Holczer József:

A Windows 2000 Server *üzemeltetése*

• Fejezet a *Benkovics-Holczer: Windows 2000 hálózatok adminisztrálása és Internet szolgáltatásai* c. előkészületben lévő könyvből.

• A könyv megrendelhető a kiadónál: Jedlik Oktatási Stúdió Bt (1212 Budapest, Táncsics M. u. 92), Tel/fax: 276-5335. Internet: www.jos.hu, E-mail: jos@jos.hu

Tartalomjegyzék

Miért építsünk hálózatot?

A helyi hálózat kialakításának számtalan előnye van, ezeket a következő szempontok szerint szokták csoportosítani.

Erőforrás-megosztás

A winchester, CD, nyomtató, és a modem megosztása. Nem kell a nagyméretű telepítő anyagok vagy multimédiás anyagok eléréséhez minden gépbe CD-ROM olvasó, illetve nagyméretű winchester. Nem szükséges az összes géphez nyomtatót, illetve modemet kapcsolni, vagy a felhasználót arra kényszeríteni, hogy a nyomtatandó fájljait floppyn vigye a nyomtatóvezérlő géphez.

Alkalmazás-kiszolgálás

Ebbe a körbe tartoznak a kliens-szerver alkalmazások, és az Internet szerverek. Az alkalmazás-kiszolgálás lényegét az adatbázis-kezelés példáján érthetjük meg legegyszerűbben, azaz tegyük fel, hogy keresünk egy rekordot egy szokványos adatbázisban (aminek mérete több 10 vagy 100 megabájt is lehet).

Csupán az erőforrás-megosztás lehetőségét kihasználva, azaz a gépünkön fut az adatbázis-kezelő program, s a szerver tárolja az adatbázist, ha kérésünkkel az adatbázist tároló géphez fordulunk, akkor az adatbázisnak át kell jutnia a saját gépünkre, hiszen az adatok feldolgozását a mi gépünk végzi. Tehát elég erős hardverrel kell rendelkeznünk a feladat megoldásához és a hálózatot is meg kell terhelnünk az adatbázis mozgatásával.

Alkalmazás-kiszolgálás esetén a szerver nemcsak az adatbázist, hanem az azt kezelő szoftvert is tartalmazza, így gépünkről elmegy a kérdés a szerverhez, azon a szoftver értelmezi a kérdést és csak a választ képező rekordok fognak a hálózaton mozogni. Ebben az esetben tehát a mi gépünk teljesítményének nem kell az adatbázis méretéhez igazodni és a hálózati forgalom is sokkal kisebb lesz.

Központi rendszerfelügyelet

Távolról telepíthetünk szoftvereket, módosíthatjuk más gépek beállításait, figyelhetjük a gépek viselkedését a hibakereséshez, központilag írhatunk elő házirendet a hálózatunkon és a rutinfeladatok egy része automatizálható.

Kérdések

1. *Soroljuk fel hálózatunkban kihasznált vagy kihasználható lehetőségeket!*
2. *Milyen hátrányai vannak a hálózatépítésnek?*

A hálózat és a Windows

A számítógépek összekapcsolására a következő lehetőségeink adódnak.

Két gép összekötése soros vagy párhuzamos porton keresztül

A hálózat előnye, hogy csak a megfelelő kábel kell hozzá, hátrány: lassú és csak két gép köthető össze. (Mindkét megoldás elmarad hálózati kártya teljesítménytől.)

Peer to peer hálózat

A peer to peer hálózat egyenrangú gépek kapcsolata. Ezt a hálózattípust legfeljebb 5-10 gép esetén célszerű választani. Ekkor már hálózati kártya is szükséges. Ezt a lehetőséget a *Windows for Workgroups* megjelenésétől kezdve használhatjuk a Windows verziók körében.

Peer to peer hálózat esetén minden gép kiszolgálóként is üzemel, de az adatvédelmi lehetőségek korlátozottak. Az egyes gépek megoszthatják erőforrásaikat (meghajtó, mappa, nyomtató stb.) a többi gép részére, a többi gép csak a megosztott objektumokat látja. A megosztáshoz rendelhető jogosultságok a következők:

Windows 9x

Amikor megosztunk egy mappát, külön adhatunk meg jelszót az olvasáshoz, illetve a teljes eléréshez, de ez minden felhasználóra vonatkozni fog, aki látja[1] a gépünket.

Jogosultságok: Csak olvasásra, teljes, jelszófüggő.

Windows 2000 (és Windows NT 4)

A megosztásokhoz való hozzáférést akár felhasználónként is megadhatjuk, de peer to peer hálózatban minden gépre egyesével kell felvinni a felhasználókat, akiknek engedélyezzük az adott gép elérését. Tehát itt minden gépnek saját felhasználói adatbázisa van, míg kliens-szerver hálózat esetén központi adatbázissal dolgozunk.

Jogosultságok FAT fájlrendszer esetén: Nincs, olvasás, módosítás, teljes.

NTFS fájlrendszer használata esetén finomabban szabályozhatjuk a hozzáféréseket.

[1] Azok a gépek látják egymást, amelyeknél a hálózat tulajdonságainál azonos munkacsoport van megadva.

Tekintsük át röviden, hogyan oszthatunk meg egy mappát[2]. A kiválasztott mappára kattintsunk a jobb egérgombbal. A megjelenő menü *Megosztás* pontjára lesz szükségünk (vagy a *Tulajdonságlap Megosztás* fülére). Jelöljük ki *A megosztva az alábbi néven* választókapcsolót és adjunk nevet a megosztásnak vagy fogadjuk el a javasolt nevet. Az *Engedélyek* nevű gomb alatt állíthatjuk be a megosztáshoz rendelhető jogosultságokat. A létrehozott megosztás már elérhető a hálózat más gépeiről is. A megosztás eléréséhez válasszuk a *Hálózati meghajtó csatlakoztatása* pontot az intéző *Eszközök* menüjéből. Válasszunk egy szabad betűjelet és az elérési úthoz írjuk következőt:

\\<gépnév>\<megosztásnév> Az elérési útnak ezt a formáját használhatjuk csatlakoztatás nélkül is például fájl megnyitásakor.

Kliens-szerver hálózat

Ebben az esetben már nem egyenrangúak a gépek. A gépek egyik csoportja a hálózat felügyeletét, kiszolgálását látja el: ezek a *szerverek.* A gépek másik csoportján pedig a felhasználók dolgoznak: ezek a gépek pedig a *munkaállomások* és a kliensek.

A Microsoft operációs rendszerek csoportosítása

A Microsoft operációs rendszereit az alábbi három csoportba sorolhatjuk.

Kliensek: MS-DOS (és az erre épülő Windows 3.x), Windows 95/98. Elsősorban helyi funkciókat látnak el. Pl. az MS-DOS-ban alapértelmezésként nincsenek meg a hálózati működéshez szükséges komponensek. Egyszerűbb hardverrel is működnek, nagyfokú a hardver kompatibilitás. A fájlrendszerben nincs adatvédelem. Windows 9x esetén a név-jelszó páros csak a munkakörnyezet beállításainak kiválasztására szolgál, ráadásul az ESC gomb megnyomásával megkerülhető.

Munkaállomások: Windows 2000 Professional és Windows NT Workstation. Stabilabb működés (32-bites az operációs rendszer), lehetőség van a felhasználói adatok védelmére. A hardver kompatibilitás kisebb.

Serverek: Windows 2000 Server és Windows NT Server. Stabil működés. Védi a felhasználó adatait. A hardver kompatibilitás kisebb, mivel egy bizonytalan működésű hardvereszköz az egész hálózat működését megbéníthatja.

A kábelezés a helyi hálózatok szintjén

Az említett három gépkapcsolódási lehetőségből helyi hálózatnak csak a peer to peer hálózatot és a kliens-szerver hálózatot tekintjük. A helyi hálózatok

[2] A későbbiekben részletesebben is olvashatunk a megosztásokról és a fájlrendszerekről.

fizikai megvalósításához minden gépbe kell hálózati kártya és valamilyen kábel a gépek összekötéséhez. Szükség lehet még egyéb segédeszközökre is (jelerősítő, HUB).

A kábelezésre két lehetőség terjedt el:

Koaxiális kábel. Kevéssé érzékeny a zavarokra, átviteli sebessége 10 Mbit/s.

UTP kábel. 4 érpár fut a kábelben; 10-100 Mbit/s átviteli sebességet tud; a vezeték olcsó, de a szükséges HUB miatt lesz drágább a megoldás.

Koaxiális kábel esetén a szokásos sín topológia miatt viszonylag kevés kábel szükséges, de bármely kábelhiba az egész szegmens leállását eredményezi. Az UTP kábelnél szokásos csillag topológia eléggé sok kábelt igényel, feltétlenül kell HUB is (kettőnél több géphez), de a kábelhiba csak egy[3] gép kiesését eredményezi.

Feladatok

3. *Családi géppark*

Egy családban két számítógépet, egy szkennert, egy nyomtatót és egy külső modemet találunk. A gyerekek szeretnének egymás ellen is játszani. Soros vagy párhuzamos porton át kössük össze a gépeket? Esetleg szerencsésebb lenne a koaxiális kábel vagy az UTP kábel használata?

4. *Családi hálózat*

Ha az előző feladat megoldásaként hálózat kiépítése mellett döntünk, akkor szerver–kliens, vagy peer to peer hálózat a szerencsésebb?

5. *A család operációs rendszerei*

A család egyik gépén csak játszanak a gyerekek. A másik gépen is néha játszanak, de azon komolyabb munka is folyik és a felnőttek is ezen a második gépen szoktak dolgozni. Melyik gépre milyen operációs rendszert javasolhatnánk?

6. *Egy iskolai könyvtár*

Egy iskola megkapta első 3 számítógépét egy nyomtatóval és szkennerrel. Úgy döntöttek, hogy az iskolai könyvtárban helyezik el az eszközöket. Egyedi gépeket helyezzünk el vagy hálózatot építsünk? Mennyiben változik javaslatunk, ha csak egyik gépben van CD olvasó? Ha hálózat mellett döntünk, akkor melyik hálózatfajtát építsük ki? Ha az iskola a könyvtári gépeken felül még 20 db. számítógépet kap, akkor mennyiben változik javaslatunk?

[3] Ha a szerver és a HUB között adódik a kábelhiba, akkor ez természetesen az egész hálózat működését érinti.

A Windows 9x és a Windows 2000 verziók összehasonlítása

A Windows 9x és a Windows 2000 összehasonlítása

	Windows 9x	*Windows 2000*
Processzor	Intel X86.	Intel X86
	Csak egy CPU.	SMP azaz több processzor is lehet.
Biztonság	Minimális	Hitelesítés, titkosítás[4]
16 bites környezet futtatása	Co-operatív, azaz egy lefagyott alkalmazás magával rántja az egész operációs rendszert. Az alkalmazás annyi ideig birtokolja a processzort, ameddig akarja.	Pre-emptív, azaz egy alkalmazás lefagyása nem veszélyezteti az operációs rendszert[5]. Az alkalmazás csak addig birtokolhatja a processzort, amíg az operációs rendszer engedi.

A Windows 2000 Professional és a Server összehasonlítása

	Windows 2000 Professional	*Windows 2000 Server*
Cél	A gépen dolgozó felhasználó gyors kiszolgálása.	A hálózati felhasználók gyors kiszolgálása.
Memóriaigény	Legalább 64 MB (min. 32 MB, max. 4 GB).	Legalább 256 MB[6] (min. 128 MB, max. 4 GB).
Winchester	Min. 1 GB (csak operációs rendszer).	Min. 1 GB (csak operációs rendszer).
Processzor	1-2 (min. Pentium 133 MHz).	1-4 (min. Pentium 133 MHz)[7].

[4] A titkosítás a fájlrendszer szintjén működik, azaz illetéktelen még a más gépbe átrakott winchesterről sem tudja leolvasni az adatokat.

[5] Más 16-bites alkalmazásokat veszélyeztethet.

