen a biztonsági mentésből való helyreállítás szükségszerűen adatvesztéssel jár; a mentések ütemezése határozza meg az elveszíthető adatok maximális mennyiségét.

Meg kell jegyeznünk, hogy a redundáns lemez-alrendszerek (hardveres RAID) semmiképpen nem helyettesíthetik a rendszeres biztonsági mentéseket, hiszen nem nyújtanak védelmet az adatok szándékos vagy véletlen (például figyelmetlenség, vagy szoftverhiba miatt) törlése ellen, illetve a hardverrel kapcsolatos katasztrófa (több lemez egyidejű meghibásodása, tűzeset stb.) esetén is elveszíthetjük adatainkat. A redundáns alrendszerek alapvetően nem az adatbiztonságot (részben persze azt is), hanem a rendelkezésre állást növelik.

Nagyon fontos, hogy két fogalmat pontosan megkülönböztessünk egymástól:

- **Biztonsági mentés** – adatok másolása egy alternatív médiára, az adatvesztés elkerülése (csökkentése) miatt. A mentett állományok hosszú távú megőrzése általában nem szükséges.
- **Archiválás** – az adatok áthelyezése olyan médiára, mely biztosítja a hosszú távú megőrzést (ezt általában különféle előírások szabályozzák) és többnyire keresési lehetőséget is nyújt.

A mentési rendszer megtervezésével kapcsolatban számos olyan szempontot kell figyelembe vennünk, amelyek teljes mértékben a helyi, egyedi adottságoktól függenek, így sajnos nem létezik általánosan használható recept. A következőkben azokat a kérdéseket tekintjük át, amelyekre választ kell találnunk a tervezés során:

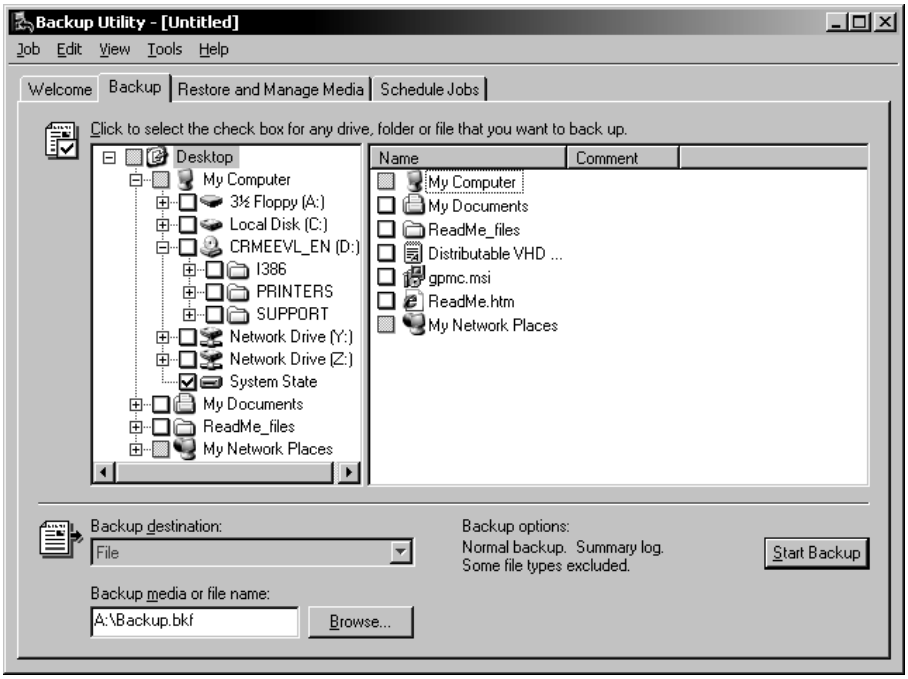
- **Mit mentsünk?** (És mit ne?) – Mentsünk rendszeresen minden olyan adatot, amelynek elvesztése problémát okoz, és más módon való helyreállítása nem lehetséges, illetve több munkával jár, mint a mentési fájl visszatöltése. Semmiképpen nem érdemes azonban lementeni tehát azokat az adatokat, amelyek helyreállítására biztosan nem lesz szükség, illetve azokat sem, amelyek más módon is könnyen helyreállíthatóak. Fölösleges adatra jó példa a TEMP könyvtár és teljes tartalma, a felhasználók profiljába az Internet Explorer által lementet weblaptöredékek stb. Könnyen helyreállítható adatnak minősülhet például az Office programcsomag, és más alkalmazások. Bár az NTBackup képes a megnyitott fájlok mentésére is, mégsem érdemes a rendszerhez tartozó nyitott fájlokkal próbálkozni. Teljesen fölösleges például bevenni a mentésbe a Windows lapozófájlját *(pagefile.sys),* vagy az Active Directory-adatbázisfájljait *(ntds.dit)* stb. (az Active Directory mentése a System State mentés része, a fájlok közvetlen mentésére nincs szükség).
- **Milyen sűrűn mentsünk?** – Amint már említettük, a mentések sűrűségét az elveszíthető adatok maximális mennyiségének kell meghatároznia. Minél kevesebb (rövidebb idő alatt keletkező) adat elvesztését képes különösebb probléma nélkül elviselni a vállalat, annál gyakrab-

ban kell mentéseket végeznünk. Természetesen a mentések gyakoriságának meghatározásakor figyelembe kell vennünk a tárolt (és mentendő) adatok közötti különbségeket is: a gyakran változó, értékes állományokat sűrűbben, a ritkábban módosított adatokat pedig ritkábban kell menteni (esetleg elegendő az egyszeri archiválás is).

- **Mire mentsünk?** – Nagyon fontos kérdés a biztonsági mentéseket tároló eszközök és a média (merevlemez, szalag, optikai lemezek stb.) kiválasztása is. A kiszolgálóban lévő második merevlemeztől, a különféle szalagos meghajtókon keresztül az önálló, automatizált tárolóegységekig számtalan megoldás közül választhatunk, az optimális megoldás megtalálásához figyelembe kell vennünk a szükséges kapacitást, a sebességet, a megbízhatóságot, tartósságot, és a fajlagos költséget is. A mentéseket tartalmazó média tárolására lehetőség szerint válasszunk olyan megoldást, ami komolyabb katasztrófa esetén is megfelelő biztonságot nyújt: szükséges lehet a kiszolgálótól fizikailag is elkülönített (akár különálló telephelyen lévő) tároló hely, tűzbiztos kazetta stb.
- **Mikor mentsünk?** – Az adatok mentését célszerű olyan időpontra időzíteni, amikor várhatóan nincsen sok megnyitott fájl (bár ezek korábbi verzióit az árnyékmásolat technológia segítségével az NTBackup képes lementeni), és a mentés által lefoglalt erőforrások hiánya nem zavarja a felhasználókat. Szokásos irodai környezetben ez azt jelenti, hogy a mentéseket az éjszakai órákra és a hétvégére kell időzítenünk. Ebből következően a mentések elvégzésére korlátozott időintervallum áll rendelkezésre, ezt figyelembe kell vennünk a mentendő adatok körének (mennyiségének) meghatározásakor, és ennek megfelelően kell kiválasztanunk a mentés típusát (a mentés különféle típusairól később még szót ejtünk) és a felhasználandó eszközöket is.
- **Mennyi ideig fog tartani a visszaállítás?** – Természetesen már a mentések megtervezésekor figyelembe kell vennünk a visszaállítással kapcsolatos szempontokat. Hogy maximálisan mennyi időt vehet igénybe a visszaállítás, azt alapvetően a vállalat működése határozza meg, az elvárt szintidőnek megfelelően kell megvalósítanunk és beállítanunk a mentési rendszert.
- **Ki fogja elvégezni a mentést?** – A fájlok mentését azok tulajdonosai és a legalább olvasási joggal rendelkező felhasználók végezhetik el, ennek megfelelően kell beállítanunk az időzített mentésekhez tartozó felhasználói fiókot. Az Administrators, Backup operators és Server operators csoportok tagjai még olyan fájlok mentésére is képesek, amelyekhez egyébként semmiféle jogosultsággal nem rendelkeznek.

Az NTBackup

A biztonsági mentések elvégzésére a Windows-rendszerek beépített NTBackup programját használhatjuk. Természetesen a megfelelő pénzösszeg ellenében választhatunk más megoldást is – számos kifinomultabb, több lehetőséggel rendelkező rendszer van a piacon –, de kisvállalati környezetben az NTBackup gyakorlatilag mindent tud, amire szükségünk lehet.



6.15. ábra: *Az NTBackup grafikus felülete*

Az NTBackup segítségével a következő feladatokat végezhetjük el:

- Kiválasztott fájlok és mappák mentése és visszatöltése.
- Megnyitott fájlok mentése az árnyékmásolat technika segítségével. Az árnyékmásolatokról *(Shadow Copies)* és a kapcsolódó beállítási lehetőségekről a negyedik, **Kiszolgáló a hálózatban** című fejezetben részletes leírás található.
- Másolat készítése a számítógép rendszerállapotáról (System State mentés).

Az NTBackup program a csak a helyi rendszerállapot adatok mentésére képes, távoli számítógépek rendszerállapotának mentésére nincs lehetőség.

- Automatikus rendszer-helyreállításhoz (*Automated System Recovery, ASR)* szükséges fájlok és konfigurációs beállítások mentése és helyreállítása.
- A távtárolókon és felcsatolt hálózati meghajtókon található adatok mentése.
- Naplófájl készítése a biztonsági mentés folyamatáról.
- Másolat készítése a rendszerpartícióról, a rendszerindító partícióról és rendszerindításhoz szükséges fájlokról.
- A biztonsági másolatok automatikus elkészítésének időzítése.
- A mentéshez felhasznált média alapszintű kezelése (például formázás). Az NTBackup gyakorlatilag bármilyen médiára képes mentést készíteni.
- Online adatbázist használó Microsoft termékek adatainak mentése.

Az NTBackup nemcsak a grafikus felület, hanem parancssori paraméterek segítségével is teljeskörűen vezérelhető, így lehetőség van a parancsfájlból, vagy különféle szkriptnyelvekből való használatára is.

System State mentés

A tartományvezérlőkön elvégezhető rendszerállapot mentésről az előző, **Tartományi környezet** című fejezetben már volt szó, most csak röviden áttekintjük, hogy a számítógép funkciójától függően milyen adatok kerülnek bele ebbe a körbe:

- Regisztrációs adatbázis – minden esetben
- Indítófájlok, rendszerfájlok – minden esetben
- A WFP érvényessége alatt lévő rendszerfájlok – minden esetben
- Tanúsítványtár – ha a számítógép Tanúsítványtár kiszolgáló
- Címtár-adatbázis *(Active Directory)* – ha a számítógép tartományvezérlő
- SYSVOL-mappa – ha a számítógép tartományvezérlő
- Klaszter szolgáltatásra vonatkozó adatok – ha a számítógép egy klaszter része
- IIS metadirectory – ha telepítve van

A mentés típusa

Az NTBackup több különböző típusú mentés elvégzésére képes, a következőkben ezekkel fogunk megismerkedni. A különböző típusú mentések közben az NTBackup a mentendő fájlok két tulajdonságát veszi figyelembe. Az egyik természetesen az utolsó módosítás dátuma, a másik pedig egy speciális fájl, illetve mappatulajdonság, az archiválandó attribútum. Az attribútumot minden olyan művelet köteles bekapcsolni, ami a fájl tartalmának módosításával jár (ebből tudja majd az NTBackup, hogy a fájl megváltozott, tehát menteni kell). A sikeres mentés után általában (a mentés típusától függően) az NTBackup törli az attribútumot. A fájlok és mappák tulajdonságlapján az archiválandó attribútum az Advanced *(Speciális)* szakaszban File is ready for archiving *(A fájl archiválásra kész*) néven szerepel.