[6] Egy komponens memóriaigénye úgy értendő, hogy ennyivel kell növelni a szerver aktuális memóriaméretét.

[7] CPU-ból azért érdemesebb erősebbet beszerezni, hiszen a minimum igény csak annyit jelent, hogy az operációs rendszer hajlandó elindulni.

Telefonkapcsolatok	1	256
Fájl- és nyomtatómegosztás	Maximum 10 kapcsolat egyszerre.	A licencek (CAL) számától függ.
FTP, HTTP kapcsolatok	Maximum 10 kapcsolat egyszerre.	Nincs korlátozva.
Hibatűrő lemezkezelés	Nincs.	Van.
Rendszerfelügyelet	Helyi, távoli csak részleges.	Szerverek, munkaállomások központi felügyelete.
Prioritások	Az előtérben futó alkalmazásé a legmagasabb prioritás.	A hálózati szolgáltatásoké a legmagasabb prioritás.
DNS, DHCP, WINS kiszolgálók, Index Server	Nincs.	Van.
Macintosh szolgáltatások	Nincs.	Van.
Netware szolgáltatások	Nincs.	Külön termékkel van.

Feladatok

7. *Biztonság*

Egy kis cég hálózata egy szerverből és 30 db Windows 98-as gépből áll. Annak ellenére, hogy a Windows 98 alatt nincs adatvédelem a gépek mégsem „engednek be" a helyes név – jelszó páros nélkül. Mi lehet a látszólagos ellentmondás oka?

8. *Webszerkesztés*

Vegyünk egy hálózatot, ahol nem üzemeltetnek webszervert. Ha egyik felhasználó elkészít egy oldalt, akkor azt más felhasználók más gépekről megnézhetik-e böngészőjükkel?

A Windows 2000 tartomány működése és részei

Az Active Directory

A Windows 2000 hálózat alapja az *Active Directory(címtár)*. Az Active Directory tartja nyilván a hálózat különböző objektumait (felhasználók, csoportok, számítógépek, szervezeti egységek stb.). A *címtár* teszi lehetővé, hogy az egyes objektumokat változatos szempontok alapján kereshessék meg a felhasználók. Például a címtártól megkérdezheti a felhasználó, hogy hol talál az irodája közelében egy színes tintasugaras nyomtatót.

A Windows 2000 hálózatban a *tartományvezérlők* (DC, Domain Controller) egyenrangúak. A Windows NT hálózatban még megkülönböztettünk *PDC* (Primary Domain Controller) és *BDC* (Backup Domain Controller) szervereket. Az *SAS* (Stand Alone Server) nem tartományi tag, míg a Member Server tartmányi tag, de nem tartományvezérlő.

A Windows 2000 esetén minden tartományvezérlőnek írható címtára van, míg Windows NT-ben a BDC-nek csak olvasható az adatbázisa. Windows 2000 használatakor tetszőleges tartományvezérlőn módosíthatunk az adatokon és ez a többszörözés (replicatio - replikáció) útján jut el a többi tartományvezérlőhöz. Ez a többközpontú (multimaster) többszörözés jól hasznosítható a mindennapokban, de gondoljunk bele a következő esetbe. Két rendszergazda, két különböző szerveren egyszerre változtatja meg egy adott objektum azonos tulajdonságát! Természetesen a többszörözési rendszer ezen ellentmondások feloldását automatikusan elvégzi, de a rendszergazda a naplózás alapján megoldhatja, hogy utólag az elvetett beállítást nyilvánítsa-e helyesnek.

A fentiek ellenére vannak bizonyos ún. *FSMO* (Flexible Single Master Operation) *szerepek*, amelyeket egyszerre csak egy szerver birtokolhat (bár az tetszőleges lehet és akár szerepenként is eltérhet). Ilyen, például a sémamester és a PDC emulátor. A *sémamester* azt adja meg, hogy a címtárban milyen objektumokhoz milyen tulajdonságokat rendelhetünk. A *PDC emulátornak* pedig fontos szerepe van abban, hogy minden gépnek egyedi azonosítója van a hálózaton. Hibásan megadott név–jelszó párok esetén is a PDC emulátorhoz fordulnak a beléptetést megkísérlő szerverek, mert a PDC emulátor az elsők között értesül a jelszavak megváltozásáról[8].

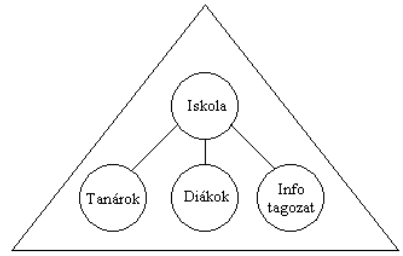
[8] Az öt FSMO szerep: schema master, domain naming master (forestenként egy) illetve PDC emulátor, RID master, Infrastructure master (domainenként egy)

A tartomány üzemmódja

A Windows 2000 szerver alapú tartomány kétféle üzemmódban működhet. Ezek a *natív mód* és a *kevert mód* (mixed mode). Az alapértelmezés a kevert mód. A kevert mód biztosítja, hogy a Windows 2000 szervereink együttműködhessenek a hálózatunkban még esetleg megtalálható Windows NT4 BDC-kkel. A natív mód annyit jelent, hogy tartományvezérlőink kizárólag Windows 2000 szerverek. A kevert móddal válik lehetővé egy NT4 szerver alapú hálózat fokozatos átállítása Windows 2000 alapúra. Ha minden tartományvezérlőt lecseréltünk Windows 2000 tartományvezérlőre, akkor hálózatunkat átállíthatjuk kevert módról natív módra, a visszaállítás azonban nem lehetséges. Természetesen a natív módnak is igen sok előnye van, hiszen ekkor már nem kell figyelni a kisebb tudású NT4 szerverekre, például az NT4 még nem kezeli a címtárat és nem különböztet meg terjesztési és biztonsági csoportot sem.

A szervezeti egységek

A tartomány kezelését jelentősen megkönnyítheti egy jól átgondolt szervezeti egységekből álló hierarchia. *A szervezeti egységekkel* (OU azaz Organizational Units) *a tartomány objektumait (gépek, felhasználók) felügyelet szempontjából egységesen kezelhető csoportokká szervezhetjük.*

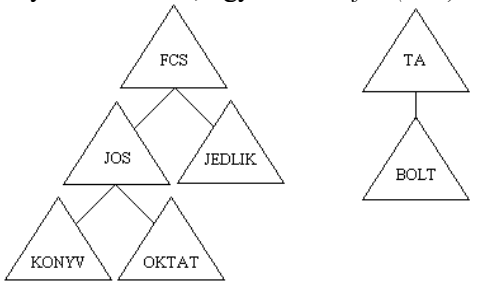


Példánkban a háromszög jelöli egy elképzelt iskola tartományát, a körök pedig a tartományon belüli szervezeti egységeket. Például előírhatjuk, hogy az iskolában egységesen az iskola címere legyen a háttér és minden munkaállomáson megjelenjen az Office 2000 programcsomag. Az info tagozat számára szeretnénk elérhetővé tenni a FrontPage 2000 programot is. Ha egy Windows 2000 Professionalt futtató munkaállomást elhelyezünk egy ilyen szervezeti egységben, akkor a háttér és a megfelelő program automatikusan megjelenik.

A szervezeti egységeken kívül fontos szerep jut a *felhasználói csoportoknak* is. Az egyes erőforrásokhoz a hozzáférési jogosultságokat a csoportok segítségével tudjuk hatékonyan szabályozni. A szervezeti egységekkel nem tudjuk szabályozni a hozzáféréseket, a felhasználói csoportokhoz viszont nem rendelhetünk a felügyelet szempontjából igen fontos házirendeket.

A Windows 2000 szerver alapú hálózat nagyobb egységei

A Windows 2000 szerver alapú hálózat alapegysége az egy címtárat használó tartomány. A tartományokat hierarchiába szervezhetjük. A mellékelt ábrán két ilyen struktúrát, úgynevezett *fát (tree)* láthatunk. Az egyes tartományok



megnevezése Internetes alapokon nyugszik, például az *oktat* nevű tartomány pontos megnevezése: *oktat.jos.fcs* A *jos* nevű tartomány pontos neve pedig: *jos.fcs*[9] A bal oldali fának a gyökere az *fcs* nevű tartomány. Ez az elnevezési módszer megegyezik az Interneten használt tartománynevek rendszerével ezért Active Directory helyes működéséhez feltétlenül szükséges a TCP/IP protokoll és a DNS szolgáltatás. A fa tartományai között úgynevezett *trustkapcsolat* áll fenn, ami annyit jelent, hogy a fa tetszőleges tartományának tetszőleges gépe elé leülhetünk dolgozni. Ha megadjuk a minket nyilvántartó tartomány nevét és ott érvényes jelszavunkat, akkor a hitelesítési kérdéseket a tartományok automatikusan elrendezik. A tartományoknak tehát önálló címtáruk van, de a tartományok kölcsönösen hozzáférnek egymás címtáraihoz.

A fákból kialakítható nagyobb egység az *erdő (forest)*. Akkor szükséges erdő létrehozása, ha olyan tartományokat kell egységbe szerveznünk, amelyek nem használhatnak egyetlen tartománynév-rendszert (pl. két cég egyesülése). Ilyenkor természetesen több gyökér is van. Az ábrán tehát egy Active Directory erdőt látunk, amit két fa alkot és az egyes fák gyökerei az *fcs* és a *ta* tartományok. Ha a fákat erdőbe szerveztük, akkor a fák között is fennáll a trustkapcsolat.

Fontos tudni, hogy csak kevés esetben indokolható megfelelően több tartomány használata. Az egytartományos rendszer kezelése mindig egyszerűbb, ezért egy intézmény felépítését ne tartományokra bontással fejezzük ki, hanem a szervezeti egységek hierarchiájával.

Érdekességként megemlíthető, hogy ha az intézményünk belsőleg használt tartománynév-rendszere illeszkedik az Internen névterébe, akkor a tartományaink elvileg láthatóak az Internetről is. Például az ábra szerinti *bolt.ta* tartomány egy belsőleg használt név, de a *bolt.ta.hu* név használata esetén a tartomány elvileg már az Internet felől is látszik, feltéve, hogy a *ta* domain a hu domain alatt már regisztrálva van. Egy tartomány Internet felől való láthatósága már

[9] A Windows 2000 előtti rendszerek számára is értelmezhető úgynevezett NetBIOS tartománynév. Pl. a jos.fcs tartomány esetén: jos, amit pl. belépéskor kell megadni.

biztonsági kérdéseket is felvet. Javasolt, hogy a külső és a belső tartománynév ne egyezzen meg, tehát mindig pontosan kiderüljön, hogy belső vagy külső erőforrásról van szó. Például iskolánk külső tartományneve mezga.hu a belső pedig röviden mezganet.

A fizikai kábelezés és a tartomány kapcsolata

Legegyszerűbb esetben *egy fizikai hálózat egy tartomány*. Lehetséges azonban *egy fizikai hálózatot több domain*-re (tartományra) szétosztani. Például manapság egy irodaház építésekor már eleve kiépítik a hálózathoz szükséges kábelezést. A beköltöző cégek hálózatai viszont jobb, ha elkülönülnek, ebben az esetben célszerű több tartományt létrehozni az egyetlen fizikai hálózaton.

Több fizikai hálózat is lehet egyetlen tartomány. Például egy iskolának két épületben is van gépterme. Ekkor mindkét terem egy-egy önálló fizikai hálózat, viszont a két termet célszerű egyetlen iskolai tartományként kezelni. Természetesen működhetne ebben az esetben két tartomány is, de ez feleslegesen bonyolítaná a rendszergazda munkáját.

A hálózat számítógépeinek neve

A hálózat számítógépeire nevük megadásával hivatkozhatunk. Ezt a nevet a gépeken a hálózati szolgáltatások telepítésekor kell megadni. Mivel a név az azonosításra szolgál, ezért feltétlenül egyedinek kell lennie a hálózaton. Ha gépünknek pl. a goliat nevet adtuk, a következő módon hivatkozhatunk rá, ha valahol gépnevet szükséges megadni: \\goliat .