Az NTBackup program segítségével a következő mentési típusokat használhatjuk:

- **Copy backup** *(Másolat)* – A másolás lementi az összes kijelölt fájlt, de nem jelöli meg a fájlokon a biztonsági mentés elvégzését (vagyis nem törli az archiválandó attribútumot). A másolás akkor lehet hasznos, ha például az ütemezett normál és növekményes biztonsági mentések között egy extra másolatot is szeretnénk készíteni adatainkról, mivel a másolás semmiképpen nem befolyásolja a szokásos mentéseket.
- **Daily Backup** *(Napi mentés)* – a kijelölt fájlok közül csak azokról készít mentést, melyek a mentés futtatásának napján módosultak. A biztonsági mentést az NTBackup nem jelöli a fájlokon (más szóval nem törli az archiválandó attribútumot).
- **Differential Backup** *(Különbségi mentés)* – a különbségi mentés a legutolsó normál vagy növekményes mentés óta létrehozott vagy módosított fájlokról készít biztonsági másolatot. A különbségi mentés nem törli az archiválandó attribútumot. A normál és különbségi biztonsági mentés kombinációjának (például hetente normál, naponta pedig különbségi mentés) használatakor a visszaállításhoz a legutolsó normál és a legutolsó különbségi másolatra lesz szükség.
- **Incremental Backup** *(Növekményes mentés)* – A növekményes mentés a legutolsó normál vagy növekményes biztonsági mentés óta létrehozott vagy módosított fájlokról készít másolatot. A mentés végrehajtását a rendszer megjelöli a fájlokon, vagyis ebben az esetben törlődni fog az archiválandó attribútum. A normál és a növekményes biztonsági mentés kombinációjának használatakor a visszaállításhoz a legutolsó normál és az azóta létrehozott valamennyi növekményes biztonságimásolat-készletre szükség lesz.

- **Normal Backup** *(Normál mentés)* – A normál biztonsági mentés az összes kijelölt fájlt lementi, és törli rajtuk az archiválandó attribútumot. Normál biztonsági másolat esetén valamennyi fájlt egyetlen biztonságimásolat-készlet használatával visszaállíthatjuk. A legelső biztonságimásolat-készlet létrehozásakor általában normál biztonsági másolatot kell készítenünk.

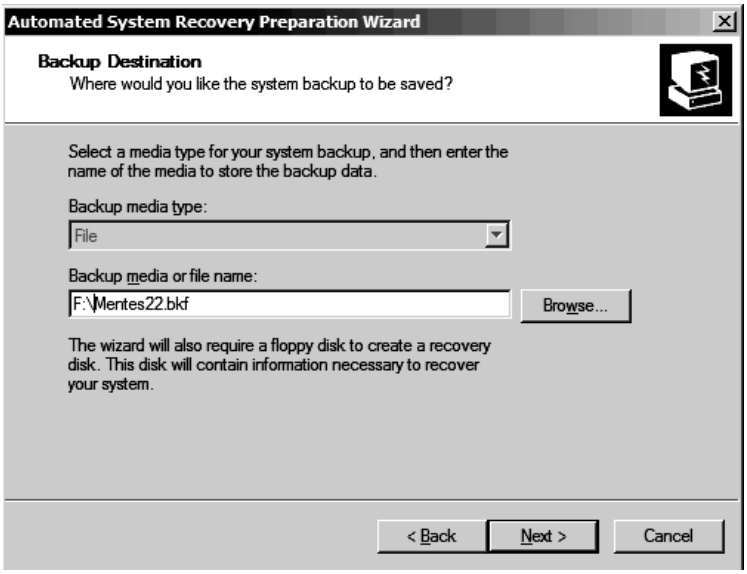
Adataink biztonsági mentéséhez a normál és a növekményes mentés kombinációjának használatával van szükség a legkisebb tárolókapacitásra, és a növekményes mentések végrehajtásához viszonylag kevés idő is elegendő lehet. A fájlok visszaállítása azonban ezzel a módszerrel időigényes és bonyolult lehet, mivel több biztonságimásolat-készletet kell használnunk, amelyek akár több lemezen vagy szalagon is lehetnek. Ha például hétvégén végezzük el a normál mentést (ekkor viszonylag sok idő állhat rendelkezésre), éjszakánként pedig a növekményes mentéseket, akkor egy pénteki visszaállítás esetén szükségünk lesz az előző hétvégén készült normál mentésre és minden azóta készült növekményes mentésre is.

Ha a normál és a különbségi biztonsági mentés kombinációját használjuk, akkor a különbségi mentések több időt vehetnek igénybe (különösen gyakran módosuló adatok esetén), de egyszerűbb lesz az adatok visszaállítása, mivel csak az utolsó normál, és az utolsó különbségi készletre lesz szükségünk.

Automatikus rendszer-helyreállítás

Az Automatikus rendszer-helyreállítás *(Automated System Recovery, ASR)* segítségével egy hajlékonylemezből és egy mentési fájlból álló készletet lehet létrehozni, amelynek segítségével visszaállítható a sérült rendszer mentéskori állapota. Természetesen mielőtt ezt a módszert használnánk érdemes megpróbálkozni más lehetőségekkel is (csökkentett mód, Last Known Good Configuration, Helyreállítási konzol stb.).

Az automatikus rendszer-helyreállítás két részből áll: elsőként a működő rendszeren az NTBackup program Automatikus rendszer-helyreállító varázslójának *(Automated System Recovery Wizard)* segítségével létre kell hoznunk a megfelelő helyreállító készletet. A készlet egyik eleme egy mentési fájl, ami tartalmazza a rendszerállapot adatokat, a rendszerszolgáltatásokat és az operációs rendszerhez tartozó valamennyi kötet adatait. A varázsló a mentési fájl mellé egy hajlékonylemezt is készít, amelyen megtalálhatjuk a biztonsági másolatra és a lemezbeállításokra (alap- és dinamikus kötetek), valamint a visszaállítás menetére vonatkozó információkat.



6.16. ábra: *ASR-készlet létrehozása az NTBackup használatával. Szükség lesz egy floppylemezre is (és nem árt egy floppymeghajtó sem)*

Időzített mentés

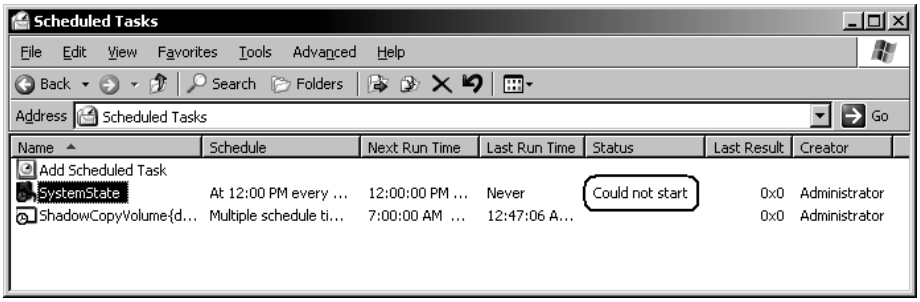
Az NTBackup segítségével összeállított mentési feladatokat végrehajthatjuk közvetlenül a felületről történő indítással, illetve (a mentési beállítások fájlba írása után) a beállítható időzítésnek megfelelő időpontokban automatikusan. A mentések ütemezéséhez az összeállított beállításokat fájlba kell mentenünk, és meg kell adnunk egy felhasználónevet (és jelszót), akinek nevében az ütemezetten induló feladatok futni fognak.

A következő időzítések beállítására van lehetőségünk:

- **Egyszer** *(Once)* – A feladat egyetlen egyszer, a megadott időpontban fog lefutni.
- **Napi** *(Daily)* – A feladat naponta egyszer, a megadott időpontban fog lefutni.
- **Heti** *(Weekly)* – a feladat hetenként ismétlődve a megadott napok megadott időpontjában fog lefutni.
- **Havi** *(Monthly)* – a feladat havonta egyszer, a megadott időpontban fog lefutni.
- **Rendszerindításkor** *(At System Startup)* – A következő rendszerindítás alkalmával.

- **Belépéskor** *(At Logon)* – A következő belépés alkalmával (a mentést időzítő felhasználó belépésről van szó).
- **Üresjárati időben** *(When idle)* – A feladat akkor fog elindulni, amikor a rendszer a megadott idő óta nyugalmi állapotban van.

Az ütemezett feladatok (így a beállított biztonsági mentések) végrehajtásáért a Windows-rendszerek beépített Feladatütemező szolgáltatása *(Task Scheduler)* a felelős. A Control Panel → Scheduled Tasks elemének használatával ellenőrizhetjük mentési feladataink végrehajtásának eredményét, és szükség esetén itt is módosíthatjuk a beállításokat (időzítés, futtató felhasználó stb.).



6.17. ábra: *A mentési feladatok futásának eredményét a Feladatütemezőben nézhetjük meg*

A visszaállítás

A visszaállítás az a lépés, amit soha senki nem szokott előre kipróbálni, éles helyzetben meg úgysem sikerül. Nagyon fontos, hogy a mentési feladatok beállítása után teszteljük a visszaállítást is. A következőkben végigkövetjük a mentésből való helyreállítás lépéseit. Tételezzük fel, hogy az egyik tartományvezérlőnk rendszerlemeze meghibásodott, a gép nem indítható, és semmi esély nincs rá, hogy más módon üzemképessé tehetjük. A gépben lévő második merevlemezen (vagy szalagon, ez tulajdonképpen lényegtelen) van egy előző nap készített normál mentés (d:\mentes\backup.bkf) ezt szeretnénk visszaállítani. Mi a teendő?

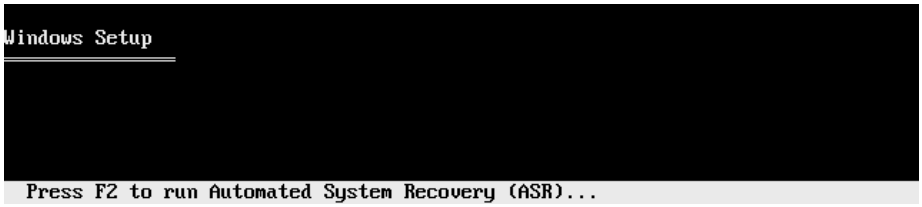
A mentési fájl beolvasásához és a visszaállításához szükségünk van az NTBackup-programra, mégpedig éppen azon a gépen, amelyre a rendszerállapot adatokat vissza szeretnénk állítani. A hibás merevlemez cseréje után tehát telepítenünk kell a gépre egy Windows Server 2003 rendszert, hogy legnagyobb részét azonnal felülírhassuk a korábbi mentésünkkel. A következő lépéseket kell tehát elvégeznünk:

- Telepítünk egy üres Windows Server 2003-at a telepítőlemezről.
- Az új rendszerben elindítjuk az NTBackup-programot, és a mentési fájlból visszatöltjük a rendszerállapot adatokat.
- Végül újratelepítjük a szükséges alkalmazásokat, és megint az NTBackup segítségével visszamásoljuk a mentett adatokat is.

A visszaállítás (csak a megfelelő jogosultság birtokában végezhető el) értelemszerűen felülírja mentésben szereplő fájlokat és mappákat, illetve a rendszerállapot adatokat is. A mentett fájlok és mappák nem csak az eredeti helyükre, hanem bárhová visszaállíthatók, de a rendszerállapot adatok csak az NTBackup programot futtató számítógép aktuális beállításainak helyére kerülhetnek, vagyis mindenképpen felülírják azokat

Visszaállítás ASR-készlet alapján

Az Automatikus rendszer-helyreállítási készletek segítségével történő helyreállítás a Windows telepítőprogramjának futtatása közben érhető el (CD-ről való rendszerindításkor). A telepítési folyamat elején az F2 billentyű lenyomásával indíthatjuk el a helyreállítási folyamatot.



6.18. ábra: *Az automatikus rendszer helyreállítást a telepítőlemezről bootolva indíthatjuk el*

Az ASR a készlet részeként létrehozott hajlékonylemez alapján helyreállítja a számítógép indulásához szükséges lemezek összes kötetét és partícióját, és a Windows néhány másik létfontosságú összetevőjét, majd a mentési fájl alapján visszaállítja a korábban elmentett fájlokat és adatokat. Az ASR visszaállítás tehát a következő műveleteket végzi el:

- Beolvassa a lemezkonfigurációt
- Visszaállítja a bootlemez szignatúrákat, a köteteket és a partíciókat
- Telepíti a Windows lementett verzióját
- Az NTBackup segítségével visszaállítja a rendszerállapotot és a mentett fájlokat

Külső eszközök

A Windows operációs rendszerek beépített hibakereső eszközein kívül számos külső program is rendelkezésünkre áll erre a célra. A következőkben a Sysinternals által jegyzett eszközök közül tekintünk át néhányat, amelyek igen jól használhatók szinte bármilyen hibakeresési feladat során, illetve némelyikkel az operációs rendszer működésének olyan mélységeibe láthatunk bele, ami semmiféle más eszközzel nem lehetséges. Az eszközöket világszerte rengetegen használják, így azok megbízhatóságához és hasznosságához nem férhet kétség.