A \\goliat\játékok hivatkozás a goliat nevű számítógép jatekok nevű megosztott mappáját jelenti. Ez a hivatkozás az úgynevezett *UNC* (Universal Naming Convention) formában van megadva.

A hálózati protokoll

A gépek kábelek útján össze vannak kötve, egyedi nevük is van, de a sikeres információáramlás érdekében valamilyen közös nyelvet kell „beszélniük”. *Az adatátviteli szabványt protokollnak nevezzük.* Windows környezetben a két legelterjedtebb protokoll a TCP/IP és a NetBEUI. A Windows 2000 estén a TCP/IP az alapértelmezett, mert az Active Directory helyes működéséhez feltétlenül szükséges a TCP/IP protokoll (és a DNS szolgáltatás). A NetBEUI inkább kisebb hálózatokban használatos.

Feladatok

9. *IP címek*
Munkatársunk éppen az iskola újonnan kapott 20 gépének TCP/IP paramétereit tervezgeti. A következő IP címeket szeretné a gépekhez rendelni: 192.168.55.100; 192.168.55.110… Milyen észrevételünk lehetne ezzel kapcsolatban?

10. *Hány gépünk lehet?*
A 255.255.255.0 alhálózati maszk hány gépet enged meg a hálózaton, ha tudjuk, hogy az első és az utolsó cím technikai okok miatt foglalt? A Sulinet keretében osztott 255.255.255.240 maszk hány gépet enged meg?

11. *Az alhálózati maszk*
Vizsgáljuk meg a következő alhálózati maszkokat! Egy fontos szabályt állapíthatunk meg az alhálózati maszkkal kapcsolatban. Mi ez a szabály?
255.255.255.0 ; 255.255.240.0 ; 255.128.0.0 ; 255.255.255.192 (a bináris formát vizsgáljuk!)

A Windows 2000 hálózat felhasználói

A hálózat felhasználói

A tartományba való belépéshez egy felhasználói név és egy hozzá tartozó jelszó megadása szükséges. Üzemeltethetjük ugyan úgy is a hálózatot, hogy megengedjük az üres jelszó használatát, de ez a lehetőség biztonsági okokból nem javasolt. A felhasználói névnek egyedinek kell lennie, természetesen különböző felhasználók adhatnak meg azonos jelszót, mert a felhasználó hitelesítése a név-jelszó párossal együtt történik. A felhasználó precíz megnevezése a tartománynév és a felhasználói név együttes magadásával történik meg. Például: jedlikdomain\farkascs vagy Windows 2000 esetén használhatjuk a „Mézga Géza@belso.suli.hu" formát is. Ez a forma nem e-mail cím és akkor is is használható, ha nem üzemeltetünk levelező kiszolgálót. A tartomány megadására szükségünk is van, ha olyan gépről szeretnénk tartományi erőforrást elérni, amely éppen nem tagja a tartománynak.

Automatikusan létrejövő felhasználók

A hálózat egyik legfontosabb felhasználója a rendszergazda. A *rendszergazdai jogokkal rendelkező felhasználó látja el a hálózat felügyeletét.* Természetesen több rendszergazda is lehet egy hálózaton. Rendszergazda jogosítványokkal gyakorlatilag bármit meg lehet tenni a hálózaton, ilyen jogosítványok szükségesek pl. rendszerfelépítés megváltoztatásához; rendszerkomponensek telepítéséhez; IP paraméterek változtatásához; felhasználók, csoportok kezeléséhez; elfelejtett jelszavak visszaállításához. A rendszergazda át is adhatja az említett feladatok egy részét.

Egy rendszergazdai azonosító már a szerver (munkaállomás) installálásakor létrejön. A létrejött azonosító nyelvtől függően *rendszergazda* vagy *administrator*. Célszerű az alapértelmezett rendszergazda nevet megváltoztatni és létrehozni egy másik rendszergazdai jogokkal rendelkező felhasználót, továbbá javasolt még egy rendszergazdai azonosítót és jelszót biztonságos módon őrizni, amihez vész esetén hozzáférhetünk.

A szerver telepítésekor létrejön még néhány felhasználó. Például *vendég* vagy *guest* néven gép/tartomány vendégként való eléréséhez, de a vendég alapértelmezés szerint tiltott. Létrejön egy felhasználó az Internet kiszolgálóhoz való hozzáférés biztosítására, ez azért kell, mert a szerver csak hitelesített felhasználókat enged hozzáférni a fájlokhoz, mappákhoz. Az egész világnak természetesen nem lehet azonosítója a szerverünkön, ezért az ismeretlen felhasználók ennek a minimális jogokkal rendelkező felhasználónak a nevében tudják nézegetni az oldalakat. Létrejön még néhány csoport a rendszert üzemeltetők számára és a felhasználók számára. Ilyenek pl. a

tartományfelhasználók (Domain Users) amelynek alapértelmezés szerint minden tartományi felhasználó a tagja; a *fiókfelelősök (Account Operators)* csoport tagjai a felhasználói- és a csoportfiókok kezelését végezhetik; a *rendszergazdák (Administrators)* csoport tagjai teljes körű hozzáférést kapnak gyakorlatilag mindenhez.

Feladatok

12. *Irodaház*
Soroljunk fel minél több érvet arra, hogy miért érdemes egy nagy irodaház fizikailag egységes hálózatát domain-ekre bontani! Megfelelő lenne a szervezeti egységek használata a tartományok helyett?

13. *Egy középiskola hálózata*
Vegyünk egy középiskolát, amely gimnáziumi és szakközépiskolai tagozattal is rendelkezik egy épületben. A két tagozatot szeretnénk elkülöníteni a hálózat adminisztrációja szempontjából is. Hogyan alakítsuk ki a hálózatot?

14. *Két szupermarket*
Van két épületünk, kész kábelezéssel és az épületek között jó minőségű hálózati kapcsolattal. Az egyik épületben van mindkét cég üzlete, a másik épületben pedig mindkét cég központja. Hogyan alakítsuk ki a hálózatot?

15. *Marcipán Könyvkiadó*
A cég könyvek kis- és nagykereskedelmével illetve csomagküldéssel is foglalkozik. A céget újonnan felépült épületében találjuk meg teljes egészében. Tegyünk javaslatot a cég hálózatának logikai kialakítására!

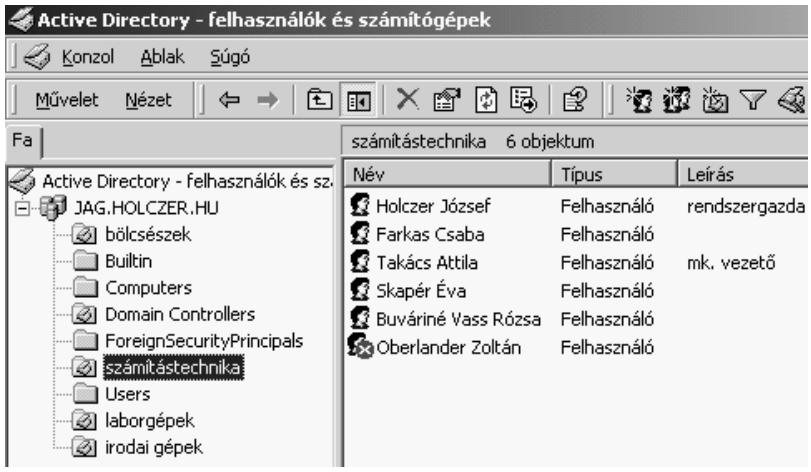
16. *Szervezeti egységek, vagy tartományok?*
Miért jobb, ha egy iskola osztályok szerinti felépítését szervezeti egységekkel valósítjuk meg tartományok használata helyett?

Új felhasználó létrehozása

A felhasználói fiók

A felhasználó létrehozása egy *felhasználói fiók* létrehozását jelenti. A felhasználói fiók mögött egy azonosító, az ún. *SID (Security ID)* áll, akár csoportról, akár egyéni felhasználóról van szó. Ez a felhasználóhoz rendelt egyedi szám (mint egy személyi szám.) és valójában a SID segítségével történik meg a felhasználó jogosultságainak ellenőrzése, ezért lehetséges a felhasználók átnevezése. A SID-et a rendszer adja és annyira egyediek, hogy a törölt felhasználóhoz tartozó SID sem kerül újra kiadásra.

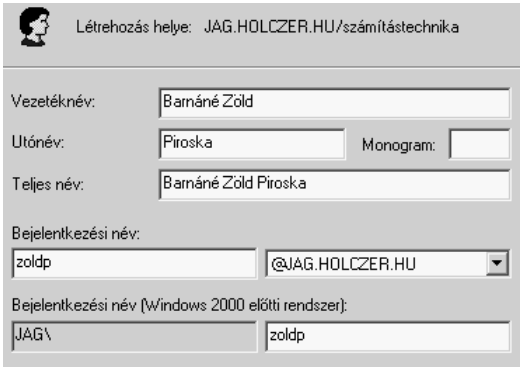
A tartomány felhasználóinak fiókjait létrehozni, és a fiókokat karbantartani a *Start* menü *Programok* menüpontjában a *Felügyeleti eszközök* csoport *Felhasználók és számítógépek* pontjával lehetséges.



Az ábrán a JAG.HOLCZER.HU nevű tartomány felhasználói közül a számítástechnika szervezeti egységbe tartozókat láthatjuk. Az ábrán láthatunk még két szervezeti egységet a felhasználók számára (számítástechnika, bölcsészek) és másik két szervezeti egységet a számítógépek számára (laborgépek, irodai gépek). A gépek és a felhasználók számára alkotott szervezeti egységek egyformán jelennek meg, csak a rendszergazdán múlik, hogy mennyire lesz áttekinthető a felépített rendszer. Láthatunk még néhány automatikusan létrejött tárolót pl. *Domain Controllers*, ami a tartományvezérlőket tartalmazza vagy a *Users* ami az automatikusan létrejövő felhasználókat és felhasználói csoportokat tartalmazza.

Új felhasználó létrehozása

Új felhasználó létrehozásához elsőként válasszuk ki azt a tárolót ahová az új felhasználó kerülni fog. Ha nincs kijelölve egyetlen felhasználó sem, akkor a *Műveletek* menü *Új* csoportjának *Felhasználó* pontját választva megadhatjuk az új felhasználónk alapvető adatait.

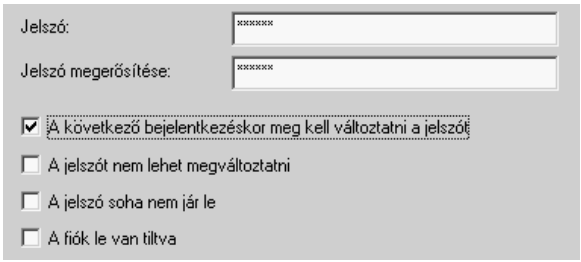


A *Vezetéknév*, *Utónév*, *Monogram* és *Teljes név* közül elegendő egyiket kitölteni a továbbhaladáshoz, de célszerű a vezetéknév és utónév mezők kitöltése (a teljes név ekkor automatikusan kitöltődik). Például az Active Directory-tól kérhetjük a Piroska keresztnevű felhasználók keresését. Elvileg megadhatunk különböző bejelentkezési neveket a Windows 2000 és a megelőző rendszerek számára, de ezt megfontoltan tegyük, hiszen könnyen kaotikus állapotot hozhatunk létre.

A *Bejelentkezési név* megadása kötelező. Ez lesz a felhasználó neve a hálózat számára. Az ábra szerinti felhasználónak a bejelentkezéskor elegendő a név mezőbe annyit írni, hogy „zoldp@jag.holczer.hu" Ha másképp töltenénk ki a panelt, akkor használhatnánk például a „Zöld Piroska@jag.holczer.hu" formát is. A kisbetűk, illetve a nagybetűk között csak a képernyőn van különbség. Néhány karakter tiltott a felhasználói névben. Ezek: „ \ / < >: ; , = + | [ ] * ? szóköz[10]

A tovább gombra kattintva újabb adatokat adhatunk meg.