Sysinternals segédprogramok

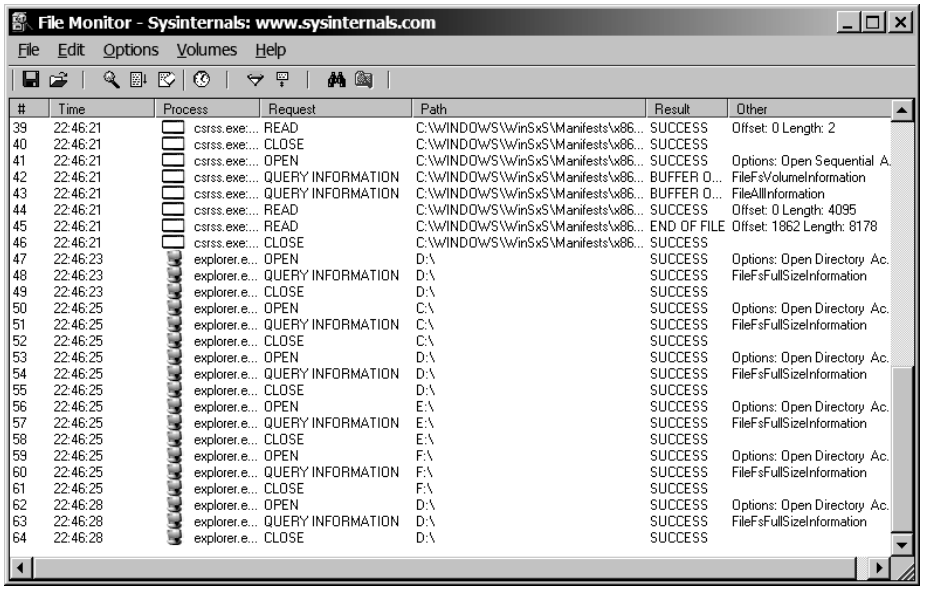
A Sysinternals által készített eszközök tulajdonképpen az operációs rendszer beépített eszközeinek többé-kevésbé (általában inkább többé) felokosított változatai, amelyeknek funkciói és kezelése kifejezetten a rendszergazdák szemléletmódját tükrözi. A Sysinternals cég számtalan ilyen eszközt készített, ezen felül pedig több igen érdekes és fontos könyv (Inside Windows-sorozat), előadás és oktatóanyag fűződik nevükhöz. A vállalatot 2006-ban a Microsoft megvásárolta (a cég alapítói azóta a Microsoft alkalmazásában állnak), de az eszközök továbbra is rendszeresen frissülnek (sőt újak is készülnek), és a http://www.microsoft.com/technet/sysinternals/default.mspx címről valamennyi ingyenesen, bárki számára letölthető.

Valamennyi eszköz futtatásához rendszergazda-jogosultság szükséges (Vista alatt *Run as Administrator)*, viszont telepítésre egyáltalán nincs szükség, a letöltött exe fájl minden további nélkül futtatható. A legfontosabb eszközök egyetlen csomagban is letölthetők a *http://tinyurl.com/ybce37* címről (Sysinternals Suite).

A Sysinternals eszközök
Ebben a screencastban kipróbáljuk a legfontosabb és a legérdekesebb Sysinternals eszközöket.
Fájlnév: II-3-2b-Sysinternals.avi

FileMon (File Monitor)

A FileMon segítségével megfigyelhetjük és naplózhatjuk valamennyi a fájlrendszerrel kapcsolatos műveletet (fájlok megnyitása, olvasás, írás stb.). A valós időben listázott adatok között megtalálhatjuk valamennyi fájlművelet pontos időpontját és típusát, a műveletet kezdeményező folyamat és az érintett fájl nevét, valamint a művelet eredményét is.



#	Time	Process	Request	Path	Result	Other
39	22:46:21	csrss.exe:...	READ	C:\WINDOWS\WinSxS\Manifests\x86...	SUCCESS	Offset: 0 Length: 2
40	22:46:21	csrss.exe:...	CLOSE	C:\WINDOWS\WinSxS\Manifests\x86...	SUCCESS	
41	22:46:21	csrss.exe:...	OPEN	C:\WINDOWS\WinSxS\Manifests\x86...	SUCCESS	Options: Open Sequential A...
42	22:46:21	csrss.exe:...	QUERY INFORMATION	C:\WINDOWS\WinSxS\Manifests\x86...	BUFFER O...	FileFsVolumeInformation
43	22:46:21	csrss.exe:...	QUERY INFORMATION	C:\WINDOWS\WinSxS\Manifests\x86...	BUFFER O...	FileAllInformation
44	22:46:21	csrss.exe:...	READ	C:\WINDOWS\WinSxS\Manifests\x86...	SUCCESS	Offset: 0 Length: 4095
45	22:46:21	csrss.exe:...	READ	C:\WINDOWS\WinSxS\Manifests\x86...	END OF FILE	Offset: 1862 Length: 8178
46	22:46:21	csrss.exe:...	CLOSE	C:\WINDOWS\WinSxS\Manifests\x86...	SUCCESS	
47	22:46:23	explorer.e...	OPEN	D:\	SUCCESS	Options: Open Directory Ac...
48	22:46:23	explorer.e...	QUERY INFORMATION	D:\	SUCCESS	FileFsFullSizeInformation
49	22:46:23	explorer.e...	CLOSE	D:\	SUCCESS	
50	22:46:25	explorer.e...	OPEN	C:\	SUCCESS	Options: Open Directory Ac...
51	22:46:25	explorer.e...	QUERY INFORMATION	C:\	SUCCESS	FileFsFullSizeInformation
52	22:46:25	explorer.e...	CLOSE	C:\	SUCCESS	
53	22:46:25	explorer.e...	OPEN	D:\	SUCCESS	Options: Open Directory Ac...
54	22:46:25	explorer.e...	QUERY INFORMATION	D:\	SUCCESS	FileFsFullSizeInformation
55	22:46:25	explorer.e...	CLOSE	D:\	SUCCESS	
56	22:46:25	explorer.e...	OPEN	E:\	SUCCESS	Options: Open Directory Ac...
57	22:46:25	explorer.e...	QUERY INFORMATION	E:\	SUCCESS	FileFsFullSizeInformation
58	22:46:25	explorer.e...	CLOSE	E:\	SUCCESS	
59	22:46:25	explorer.e...	OPEN	F:\	SUCCESS	Options: Open Directory Ac...
60	22:46:25	explorer.e...	QUERY INFORMATION	F:\	SUCCESS	FileFsFullSizeInformation
61	22:46:25	explorer.e...	CLOSE	F:\	SUCCESS	
62	22:46:28	explorer.e...	OPEN	D:\	SUCCESS	Options: Open Directory Ac...
63	22:46:28	explorer.e...	QUERY INFORMATION	D:\	SUCCESS	FileFsFullSizeInformation
64	22:46:28	explorer.e...	CLOSE	D:\	SUCCESS	

6.19. ábra: *Valamennyi fájlműveletet megfigyelhetjük a FileMon segítségével*

A FileMon kiválóan felhasználható a rendszer működésnek megfigyelésére (eléggé megdöbbentő mennyiségű fájlművelet történik egy érintetlen, semmi különöset nem csináló rendszerben is, nem beszélve mondjuk egy Word, vagy Outlook indításáról…), de talán a legfontosabb felhasználási területe a fájlrendszerbeli jogosultsághiányok „kimérése”.

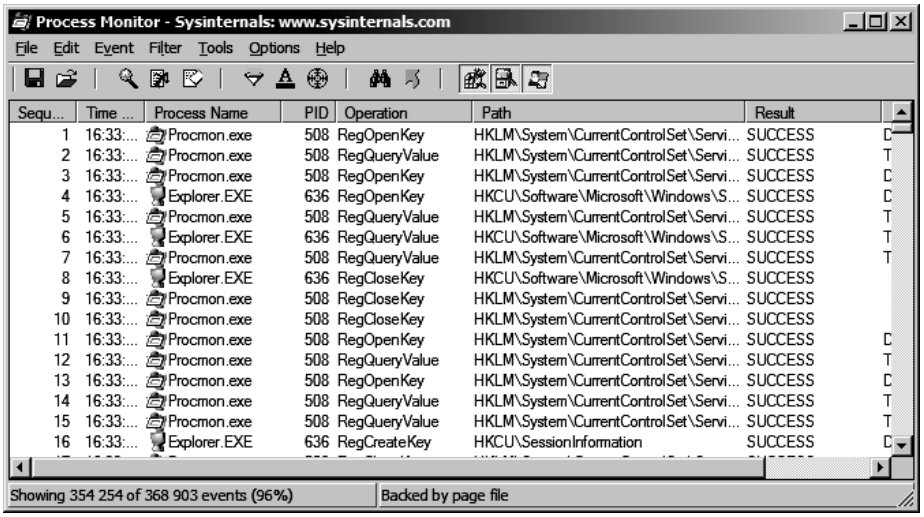
Ha egy rosszul megírt felhasználói alkalmazás nem hajlandó felhasználói jogosultságokkal elindulni, akkor a FileMon segítségével könnyen megtalálhatjuk a sikertelen műveletben szereplő fájlt vagy mappát, és így csak arra az egy elemre kell megadnunk a program futásához szükséges jogosultságot. A listába kerülő adatokat szűrhetjük például a műveletet kezdeményező folyamat neve szerint, és lehetőség van részletes keresésre és fájlba mentésre is.

RegMon (Registry Monitor)

A Regmon a registry-műveletek megfigyelésére használható, működése és felülete is erősen hasonlít a FileMon-ra. Hasonló a felhasználási terület is; megtudhatjuk, hogy a hibát generáló alkalmazás pontosan milyen registry-érték olvasása vagy írása közben adta meg magát (például egy hiányzó kulcs, vagy jogosultsághiány miatt), és így könnyen megoldhatjuk a problémát.

A FileMon és a RegMon helyét a Process Monitor vette át, ami viszont csak Windows 2000 SP4, Windows XP SP2, Windows Server 2003 SP1, és Windows Vista rendszereken futtatható. A régebbi rendszerek támogatása miatt azonban megmaradt az önálló FileMon és RegMon is (ezek még a Windows 9x rendszereken is elindulnak).

Process Monitor



Sequ...	Time ...	Process Name	PID	Operation	Path	Result
1	16:33:...	Procmon.exe	508	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS
2	16:33:...	Procmon.exe	508	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS
3	16:33:...	Procmon.exe	508	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS
4	16:33:...	Explorer.EXE	636	RegOpenKey	HKCU\Software\Microsoft\Windows\S...	SUCCESS
5	16:33:...	Procmon.exe	508	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS
6	16:33:...	Explorer.EXE	636	RegQueryValue	HKCU\Software\Microsoft\Windows\S...	SUCCESS
7	16:33:...	Procmon.exe	508	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS
8	16:33:...	Explorer.EXE	636	RegCloseKey	HKCU\Software\Microsoft\Windows\S...	SUCCESS
9	16:33:...	Procmon.exe	508	RegCloseKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS
10	16:33:...	Procmon.exe	508	RegCloseKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS
11	16:33:...	Procmon.exe	508	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS
12	16:33:...	Procmon.exe	508	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS
13	16:33:...	Procmon.exe	508	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS
14	16:33:...	Procmon.exe	508	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS
15	16:33:...	Procmon.exe	508	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS
16	16:33:...	Explorer.EXE	636	RegCreateKey	HKCU\SessionInformation	SUCCESS

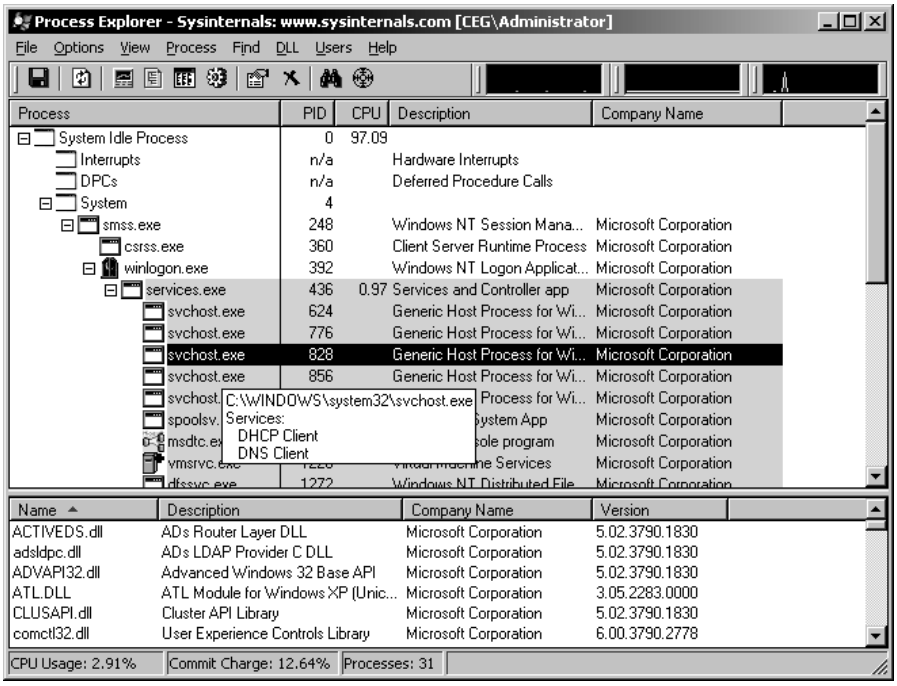
6.20. ábra: *A Process Monitor a fájlrendszer és registry mellett a folyamatok és programszálak monitorozására is képes*

A Process Monitor egy összetett rendszermonitorozó eszköz, amely képes a fájl- és registryműveletek, valamint a folyamatok és szálak valós idejű megfigyelésére (külön-külön és párhuzamosan is). Az eszköz egyben valósítja meg a FileMon és a RegMon képességeit, és számos új lehetőséget is nyújt.