A *Jelszó* a felhasználó jelszava. A Windows 2000 maximálisan 127 karakterből álló jelszavakat, míg a Windows más változatai legfeljebb 14 karakter hosszú jelszót kezelnek. Az ennél hosszabb jelszavak pl. a Windows 98 alóli bejelentkezéskor problémát okozhatnak. A jelszó minimális hosszúságát a rendszergazda határozhatja meg. Alapértelmezés szerint a jelszó megadása nem kötelező, de ez nagy biztonsági rés lehet a rendszerben. A felhasználói



[10] A Windows 2000 megengedi pl. a ? használatát a bejelentkezési névben, de a megelőző rendszerek egyértelműen tiltják az említett karakterek használatát, így ha lehet ne éljünk a lehetőséggel. A bejelentkezési név hossza a Windows 2000 előtti rendszerek számára maximum 20 karakter lehet.

névtől eltérően a jelszónál már különbség van a kisbetűk és a nagybetűk között. Jelszavunk feltörését nagyon megnehezíthetjük, ha betűket, számokat és szimbólumokat vegyesen alkalmazunk benne. A jelszó se itt se belépéskor nem fog megjelenni, helyette csillagokat fogunk látni. A felhasználó jelszava tehát nem tudható meg, sőt még a hossza sem, mert egy létező felhasználó tulajdonságait megtekintve a jelszó helyén semmit sem látunk.

Jelszó megerősítése: Csak a kétszer azonosan beírt jelszót fogadja el a rendszer, mert így megakadályozható, hogy egy elgépelt jelszó megadásával kizárjuk magunkat a rendszerből.

A következő bejelentkezéskor meg kell változtatni a jelszót: Ha bejelöljük, akkor ez annyit jelent, hogy a belépéskor a jelszó megadása után - ha azt elfogadta a rendszer - csak akkor enged dolgozni, ha megadta a felhasználó az új jelszavát.

A jelszót nem lehet megváltoztatni: A *Vendég* azonosítónál pl. alapértelmezésként be van jelölve, mert ez lényegében egy csoport által közösen használt név-jelszó pár, így megelőzhetjük, hogy egyik csoporttag jelszóváltoztatása megakadályozza a többi csoporttag belépését. Értelemszerűen ez és az előző jelölőnégyzet egyszerre történő kiválasztása hibajelzést fog okozni.

A jelszó soha nem jár le: Biztonsági okokból célszerű a jelszónak lejárati határidőt szabni. Ez a beállítás a jelszó kötelező módosítása beállítással van ellentmondásban és együttes beállítási kísérlet esetén figyelmeztetést kapunk az ellentmondásról és a kötelező jelszómódosítás beállítást érvényteleníti *A jelszó nem jár le* beállítás.

A fiók le van tiltva: Amikor egy felhasználót ideiglenesen ki akarunk tiltani a hálózatból mindig ezt a lehetőséget használjuk. Biztonsági okokból célszerű alkalmazni ezt a lehetőséget, ha például egy kollégánk hosszabb külföldi tanulmányúton vesz részt. A tiltott fiók felhasználója a leveleit sem fogja elérni például weben keresztül.

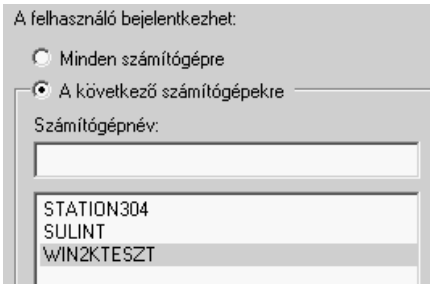
Új felhasználó létrehozásakor csak az előbbi adatok beállítását végezhetjük el, a többi jellemző megadásához a kérdéses felhasználót nyilvántartó tárolót kell felkeresnünk, majd megnyitni a felhasználó tulajdonságlapját. Itt megadható még egy rövid megjegyzés a leírás mezőben, az iroda, a telefonszám, az e-mail cím, a felhasználó weblapjának a címe stb. Az adatok megadása nem kötelező, de hasznos lehet a tartomány minden felhasználójának.

A bejelentkezés idejének és helyének korlátozása

A *Fiók* fülön *A nyitvatartási idő* gomb alatt meghatározhatjuk, hogy a kérdéses felhasználó mikor léphet be, ez a beállítás csak a bejelentkezés idejére vonatkozik. Ha már bejelentkezett a felhasználó és munkája közben jár le a bejelentkezési idő, akkor a felhasználót alapértelmezés szerint nem fogja kiléptetni a rendszer, de ha önszántából kilép, akkor az újabb csatlakozási kísérlet már sikertelen lesz. Lehetőség van a bejelentkezési idő lejártakor a már belépett fel-

használó erőszakos leválasztására is. Ilyenkor felhasználónak megszakadnak a hálózati kapcsolatai. A beállítást a csoportházirendben tehetjük meg. Egy banktisztviselő esetén például a szombat éjféli bejelentkezés biztonsági problémákat vethet fel.

A *Bejelentkezési hely* gomb alatt szabályozhatjuk, hogy mely gépekről jelentkezhet be egy felhasználó.



A fiók beállításai

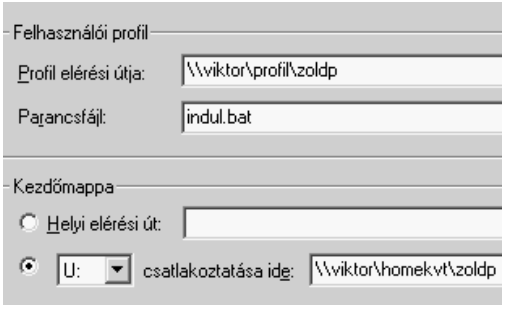
A *Fiók* fül alatt található *A fiók zárolt* jelölőnégyzetet kizárólag a rendszer állíthatja be, mi csak feloldhatjuk ezt, ha rendelkezünk a megfelelő jogosultságokkal. A zárolás bekövetkezhet például 3 hibás jelszó megadása után, ha a csoportházirendnél beállítottuk ezt a lehetőséget.

A fiók lejár szekcióban az ábra szerint a határozhatjuk meg a felhasználó fiókjának érvényességi idejét. A lejáratkor természetesen nem törli a rendszer a felhasználót, de a bejelentkezési kísérletre a felhasználó „A fiók le van tiltva” jelzést kapja. Ilyenkor ne a fiók tiltását próbáljuk feloldani, hanem a lejárat dátumát vizsgáljuk meg először. A fiók érvényességi idejét és a jelszó érvényességi idejét ne keverjük össze, hiszen nem azonos fogalmakról van szó!

A profil beállításai

Az ábra a *Profil* fül beállítási lehetőségeit tartalmazza. *Profilnak nevezzük azokat a fájlokat melyek a felhasználó egyéni beállításait* (asztal, háttér…) *tárolják.*

Profil elérési útja: A profil szerveren való tárolásával elérhető, hogy a felhasználót mindig saját beállításai fogadják bárhonnan is jelentkezik be a tartományba. A profil elérési útját például az ábrán látható módon \\gépnév\megosztásnév formában adhatjuk meg. A felhasználó profilja az első belépéskor fog létrejönni a



felhasználói névvel jelölt mappában.

A *Parancsfájl* a belépési parancsfájl neve, a megadott parancsállományt minden bejelentkezéskor le fogja futtatni a felhasználó gépe, tehát fontos hogy a neve és tartalma értelmezhető legyen a felhasználó gépén futó operációs rendszer számára. Helyét nem kell megadni, mert a kötelező hely a tartományvezérlők esetén a tartomány NETLOGON megosztása. Ennek a mappának a fizikai helye: %SYSTEMROOT% \SYSVOL \SYSVOL \JAG.HOLCZER.HU \SCRIPTS mappa. Itt a %SYSTEMROOT% az operációs rendszer helyét jelöli meg (pl. D:\WINNT). A JAG.HOLCZER.HU helyére természetesen a megfelelő tartománynév értendő.

A kezdőmappa megadása

Kezdőmappa: a felhasználó ún. „home" könyvtára. Ha ezt beállítjuk, akkor valamely háttértáron saját területet adunk a felhasználónak. Az ábra szerinti beállítások mellet automatikusan létre fog jönni a VIKTOR nevű gépen a HOMEKVT nevű megosztásban egy ZOLDP nevű mappa[11]. Ehhez a könyvtárhoz alapértelmezés szerint csak az adott felhasználó és a rendszergazdák férnek hozzá teljes hozzáférés jogosultsággal.

A home könyvtár két helyen lehet

Helyi elérési út: a home könyvtár a helyi meghajtón található. Ezt akkor célszerű választani, ha a felhasználó mindig azonos munkaállomást használ.

Csatlakoztatása ide: a home könyvtár a szerveren található. A home könyvtárat a megadott betűjellel, mint hálózati meghajtót látja a felhasználó. Ez a csatlakoztatás belépéskor automatikusan megtörténik. Win9x-et futtató kliens esetén nem automatikus a hozzárendelés, ezért a belépési parancsfájlban szükség volna még a következő sorra, ha pl. U: meghajtóként szeretnénk viszontlátni a home könyvtárat: NET USE U: \\SERVER\ZOLDP

Csoporttagság

A következő csoportok tagja fül alatt meghatározhatjuk, hogy mely csoportoknak legyen tagja a kérdéses felhasználó. Alapértelmezés szerint minden felhasználó tagja lesz a *Tartományfelhasználók* nevű csoportnak.

A távelérés

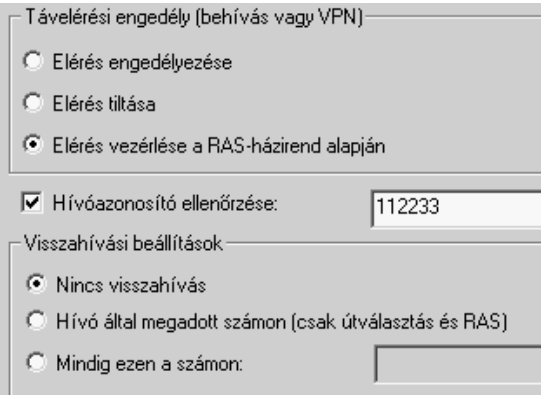
A *Behívás* nevű fülön a felhasználó telefonos hálózatelérését szabályozhatjuk. Természetesen a távelérés előfeltétele, hogy a számítógéphez legyen csatlakoztatva modem, továbbá szükséges a távelérés szolgáltatás beállítása is. Ez

[11] Az ábra szerint beállítva automatikusan létrejön a *zoldp* nevű mappa, de nem lesz megosztva. Az U: meghajtó is csak a Viktor nevű gép *homekvt* megosztása lesz. Másik megoldásként hozzuk létre előre a *zoldp* nevű megosztást, és akkor írhatjuk rövidebben: \\viktor\zoldp.

teszi lehetővé a szerver és egy másik gép telefonon keresztül való kapcsolódását. A szolgáltatás beállítása a *Felügyeleti eszközök* programcsoport *Útválasztás és távelérés* pontjának kiválasztásával történhet meg, a beállítás lépésein egy varázsló vezet végig.

Tartományunk telefonos elérését *engedélyezhetjük*, *tilthatjuk* vagy az úgynevezett *RAS-házirend alapján* szabályozhatjuk.

Egy érdekes lehetőség a *Hívóazonosító ellenőrzése*. Ha ezt bejelöljük, akkor a szerver megkísérli a hívó telefonszám azonosítását, ez csak akkor lehetséges, ha a hívó és a hívott gép között a távközlési eszközök támogatják ezt a szolgáltatást. Ha kiválasztjuk a lehetőséget és sikertelen a hívóazonosítás, akkor a szerver nem engedélyezi a kapcsolatot.



A *Visszahívási beállítások* csoportban beállított állapottól függ, hogy ki viseli a kapcsolat telefonszámláját.

Nincs visszahívás: minden költség a hívót terheli.