DiskMon (Disk Monitor)

A DiskMon a lemezműveletek közvetlen megfigyelésére ad lehetőséget. Segítségével nyomon követhetjük, és fájlba menthetjük a lemezműveletekre vonatkozó különböző adatokat (időpont, időtartam, művelet fajtája, érintett szektor sorszáma stb.). A DiskMon elhelyezhető a tálcán is, ekkor zöld színnel jelzi az olvasási, pirossal pedig az írási műveleteket.

Process Explorer



6.21. ábra: *Process Explorer, a szuperokos Task Manager*

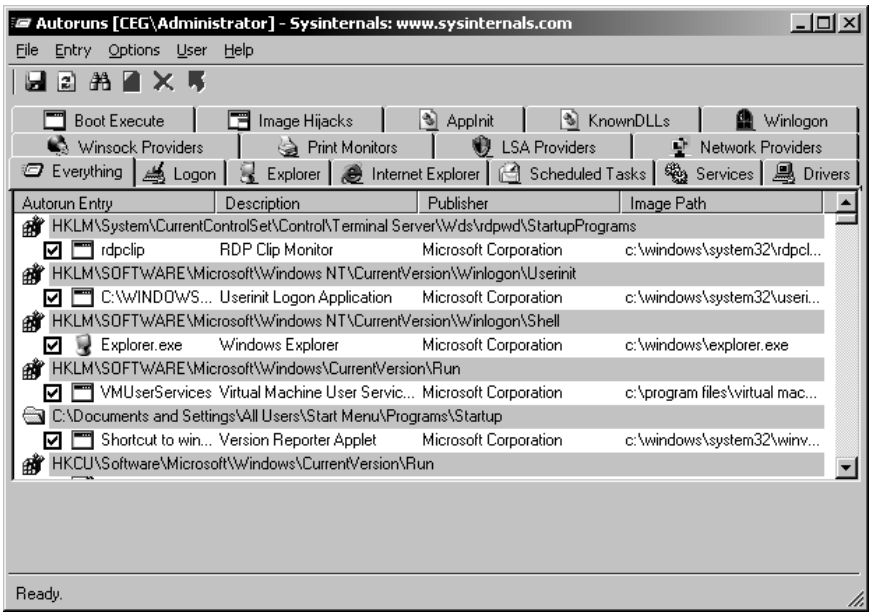
A Process Explorer képes a számítógépen futó folyamatok szinte minden tulajdonságának megjelenítésre. Funkcióinak egy része megtalálható a Feladatkezelőben is, de segítségével rengeteg olyan információhoz is hozzájuthatunk, amelyek megjelenítésére a Feladatkezelő nem képes.

A folyamatok a szülő-gyermek kapcsolatoknak megfelelő fastruktúrában jelennek meg, és valamennyi folyamathoz megjeleníthetjük a használt rendszererőforrások és a nyitva tartott dll-ek listáját is. A Process Explorer igen kifinomult keresési lehetőségekkel rendelkezik, így pillanatok alatt megtalálhatjuk például azt a rendszerfolyamatot, amelyik egy adott erőforrást vagy dll-t megnyitva tart.

AutoRuns

Az AutoRuns segédprogram megkeresi és megjeleníti a rendszerindításkor automatikusan induló valamennyi programot, szolgáltatást stb., vagyis mindent, amit az operációs rendszer automatikusan elindít. A listába kerülnek az indítópultban és a különféle registrykulcsokban *(Run, RunOnce* stb.) szereplő bejegyzések, az Explorer shellbővítmények, a betöltődő eszköztárak és még sok minden más is.

A programhoz tartozik egy parancssori felülettel rendelkező eszköz is *(AutoRunsc.exe),* amellyel lehetőségünk van a kimenet *csv* fájlba való elmentésére is.

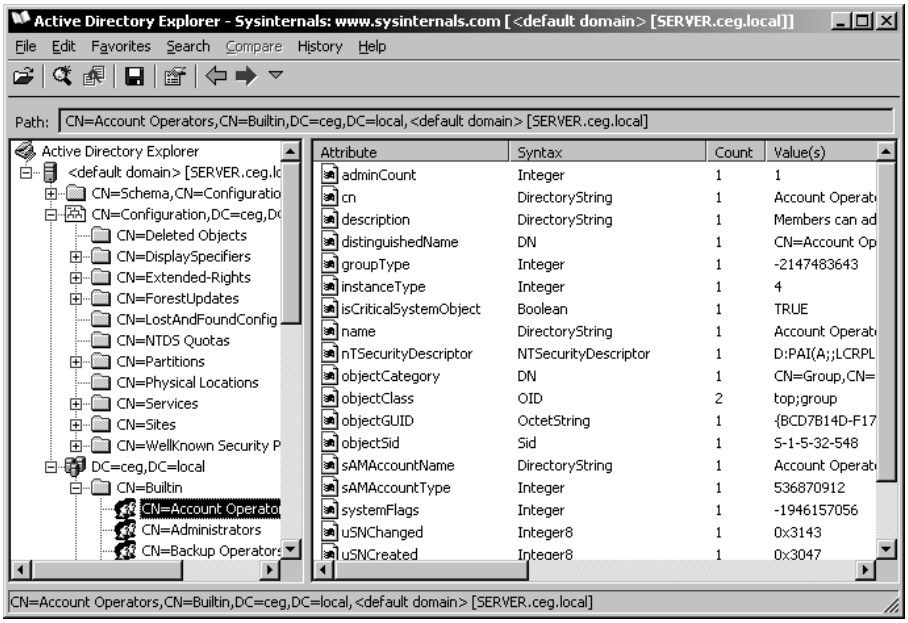


6.22. ábra: *Minden (de tényleg), ami elindul rendszerünkben*

AD Explorer

Az AD Explorer képes a címtáradatbázis nyers formájának megjelenítésére, segítségével elérhetjük valamennyi címtárpartíciót és megjeleníthetjük, illetve szerkeszthetjük az egyes objektumokhoz tartozó tulajdonságértékeket. Az ADExplorer nagyon kifinomult keresési lehetőségekkel rendelkezik, és lehetőségünk van a keresések elmentésére és későbbi újrafelhasználására is.