Hívó által megadott számon: Ha ezt a lehetőséget választjuk, akkor a felhasználó bejelentkezésekor a szerver kéri a nevet és a jelszót, majd a sikeres azonosítás esetén választhatunk, hogy kérünk visszahívást, vagy sem. Ha igen, akkor meg kell adnunk, hogy mely számon kérünk visszahívást. Ezután a szerver bontja a vonalat és a megadott számon visszahívja a felhasználót.

Mindig ezen a számon: Az előzőtől abban tér el, hogy ezt a számot nem a felhasználó, hanem a rendszergazda állítja be, így a telefonszámot már nem fogja kérni a szerver.

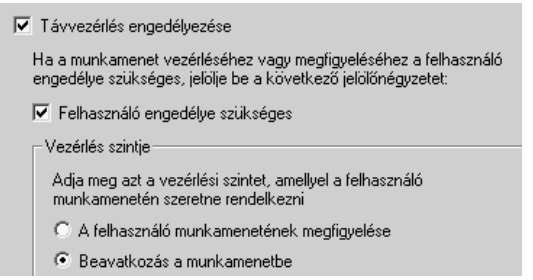
Ha nem kértünk visszahívást, akkor a kapcsolat költségei minket terhelnek, ha kértünk visszahívást, akkor a szerver üzemeltetője viseli a költségeket. A hívó által megadott visszahívás típus szabadabb hálózat elérési lehetőséget biztosít, míg az adott számon történő visszahívás a szerver üzemeltetőjének szempontjából biztonságosabb.

A terminálszolgáltatás

A felhasználók tulajdonságlapjának utolsó négy füle a *terminálszolgáltatás* beállítására vonatkozik. Ennek lényege a következő:

Ha egy kliensgép fizikailag nem képes futtatni a Windows 2000 Professionalt, akkor a Windows 2000 Server felkínálja a következő lehetőséget. Mind az operációs rendszer, mind a hozzá tartozó programok a szerveren futnak, a munkaállomás pedig egyfelől továbbítja a billentyűzet és az egér adatait a

szervernek, másfelől megjeleníti a monitoron a képet. Így akár egy Windows 3.1-est futtató 386-os gépen is működhet a Windows 2000, persze a szolgáltatást igénybe vevő kliensek számától függően a szervernek „erősebbnek” kell lennie. Természetesen a szolgáltatás használatához a kliensen a szolgáltatást telepítenünk kell[12].



A terminál-szolgáltatásnak igen hasznos lehetősége a *távvezérlés*. A felhasználó tulajdonságlapjának *Távvezérlés* nevű fülén az ábra szerinti beállításokat végezhetjük el.

A távvezérlés lényege az, hogy ha a felhasználó elakad a munkájában, akkor a rendszergazda úgy mutathatja meg neki, hogy mit kell tennie, mintha mellette állna, pedig lehet, hogy egy másik országban van. A távvezérlésnél a rendszergazdánál is az elakadt felhasználó képernyője jelenik meg. A rendszergazda által végzett műveletek a felhasználó képernyőjén is megjelennek és természetesen ennek fordítottja is igaz. A felhasználó meg tudja mutatni, hogy mit tett, a rendszergazda pedig meg tudja mutatni, hogy mit kellett volna tenni.

A távvezérlés használatához csupán annyi szükséges, hogy mindketten a terminálszolgáltatások ügyfeleként legyenek bejelentkezve a szerverre. Ez a bejelentkezés lehetséges táveléréssel vagy az Interneten át is.

Fontos tudni, hogy terminálszolgáltatás használata esetén programok telepítése és eltávolítása csak a vezérlőpult Programok telepítése/törlése ikonjának útján lehetséges a szerveren.

A felhasználó törlése

A kijelölt felhasználó vagy felhasználók törölhetők a *Művelet* menü vagy a helyi menü *Törlés* menüpontjával, vagy egyszerűen a *Del* gombbal. A *Ctrl* és a *Shift* billentyűk segítségével a Windows-nál megszokott módon egyszerre több felhasználót is kijelölhetünk a törléshez. A törlés a SID törlését jelenti, tehát az azonos név-jelszó párossal létrehozott új felhasználó sem kapja vissza a törölt azonosító jogosítványait.

[12] Ez úgy történik, hogy a szolgáltatást nyújtó szerver TSCLIENT megosztásából csatlakoztatás vagy lemezek útján a megfelelő kliensprogramot el kell juttatni a szolgáltatást igénylő géphez, és le kell futtatnunk a megfelelő setup.exe programot.

Feladatok

17. *A SID*
Milyen az előnye annak, hogy ugyanazt a SID-et a rendszer még egyszer nem osztja ki?

18. *Távelérés biztonsága*
Milyen biztonsági előnyei vannak, ha a távelérés beállításánál a „Mindig ezen a számon" lehetőséget adjuk meg egy felhasználó, pl. a Rendszergazda esetében? Milyen hátrányai lehetnek ennek a beállításnak?

19. *Távvezérlés*
A távvezérlés Interneten át történő használata meglehetősen lassú lehet. Milyen esetekben éri meg mégis használni?

20. *Hozzunk létre felhasználókat!*
Hozzunk létre a legegyszerűbb módon *Vezér* néven egy rendszergazda jogosítványokkal rendelkező felhasználót! Hogyan korlátozhatjuk a bejelentkezés idejét? A *Vezér* meg tudja kerülni a beállításainkat?

21. *Irodai hálózat*
Egy utazási iroda 10 munkaállomásból és egy szerverből álló hálózatot kapott. Hány rendszergazdát javasolnánk? Az irodavezető rendszergazda legyen-e? Mely gépeken léphessen be az irodavezető és az információ munkatársa? Milyen távelérése legyen a rendszergazdának, az irodavezetőnek és a pénztárkezelési jogokkal rendelkező felhasználóknak?

22. *Iskolai hálózat*
Egy iskolai hálózat felépítése a következő. Egy kimenő ISDN vonal az Internet felé; két bejövő telefonvonal a táveléréshez; két tanteremben 15-15 gép; az öt tanári szobában is találunk 1-1 gépet; az iskola büféjében is van egy számítógépet; az iskolába kb. 500 diák jár. Tegyünk javaslatot a felhasználók létrehozásánál tehető beállításokra!

Felhasználói csoportok

A szervezeti egység és a felhasználói csoport viszonya

A szervezeti egységek csak adminisztratív csoportosítást jelentenek. Segítségükkel meg tudjuk valósítani a felügyelet szétosztását, sőt különböző házirendeket rendelhetünk hozzájuk, azonban nem használhatók a jogosultságok beállítására. A jogosultsági beállítások továbbra is a felhasználókhoz, a csoportokhoz és a számítógépekhez kötődnek.

A *csoportok* egyrészt jogosultsági beállítások szempontjából foglalják egységbe a felhasználók egy-egy részét másrészt az elektronikus levelezés szempontjából terjesztési listaként is működnek. A terjesztési lista funkció akár önállóan is működhet.

A felhasználók csoportokba sorolása megkönnyíti a felhasználók jogainak beállítását és karbantartását. Egy csoportra beállított jog rögtön érvényesül a csoport tagjaira is. Ha egy csoportnak beállítottuk a jogosultságait, akkor elegendő a felhasználót behelyezni a csoportba és ő is rögtön rendelkezni fog a megfelelő jogosultságokkal. A felhasználók csoportokba sorolása nem kötelező, ám alkalmazása egyszerűsíti és áttekinthetővé teszi a rendszergazda munkáját.

Minden létrehozott felhasználó automatikusan tagja lesz a *Tartományfelhasználók* csoportnak.

A felhasználói csoportok osztályozása

Típus alapján kétféle, hatókör alapján háromféle csoportot különböztetünk meg.

A csoportok osztályozása típus alapján:

Biztonsági csoport. Ezeket a csoportokat jogosultságok osztásához használjuk, de akár e-mail terjesztési listaként is használhatóak.

Terjesztési csoport. Csak e-mail terjesztési listaként használhatóak, jogosztásra alkalmatlanok.

A terjesztési listaként való használat gyakorlatilag annyit jelent, hogy a csoportnévre, mint e-mail címre levelet is írhatunk, amit minden csoporttag meg fog kapni.

A csoportok osztályozása hatókör alapján:

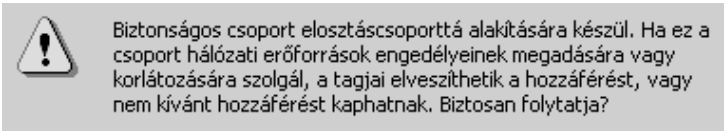
Univerzális csoport: Tagja lehet az Active Directory erdő tetszőleges tartományából bármely felhasználó vagy univerzális illetve globális csoport. Ez a csoporttípus csak natív módú tartományban használható.

Globális csoport: Tagja lehet bármely felhasználó és globális csoport is, de kizárólag abból a tartományból, amelyben létrehoztuk az adott csoportot. A globális csoportok egymásba ágyazása csak natív módú tartományok esetén használható.

Tartományi lokális csoportok: Csak egy adott tartomány kiszolgálóján fog megjelenni. Tagja lehet az Active Directory erdő tetszőleges tartományából származó univerzális csoport és globális csoport illetve saját tartományunk felhasználói és lokális csoportjai.

A Windows 2000 már megengedi a *csoportok egymásba való átalakítását* is. A lokális, globális és az univerzális csoportok egyaránt lehetnek terjesztési csoportok, vagy biztonsági csoportok. A biztonsági rendszer teljesítményének szempontjából lényeges a csoport típusa, mert a belépéskor létrejövő biztonsági tokennek nem része a terjesztési lista.

A biztonsági csoport és a terjesztési lista is átalakítható egymásba, de a biztonsági csoport átalakításánál az ábra szerinti figyelmeztetést kapjuk.



A legegyszerűbb esetben egyetlen tartományunk van, azaz nem kell számolnunk az erdő illetve a fa többi tartományával, ekkor természetesen az univerzális csoport és a globális csoport gyakorlatilag azonos.

Példa a csoportok alkalmazására

Vegyük példaként a következő egytartományos iskolai helyzetet. Van két csoportunk. Egyik a kezdő diákok számára *kezdők* néven, a másik pedig a haladó diákok számára *haladók* néven. Két szerverünk van. Egyiken a nyomtatót szeretnénk elérhetővé tenni a másikon, pedig a CD-ROM olvasót. Szeretnénk, ha a CD mindkét csoport számára elérhető lenne, de a nyomtatót csak a haladók tudnák használni.

Ilyenkor célszerű a *kezdők* és a *haladók* csoportot univerzális csoportként létrehozni. A CD-t kezelő szerveren egy lokális csoportot is hozzunk létre, pl. *mindenkié* néven, melyeknek tagja a két univerzális csoport és ennek az univerzális csoportnak engedélyezzük a CD-hez a hozzáférést. Célszerű létrehozni a nyomtatót tartalmazó szerveren pl. egy *nyomtathat* nevű lokális csoportot, majd ebben elhelyezni a *haladók* csoportot és végül a *nyomtathat* csoportnak megadni a nyomtatási jogot. Itt feleslegesnek tűnhet a csoportok egymásba ágyazása, de gondoljunk arra, hogy adódhat még nyomtatási jogot igénylő csoport[13].

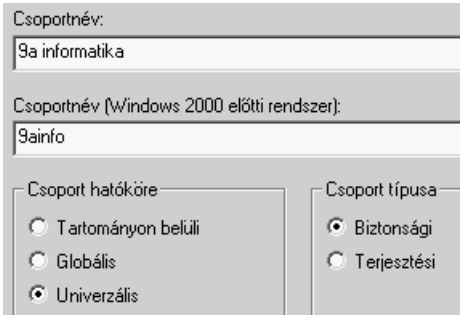
[13] Kisebb hálózatoknál megfelelő lehet, ha kizárólag univerzális csoportok használunk, de nagyobb hálózatoknál a hatékonyság miatt már célszerű a többi csoportot is használni.

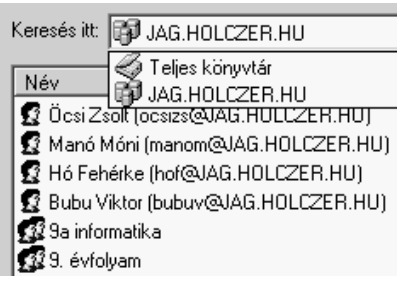
A javasolt csoportokba sorolásnak új diák érkezésekor is mutatkozik előnye. Ha új diákunk érkezik, akkor elegendő a megfelelő univerzális csoportba felvenni és már használhatja is a számára engedélyezett eszközöket. Ha nem használnánk csoportokat, akkor egyesével kellene leülnünk az egyes erőforrásokat kezelő szerverek elé.

Tegyük fel, szeretnénk a CD-hez való hozzáférési jogosultságokat megváltoztatni a *kezdők* és a *haladók* csoportra is. A *mindenkié* nevű lokális csoport létezése esetén elegendő a *mindenkié* csoportra beállítani a változásokat és ez mindkét univerzális csoportra és így tagjaira is hatással lesz.

Csoport létrehozása és törlése

Nyissuk meg a *Felügyeleti eszközök* csoportból a *Felhasználók és számítógépek* pontot, majd válasszuk ki az új csoportot tartalmazó tárolót. Ha nincs kijelölve a kérdéses tároló egyetlen eleme sem, akkor a *Műveletek* menü *Új* pontja alól válasszuk a *Csoport* lehetőséget. Adjuk meg az ábra szerinti adatokat, és már el is készültünk. A *Csoportnév* legfeljebb 64 betűs lehet, s nem szerepelhetnek benne a felhasználói névnél is tiltott karakterek.





Tagok hozzáadása a már létező csoport tulajdonságlapján át lehetséges. A tulajdonságlap *Tagok* fülén megadhatjuk, milyen tagjai legyenek a csoportnak és *A következő csoportok tagja* fülön pedig meghatározhatjuk a kérdéses csoport mely más csoportoknak legyen tagja. A tagok kijelölésénél a jobb oldali ábra szerint mindkét esetben megadhatjuk, hogy csak saját tartományunkból válogatunk, vagy az egész Active Directory tagságot szeretnénk megtekinteni.

A csoportok és a felhasználók *törlése* azonos módon zajlik. A törlés minden esetben a SID törlését jelenti.

A sablon felhasználó, felhasználók másolása

Amikor sok, közel azonos felhasználót kell létrehoznunk, akkor könnyíthetünk a dolgunkon. Gondoljunk például egy gimnáziumra, ahová tanévkezdéskor mindig új diákok érkeznek. Ilyenkor nem kell minden diáknak egyesével létrehozni a megfelelően beállított fiókot, hanem sokat könnyíthetünk munkánkon a

sablon felhasználóval. A sablon felhasználó valójában nem egy önálló felhasználótípus. A példának megfelelően, egyszerűen hozzunk létre egy felhasználót a megfelelő beállításokkal, ami majd minden új diák fiókjához alapul szolgál. A sablonként használt felhasználó fiókját feltétlen tegyük tiltott állapotba, azaz a helyi menüben válasszuk a *Tiltás* opciót.

Ha a sablonra alapozva új felhasználót szeretnénk létrehozni, akkor a következő a teendőnk. Kattintsunk a jobb egérgombbal a felhasználóra és válasszuk a *Másolás* pontot. Természetesen minden beállítás nem kerül lemásolásra. A nevet, teljes nevet, jelszót, egyéb személyes adatokat nekünk kell megadni, de a csoporttagságok, a távoli elérés beállításai és a fiók tiltottsági állapota másolásra kerül, amit célszerű kikapcsolni.

A felhasználó másolásával tetszőleges fiókot lemásolhatunk, akár a rendszergazda fiókját is. A profil és a home könyvtár egy adott felhasználóhoz tartozik, ezért úgy tűnhet, hogy nem lehet a sablon része. Ez azonban nem akadály, hiszen a profil és a home könyvtár megadásánál az elérési utakban a másolt felhasználói név helyére automatikusan bekerül az újonnan készülő felhasználó neve.

Feladatok

23. *Egy vállalkozás csoportjai*
Egy grafikával foglalkozó vállalkozásban találunk színes lézernyomtatókat a munkához és mátrixnyomtatót a számlázáshoz. Természetesen több grafikus és több számlázó is található a cégnél, a cégnek két vezetője van és várható újabb vezető is. Milyen csoportokat tudnánk javasolni?

24. *Csoport és szervezeti egység*
Az előző feladat vállalkozásához javasoljunk szervezeti egységeket is! Hasonlítsuk össze a csoportok és a szervezeti egységek felépítését!

25. *Új tanév kezdődött*
Az új diákok két osztályba kerülnek, pl. 9.a és 9.b. Mindkét osztálynak egyik fele informatika tagozatos a másik fele pedig normál tantervű. A későbbiek során lesznek olyan jogosultsági beállításaink, amelyek minden diákra vonatkoznak, egy-egy egész osztályra vonatkoznak, egy-egy egész tagozatra vonatkoznak, az osztályok tagozataira külön vonatkoznak. Hozzuk létre a megfelelő felhasználókat és csoportokat. Osztályonként legalább 5 diák legyen! Az informatika tagozatról a két legjobb tanulónak engedélyezzük a telefonos elérést visszahívás nélkül! Legyen mindenkinek profilja és home könyvtára is! Legyen mindenkinek az első jelszava „titok” és tegyük kötelezővé a jelszó megváltoztatását az első belépéskor! A két osztálynak legyen külön szervezeti egység is!

A csoportos házirend (group policy)

A házirend lehetőségei

A felhasználót a bejelentkezés után fogadó környezet két részből tevődik össze. Egyik rész a felhasználó által befolyásolható profil, a másik rész pedig a rendszergazda által előírt házirend. A teljesség igénye nélkül néhány fontosabb lehetőség, amit a házirend segítségével szabályozhatunk.

Szoftverek telepítése és törlése. Előírhatjuk, hogy egy adott gépen szerepeljen például egy könyvelőprogram, de a szoftver jelenléte felhasználóhoz is köthető. Kötelezővé tehető egy szoftver megjelenése, vagy felajánlható a felhasználónak, hogy döntse el kéri e a kérdéses szoftvert vagy sem.

Parancsfájl lefutását írhatjuk elő a gép indulásakor, illetve leállásakor, de a felhasználó be- és kijelentkezéséhez is előírhatunk parancsfájlt.

Beállíthatjuk a jelszavak élettartamát, hosszát, előzőek megjegyzését.

Megadhatjuk a fiókok zárolásának körülményeit.

A naplózás szabályait is előírhatjuk.

Speciális könyvtárak (pl. dokumentumok) hálózati helyre való átirányítása.

A Windows megjelenésének, működésének testreszabása.

A házirendet a csoportokra, a szervezeti egységekre illetve akár nagyobb egységekre külön-külön is beállíthatjuk, így létrejön a házirendek egyfajta hierarchiája. Ennek a lehetőségnek a kihasználásakor jól át kell gondolni a házirendek prioritását, nehogy egy szükséges beállítás a kiértékelés során felülíródjon. A csoportházirendek rendszerében az alacsonyabb szinten lévő tároló alapértelmezésben örökli a szülőobjektumban beállított házirendet. Természetesen a gyermekobjektumra külön is megadhatunk házirendet. A gyermekobjektum házirendje ütközés esetén felülbírálja a szülő házirendjét. A csoportházirendek rendszere a tisztán Windows 2000-es rendszerekben (szerver és munkaállomás is) használható ki teljes körűen.

A házirend beállítása

A *Felügyeleti eszközök* közül az *Active directory felhasználók és számítógépek* nevű menüpont alatt állíthatunk házirendeket. Ki kell választani azt a tárolót (tartomány, szervezeti egység), amelyre szeretnénk beállítani a házirendet majd a *Tulajdonságlap Csoportházirend* fülén láthatunk munkához. A fülön látjuk a tárolóhoz már hozzárendelt házirendeket és az alábbi műveleteket végezhetjük el.

Több házirend esetén a fel és le gombokkal állíthatjuk be a prioritásokat.

Új házirendet hozhatunk létre. Itt csak a névadás zajlik, a beállítás máshol.

Hozzáadhatunk egy létező házirendet a tárolóhoz.

A szerkesztés gomb alatt állíthatjuk be ténylegesen a házirendet

Beállíthatjuk, hogy más házirend-objektumok ne bírálhassák felül az adott beállításokat.

Törölni kétféleképpen lehet. Vagy teljesen töröljük a házirendet, vagy csak az adott tárolóból a rámutató hivatkozást.

A házirenddel kapcsolatos információkat a *Tulajdonságoknál* tekinthetjük meg. A *Csatolások* fülön megnézhetjük, hogy mely objektumokhoz van még hozzárendelve az adott házirend, a *Biztonság* nevű fülön, pedig a házirenddel kapcsolatos biztonsági beállításokat láthatjuk.

A házirend szerkesztése

Amikor a házirend szerkesztését választjuk, akkor a beállításokat két fő részben tehetjük meg. Ezek a *Számítógép konfigurációja* és a *Felhasználó konfigurációja*.

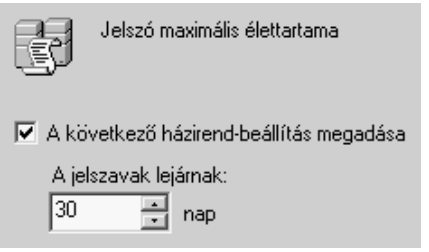
A *Csoportházirend* szerkesztőablaka az intézőhöz hasonlóan a két részre oszlik. A bal oldalon a beállítási szempontok fastruktúráját látjuk, a jobb oldalon pedig a kiválasztott szemponthoz tartozó értékeket.

Szoftverek telepítése

A *Szoftverbeállítások* alatt a *Szoftverek telepítése* ponttal az adott gépre szoftvereket telepíthetünk, illetve rendelkezhetünk a telepítés módjáról. A szoftverbeállítások alatti szoftver telepítése pontot csak a Microsoft Installer szolgáltatással együttműködő szoftverek esetében használhatjuk. Az installer szolgáltatást nem ismerő szoftverek esetében az adott alkalmazást valamilyen MSI technológiát ismerő segédprogrammal[14] be kell csomagolni. *A szoftver telepítése* pont kiválasztása után a *Művelet* menü *Új* pontját választva előbb meg kell neveznünk a telepítőcsomag helyét, majd a telepítés módjáról kell nyilatkozni.

Ha a telepítés módja *Közzétett*, akkor felhasználó dönthet, hogy kéri-e a kérdéses szoftvert vagy sem. Ha *Kötelező* a telepítés módja, akkor a szoftver mindenképpen települni fog, feltéve, hogy még nem volt a gépen. Így elérhető például, hogy meghibásodott gép helyére tett másik gépen automatikusan megjelenjenek a szükséges szoftverek.

A fiókházirend beállítása



Igen fontos lehetőség a *Windows beállításai* menüben a *Biztonsági beállítások* pont alatt a *Fiókházirend* pont. Itt egyik csoportban a jelszóval kapcsolatos beállításokat találjuk a másik csoportban pedig a felhasználói fiókok zárolásáról

[14] A telepítőkészlet CD-jén is találunk ilyen segédprogramot.

rendelkezhetünk. Mindkét esetben az ábrához hasonló ablakban adhatjuk meg a kívánt értékeket. A *Nincs megadva* érték nem azt jelenti, hogy a kérdéses beállításra nézve nem lép életbe semmilyen érték, hiszen más, magasabb szintű házirendek már rendelkezhettek erről az értékről. Ha beállítunk valamilyen értéket, akkor az felülbírálja (ha engedélyezett) más házirendek ezirányú rendelkezését. Természetesen, ha más házirendek sem rendelkeztek az adott beállítás felől, akkor valóban nincs semmilyen beállított érték.