Teljesen egyedülálló lehetőség az, hogy offline megjelenítésre és összehasonlításra alkalmas pillanatképeket készíthetünk az Active Directory adatbázisról. A mentett adatbázis bármikor újra felcsatolható, vagyis az „élő" adatbázissal megegyező módon jeleníthető meg. A különböző időpontokban készült pillanatképek összehasonlításával azonosíthatjuk a megváltozott objektumokat, tulajdonságokat és jogosultági listákat.



6.23. ábra: *Active Directory-objektumok tulajdonságai az AD Explorerben*

AD Restore

Az ADRestore a törölt címtárobjektumok megkeresésére és visszaállítására képes. A program használata nagyon egyszerű, a címtár online állapotában indíthatjuk el és paraméterként (nem kötelező) csak a törölt objektumok között válogató szűrőt kell megadnunk.

PsTools — csomag a csomagon belül

A PSTools apró parancssori programokból álló gyűjtemény. A programok segítségével egyszerű műveleteket végezhetünk el, viszont érdekes lehetőség, hogy valamennyi parancs távoli gépre is használható.

A PSTools a következő elemekből áll:

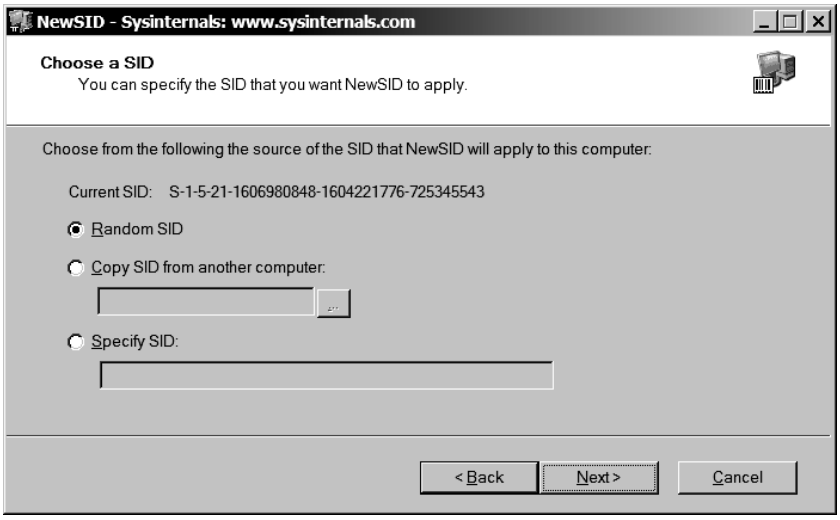
- **PsExec** – segítségével megadott nevű folyamatot indíthatjuk el (távoli gépen is).
- **PsFile** – a parancs a megnyitott fájlok listáját jeleníti meg.
- **PsGetSid** – a számítógép, illetve felhasználó biztonsági azonosítóját *(Security Identifier, SID)* írja ki.
- **PsInfo** – a program listázza az alapvető rendszerinformációkat.
- **PsKill** – a parancs segítségével lehetőségünk van a számítógépen (távoli gépeken is) futó folyamatok „könyörtelen” lezárására.

- **PsList** – a futó folyamatok listáját és az egyes folyamatok legfontosabb adatait jeleníti meg.
- **PsLoggedOn** – a parancs a számítógépre bejelentkezett felhasználókat listázza (a helyi bejelentkezéseket és a megosztott erőforrásokra vonatkozó kapcsolatokat is).
- **PsLogList** – a parancs az Eseménynapló bejegyzéseit listázza.
- **PsPasswd** – a parancs segítségével megváltoztathatjuk a felhasználói fiókokhoz tartozó jelszavakat.
- **PsService** – a parancs segítségével kilistázhatjuk a szolgáltatásokat, és elvégezhetjük a kezelésükkel kapcsolatos legfontosabb műveleteket.
- **PsShutdown** – a parancs használatával leállíthatjuk, illetve újraindíthatjuk a számítógépet (távolról is).
- **PsSuspend** – a parancs segítségével felfüggeszthetjük, illetve újraindíthatjuk a megadott szolgáltatást.

TCPView

A TCPView segítségével a TCP és UDP végpontok listáját jeleníthetjük meg. A program felületéről leolvasható az adott kapcsolathoz tartozó folyamat neve, a helyi és a távoli port száma, és a kapcsolódás állapota is. A program parancssori változatban is használható, ennek neve tcpvcon.exe.

NewSID



6.24. ábra: *A NewSID segítségével grafikus felületen változtathatjuk meg a biztonsági azonosítót*

A NewSID-program segítségével a számítógép egyedi biztonsági azonosítóját *(Security Identifier, SID)* változtathatjuk meg. A SID megváltoztatására a lemezkép alapú klónozás segítségével telepített számítógépek esetén van szükség, mivel a hálózati működés során különféle problémákat okozhat az egyforma biztonsági azonosítók használata.

BGInfo

Bár nem kapcsolódik szorosan a hibakereséshez, mindenképpen figyelmet érdemel ez az egyszerű, de nagyon ötletes program. A BGInfo segítségével egyszerűen az Asztal háttérképét állíthatjuk be, de olyan módon, hogy a képen megjelenjenek a számítógép különféle adatai (neve, IP-címe, operációs rendszere stb.). Ha a programot az Indítópultból, vagy logon szkriptből minden bejelentkezéskor lefuttatjuk, akkor a háttérkép mindig az éppen aktuális adatokat fogja tartalmazni. A program az automatikus indítás esetén sem marad a memóriában, csak elkészíti az aktuális háttérképet, és már véget is ér, vagyis biztosan nem foglalja a rendszer erőforrásait, és nem okoz semmiféle problémát a rendszer működésében.