A jelszóra vonatkozó beállítások

Az *Előző jelszavak megőrzése* alapértelmezés szerint *Nincs megadva*. Tehát az újonnan beállított jelszó, akár a régi jelszavunk is lehet. A hálózat biztonságának növelése érdekében javasolt ezt a beállítást megváltoztatni. Ha beállítottuk, például, hogy emlékezzen az utolsó 5 jelszóra, akkor az új jelszó az előző 5 közül eggyel sem egyezhet meg. A beállítható értékek 0 és 24 között vannak. A 0 jelenti, hogy nem figyeli az előző jelszavakat a rendszer.

A jelszó maximális élettartama alapértelmezése: *Nincs megadva*. Ez a gyakorlatban annyit jelent, hogy a felhasználó tetszőleges ideig használhatja a jelszavát, ami veszélyezteti hálózatunk biztonságát. Az élettartam 0 és 999 nap között állítható, ahol a 0 jelenti az örökéletű jelszót.

A jelszó minimális élettartama alapértelmezése: *Nincs beállítva*. Ilyen feltételek mellet a frissen beállított jelszó akár azonnal módosítható, egyébként a beállításnak megfelelően a jelszó módosítása csak a megadott számú nap letelte után lehetséges. Ha az *Előző jelszavak megőrzése* lehetőséget is beállítottuk, akkor célszerű a jelszónak egy minimális élettartamot is megszabni. A minimális élettartam 0 és a maximális élettartam közötti érték lehet. A 0 jelenti az azonnali változtathatóságot. Ha a minimum > maximum akkor természetesen figyelmeztet a rendszer, hogy lehetetlent akarunk.

A legrövidebb jelszó alapértelmezés: *Nincs megadva*. Ez azt jelenti, hogy a jelszó megadása nem kötelező. Biztonsági okokból célszerű, ha a jelszó megadását kötelezővé tenni. A legrövidebb jelszó hossza 0-14 karakter között változhat, ahol a 0 jelenti az üres jelszót.

A fiók zárolása

Más jelszavát legegyszerűbben próbálgatással szerezhetjük meg. Ha azonban néhány próbálkozás után a rendszer zárolja a felhasználó fiókját az növeli a hálózat biztonságát. Megjegyzendő azonban, hogy ezzel a felhasználók esetleg visszaélhetnek, hiszen a felhasználói nevek nem titkosak.

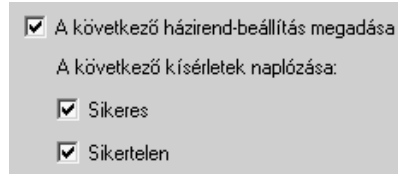
A *Fiókzárolás küszöbe* alapértelmezés: nincs megadva. Ekkor a felhasználó tetszőleges számú kísérletet tehet jelszavának eltalálására, egyébként a megadott számú hibás bejelentkezési kísérlet után a rendszer zárolja a felhasználói fiókot. A hibás bejelentkezések száma 0 és 999 között lehet. A 0 jelenti a tetszőleges számú próbálkozást.

Fiókzárolás időtartama. Itt adható meg, hogy az előző pontban megadott számú hibás bejelentkezési kísérlet után mennyi ideig ne engedje újra bejelentkezni a felhasználót. Az időtartam 0 és 99999 között lehet. A 0 jelenti az örökéletű kitiltást, ekkor csak a rendszergazda engedélyezheti újra a bejelentkezést, egyébként a megadott számú perc eltelte után a rendszer automatikusan engedélyezi a bejelentkezést. Természetesen a rendszergazda beavatkozása esetén nem kell kivárni az adott várakozási időt.

Fiókzárolási számláló nullázása. Alapértelmezés: nincs megadva. Természetesen a hibás bejelentkezések számlálása nem örökké tart, hanem itt állítható be, hogy mennyi idő eltelte után törlődjön a számláló. A beállítható érték 1 és 99999 perc között van. Érdemes megjegyezni, hogy ezek a beállítások nem függetlenek egymástól, hiszen a fiókzárolási számláló nullázásának kikapcsolása esetén a másik két beállítás is automatikusan *Nincs megadva* jelzést kap.

A naplórend

Beállítható, hogy a szerver bizonyos eseményeket naplózzon, azaz egy ún. log fájlban az esemény bekövetkeztét és annak körülményeit rögzítse.



A bejelentkezési kísérletek naplózása például a *Biztonsági házirend* menü *Helyi házirend* pontjában a *Naplórend* alatt adható meg. Az ábra szerinti esetben minden bejelentkezési kísérletet naplózni fog a rendszer. Ezzel azért óvatosan kell bánni, hiszen ilyen beállítások mellett igen gyorsan fog nőni a naplófájl mérete. Ha az ábra szerinti esetben töröljük az alsó két pipát, akkor semmit sem fog naplózni a rendszer a bejelentkezésekkel kapcsolatban.

Az objektum-hozzáférés naplózása lehetőség csak annyit jelent, hogy engedélyezzük e a naplózást vagy sem. Konkrétan egy objektum naplózását az objektum tulajdonságlapján írhatjuk elő.

A napló a *Felügyeleti eszközök* csoport *Eseménynapló* menüpontjának kiválasztásával tekinthető meg.

A felhasználói jogok

A felhasználóknak a különböző objektumokhoz való hozzáférési jogokon kívül a rendszer kezelésével kapcsolatos jogosítványokat is adhatunk. Ezeket a *Helyi házirend* menü *Felhasználói jogok kiosztása* pont alatt találjuk. Itt azokat felhasználókat és csoportokat kell megneveznünk, amelyeknek szeretnénk megadni a jogokat. Felhasználókat is megnevezhetünk, de célszerűbb csoportokhoz rendelni a jogokat.

Rendszer leállítása. Ha ezzel a joggal nem rendelkezik a felhasználó, akkor a *Start* menü *Leállítás* pontja alatt csak a *Kijelentkezést* választhatja.

Fájlok és egyéb objektumok saját tulajdonba vétele. Ennek a jognak az osztásával óvatosan bánjunk, hiszen egy tulajdonjog átvétele után pl. egy fájlal azt teszünk amit akarunk, pedig előtte még hozzáférésünk se volt.

Helyi bejelentkezés és helyi bejelentkezés megtagadása. Ha a bejelentkezési joggal nem rendelkezünk az adott gépen, akkor a rendszer nem engedélyezi a belépést akkor sem, ha jól adtuk meg a jelszavunkat.

Kvóták növelése. Ennek a jognak a birtokában változtathatjuk meg az engedélyezett lemezterület méretét. Ha az egyszerű felhasználó is megkapja ezt a jogot, akkor gyakorlatilag semmit sem ér, ha az általa használható lemezterület korlátoztuk.

Rendszeridő megváltoztatása. Ez a jog azért fontos, mert a rendszernapló értelmezésénél fontos szerepe lehet a bejegyzés időpontjának is.

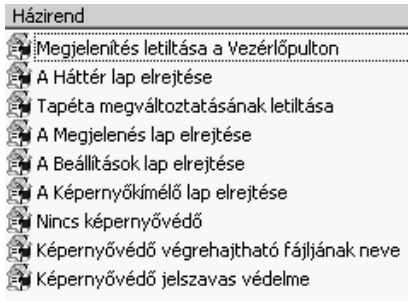
A biztonsági beállításokat megtehetjük kézzel, de előre gyártott beállításokat is importálhatunk a házirendbe. A biztonsági beállítások pontra a jobb egérgombbal kattintva a megjelenő menüben találjuk a Házirend importálása pontot. Néhány előre elkészített beállításokat tartalmazó fájl:

basicwk.infinf	Alapértelmezett munkaállomás
basicsv.inf	Alapértelmezett kiszolgáló
basicdc.inf	Alapértelmezett tartományvezérlő
securews.inf	Biztonságos munkaállomás vagy kiszolgáló
hisecws.inf	Nagy biztonságú munkaállomás vagy kiszolgáló
securedc.inf	Biztonságos tartományvezérlő
hisecdc.inf	Nagy biztonságú tartományvezérlő

Fontos tudni, hogy az inf fájlok nem kumulatívak. Ez annyit jelent, hogy a magasabb biztonsági szint eléréséhez az alacsonyabb biztonsági szinthez tatozó inf fájlokat is importálni kell. Például a hisecws.inf előtt fel kell tenni basicws.inf, majd a securews.inf állományt.

Kiegészítések a házirend beállításához

Érdeklődőknek érdemes megtekinteni még néhány érdekes lehetőséget. *A felhasználó konfigurációja* menü *Windows beállításai* pontja alatt a felhasználó be- és kijelentkezéséhez adhatunk meg parancsfájlokat. *A mappa átirányítása* pont alatt a felhasználó szempontjából fontos mappákat a hálózat adott helyére irányíthatunk át. *A felhasználó konfigurációja* menü *Felügyeleti sablonok* pont alatt



részletesen meghatározhatjuk a Windows viselkedését. A mellékelt képen a képernyő viselkedésével kapcsolatban láthatunk néhány lehetőséget.

A házirend beállításai a belépéskor automatikusan frissülnek, egyébként rendelkeznünk kell a frissítési lehetőségekről. A frissítési beállítások házirendenként eltérőek lehetnek és a következő helyen találjuk meg a házirend szerkesztőablakában a *Felhasználó konfigurációja, Felügyeleti sablonok, Rendszer, Csoportházirend*. Itt részletes magyarázatot is találhatunk a beállítások hatásairól.

Feladatok

26. *A jelszó élettartama*
Ha azt szeretnénk, hogy a felhasználó biztosan új jelszót adjon meg 42 naponként, miért nem elég *A jelszó maximális élettartama* lehetőség 42-re állítása?

27. *Új jelszó*
Ha azt szeretnénk, hogy a felhasználó biztosan új jelszót adjon meg, miért nem szükséges *A jelszó minimális élettartama* lehetőséget is beállítani?

28. *Fiókzárolási küszöb*
Milyen feltétele van annak, hogy eltérő fiókzárolási küszöböt állíthassunk be az informatika tagozat és a normál tagozat számára? Tegyük is meg a beállítást, de tagozat jelszavai legyenek védettebbek!

29. *Jelszó beállítása*
Tartományi szinten állítsunk be minimális jelszóhossznak 5-öt. A 9.a. szervezeti egységre állítsunk be minimális jelszóhossznak 7-et. Mennyi lesz a minimális jelszóhossz a 9.a. számára?

30. *Háttér beállítása*
Állítsunk be kötelező, de eltérő hátteret a 9.a. és a 9.b. számára. Milyen feltétele van annak, hogy ezt megtehessük?

31. *Belépési parancs fájl*
Készítsünk egy szövegfájlt, amiben tudatjuk az informatika tagozattal, hogy a hétvégén karbantartás miatt leállítjuk szervereinket! Csak az informatika tagozatnak jelenjen meg ez a szövegfájl belépéskor!

32. *Objektum-hozzáférés naplózása*
Mi a különbség a diákok nevű szervezeti egységre beállított következő értékek között: nincs naplózás; nincs megadva?

33. *Rendszer leállítása*
Vendégeknek nem szeretnénk engedélyezni a rendszer leállítását. Mit kell tennünk?

Fájlrendszerek

Adataink, programjaink, dokumentumaink valamilyen adathordozón foglalnak helyet, hogy a gép kikapcsolt állapotában is megőrizhessük őket. Az állományok floppyn, winchesteren, CD-n való elhelyezkedését írja le a *fájlrendszer*. A fájlrendszer határozza meg, hogyan kerülnek az állományok az adathordozóra, hogyan kell tájékozódni a lemezen, milyen adatokat tároljunk az állományainkról stb. Egy operációs rendszer természetesen több fájlrendszert is ismerhet, egy meghajtó fájlrendszere a meghajtó *tulajdonságlapjáról* is megállapítható.

A leggyakoribb fájlrendszerek a következők:

FAT (File Allocation Table)

A FAT az MS-DOS operációs rendszerhez kialakított fájlrendszer. Két változata van, a FAT 16 az eredeti MS-DOS-os, míg újabb változata a FAT 32, a Windows 95 OSR2-től kezdve használható. Míg a FAT 16-os fájlrendszert minden Windows változat és az MS-DOS is ismeri, addig a FAT 32-es fájlrendszert csak a Windows 95 OSR2, Windows 98 és a Windows 2000 ismeri, a Windows NT 4 nem látja a FAT 32 fájlrendszerű lemezeket.

A FAT rendszerek lényege, hogy a meghajtót adott hosszúságú darabokra, ún. foglalási egységekre (Allocation Unit) bontják, és ezeket mint önálló egységeket kezelik. Egy foglalási egységben legfeljebb egy fájl lehet, de egy hosszabb fájl természetesen több foglalási egységre bomlik. A fájl elhelyezkedését (kezdetét, folytatását, befejezését) a fájlrendszer a foglalási egységek sorszámával tartja nyilván. E sorszám a FAT 16-ban 16 bites, míg a FAT 32-ben 32 bites, így ez utóbbi több foglalási egységet tud kezelni, míg az előbbi egy nagyobb winchester esetén kénytelen nagyobb méretű foglalási egységekkel dolgozni, mivel a legnagyobb sorszáma is legfeljebb 16 bites szám lehet.[15]

A FAT 16 által elérhető maximális partícióméret 2GB. A FAT 32 használatával az elméleti maximum 2 TB, de ez a gyakorlatban 32 GB-ot jelent. Mivel a FAT 32 gazdaságosabban használja ki a winchesterünk területét, ha az 1GB méretű adathalmazunkat FAT 16-os fájlrendszerű lemezről áthelyezzük FAT 32-es fájlrendszerű lemezre, akkor a helyfoglalás több 10 MB-tal, de akár 100 MB-tal is csökkenhet.

A FAT fájlrendszer előnye, hogy minden MS operációs rendszer ismeri, 400 MB merevlemez-kapacitás alatt gyorsabb, mint az NTFS fájlrendszerű lemez, de hátrányként jelentkezik, hogy a FAT alkalmatlan az adatok fájlszintű védelmére. Ha FAT-ot használunk a Windows 2000 alatt, akkor nem tudjuk kihasználni a fejlett védelmi rendszer szolgáltatásait.

[15] A FAT-nak van egy 12 bites változata is, amit a hajlékonylemezek használnak. Ez maximum 4096 foglalási egység tárolását engedi meg, és 512 bájt a foglalási egység.

Az NTFS (New Technology File System) fájlrendszer

Az NTFS fájlrendszert a Windows NT számára hozták létre. A Windows 2000 ennek továbbfejlesztett változatát az NTFS 5 fájlrendszert használja. Az NTFS 5 felülről kompatibilis az előző NTFS verzióval[16]. Elméletileg a legnagyobb partíció-méret 16 EB (azaz $16 \cdot 2^{60}$ B). A jelenleg ismert legnagyobb implementáció is „csak" néhány TB méretű.

Az NTFS fájlrendszer használatával állományszintű hozzáférési jogokat állíthatunk be. A hozzáférési jogosultságok a fájlrendszerben vannak tárolva. Az adatokat akár fájlonként is tömöríthetjük működés közben. Szintén a fájlrendszer felépítéséből adódóan sokkal hibatűrőbbé tehetjük a rendszerünket. Az NTFS védelme még a törlésnél is érvényesül, ez annyit jelent, hogy amit az egyik felhasználó a lomtárba helyezett azt a másik felhasználó nem veheti ki. Mivel az NTFS fájlrendszer több információt tárol az állományokról, ezért a fájlrendszer helyigénye is nagyobb. Az NTFS fájlrendszer minimum 1,5 MB helyet igényel ezért floppykon nem is használható. A FAT rendszerű merevlemezt konvertálhatjuk NTFS rendszerűvé, még akkor is, ha van adat a winchesteren. Az NTFS fájlrendszerű merevlemezt nem lehetséges FAT fájlrendszerűvé átalakítani.

Az NTFS fájlrendszer néhány hasznos szolgáltatása

Az NTFS fájlrendszer egyik legfontosabb szolgáltatása a *Hozzáférési jogok kezelése*, amelyről a későbbiekben bővebben is szó lesz, illetve a már korábban is tárgyalt *Hozzáférések naplózása*.

Titkosítás. Ez igen hasznos lehet, mert az így titkosított fájlok még akkor sem olvashatóak, ha egy másik gépbe átraktuk a winchestert. Titkosíthatunk fájlonként is, de mappa is titkosítható. Ennek módja a következő. A fájl tulajdonságlapján az *Általános* fülön a *Speciális* gomb alatt válasszuk ki a *Tartalom titkosítása az adatvédelem érdekében* nevű pontot. A változások akkor történnek meg, amikor a tulajdonságlapot bezárjuk. Ha fájlt választottunk ki, akkor kapunk egy újabb kérdést, amely szerint eldönthetjük, hogy csak az adott fájlt szeretnénk titkosítani, vagy a kérdéses fájlt tartalmazó mappát is. Mappa titkosítása esetén eldönthető, hogy az almappákat is szeretnénk titkosítani, vagy sem. Ha nem a titkosítást végző próbál egy fájlhoz hozzáférést megkísérelni, akkor a hozzáférés megtagadva hibajelzést fogja kapni. Megfelelő jogosultságok birtokában legfeljebb letörölheti a fájlt[17]. A fájl NTFS kötetre történő másolásakor is megőrzi titkosított mivoltát, de FAT rendszerű kötetre másoláskor a titkosítottság megszűnik, hiszen a FAT fájlrendszer ilyen irányú információ tárolására nem képes. Természetesen illetéktelen nem is másolhatja a titkosított fájlt. A titkosításhoz használt kulcs erősen kötődik a titkosító felhasználóhoz, ami annyit jelent, hogy

[16] A Windows NT4 csak a SP4-től kezdve látja az NTFS 5 partíciókat.

[17] Át is nevezheti, de ettől még nem fér hozzá.

a felhasználó törlése után a titkosított fájlok nem lesznek olvashatóak. Ilyen esetben a helyreállító ügynök (recovery agent) biztosítja a titkosított fájlok elérését. A helyreállító ügynök szerepét alapértelmezésben a rendszergazda birtokolja.

A lemezkvóták engedélyezése. Ez egy régen várt lehetőség az NTFS fájlrendszerben. Megszabhatjuk az egyes felhasználók által igénybe vehető lemezterület nagyságát. Ezt a beállítást lemezenként kell/lehet megtenni, egy lemezen belül az elfoglalt területek összege számít. A kvótakezelést a megfelelő lemezegység tulajdonságlapjának kvóta nevű fülén engedélyezhetjük, alapértelmezésként nincs korlátozás a területhasználatot illetően. A kvótabejegyzések gomb lenyomása után megadhatjuk, hogy melyik felhasználónak mennyi lemezterületet szánunk.

A kvótanyilvántartásban az ábra szerinti értékeket láthatjuk. Lényeges tudni, hogy a korlát fölött jelzést kapott felhasználónak automatikusan nincs megtiltva további lemezterület felhasználása, ehhez a tulajdonságlap kvóta nevű fülén *A lemezterület tiltása a kvótát túllépő felhasználóknak* jelölőnégyzetet is ki kell választanunk. A *Kvóta* fülön megadhatjuk, hogy mi legyen az újonnan létrejövő felhasználók esetén az alapértelmezett korlát, természetesen korlátlan lemezhasználatot is megadhatunk az új felhasználóinknak alapértelmezésként. Ha a korlátozás mellett döntünk, akkor meg kell adnunk, hogy mi legyen a felhasználható terület mérete és mi legyen a figyelmeztetési korlát küszöbe[18]. Ha megtiltottuk a kvótát túllépők további területhasználatát, akkor ezek a felhasználók a *Hozzáférés megtagadva* hibajelzést kapják az írási kísérletre. A kvótanyilvántartásban az ábra szerinti értékeken kívül a következő értékeket láthatjuk: *felhasznált mennyiség*, *kvótakorlát*, *figyelmeztetési szint*, *felhasznált százalék*. Jó tudni, hogy a másolással készült felhasználó örökli a kvóta-beállításokat is.

Röptömörítés: A rendszer automatikusan elvégzi a tömörítést a háttérben. Ekkor nem készül archív állomány és változatlanul használhatjuk tovább állományainkat. Ha egy tömörített mappába fájlt másolunk, akkor a rendszer a másolás folyamata alatt „röptében” tömöríti az adatokat. A tömörítés - akár fájlonként – az adott objektum tulajdonság-lapjának általános fülén a *Speciális* gomb alatt állítható be.

Kiterjeszthetőség: A kötet kapacitása adatvesztés nélkül növelhető azáltal, hogy területet adunk a már létező lemezhez.

Tranzakció alapú lemezkezelés: Egy ilyen rendszerben, *vagy teljes egészében végrehajtódott egy lemezművelet vagy el sem kezdődött*. Köztes lehetőség nincs. Ha mégis előállna ilyen helyzet, pl. egy írásközben történt áramszünet mi-

[18] Csak a naplóba és a kvótanyilvántartásba kerül bejegyzés

att, akkor a rendszer a tranzakciós napló segítségével visszaállítja az utolsó helyes állapotot.

Rugalmas szektorkizárás (Hot fixing): A munka közben talált hibás foglalási egységeket a rendszer megjelöli és ilyen esetekre tartalékolt helyre áthelyezi a még menthető adatokat.

A CDFS fájlrendszer

A CDFS fájlrendszert használja az operációs rendszer a CD-ROM-ok kezelésére. Ilyen formátumban csak olvasható a lemez. Ha a CD-lemez gyökérkönyvtárában van egy autorun.inf nevű állomány, akkor a lemez behelyezése után azonnal elindul a benne megadott alkalmazás

Feladatok

34. *FAT 12*
Számoljunk utána, hogy a floppykon miért elegendő az a 12 bit! A „FAT11” jó lenne a floppykhoz? Miért?

35. *CD másolása*
Van egy adattal teleírt CD lemezünk. Ha a CD író másoló funkcióját használjuk, akkor minden rendben megy. Ha előbb felmásoljuk adatainkat a winchesterre, majd mindent szeretnék kiírni CD-re, akkor szól a program, hogy túl sok az adat egy CD-hez. Mi történt?

36. *Hozzáférés korlátozása*
Titkos anyagainkat úgy tároltuk egy munkaállomáson, hogy csak mi értük el. Átépítés miatt újra kellett telepíteni az operációs rendszert a munkaállomáson ezért lemezre mentettük anyagainkat, majd a telepítés után visszamásoltuk a munkaállomásra. Mire kell ügyelnünk, ha ezt a módszert alkalmazzuk?

37. *Fájlmásolás*
Floppynkon 100 KB szabad hely van. Egy 110 KB-os állományra a winchesteren bekapcsoljuk a tömörített attribútumot, aminek hatására a kérdéses fájl 60 KB méretűvé válik. Elkezdjük a másolást. Mit fogunk tapasztalni?

38. *Tömörítés*
A sakk.exe nevű állományt és másolatát is tömörítettük. Az eredeti állományt a tömörített attribútum bekapcsolásával, a másolatot a winzip nevű segédprogrammal. Az eredmény tekintetében milyen hasonlóságot és eltérést állapíthatunk meg?

39. *Meghajtó tömörítése*
Egy winchester tulajdonságlapján kiválasztottuk a *meghajtó tömörítése helymegtakarítás végett* jelölőnégyzetet. Mi válik ekkor bizonytalanná?

Megosztások

A megosztás fogalma

Ha hálózaton át elérhető egy számítógép, akkor felmerül a kérdés, hogy a felhasználók mit tudnak tenni ezen a gépen. A hálózatból természetesen láthatjuk a kérdéses gépet, de alapértelmezésként a többi munkaállomáson semmilyen és a szerverek esetén is csak néhány alapértelmezett mappát láthatnak a felhasználók.

Azokat a mappákat, amelyeket szeretnénk elérhetővé tenni a hálózat felhasználói számára a szerveren, a munkaállomáson vagy a kliensen meg kell osztani. A megosztott mappákat egyszerűen *megosztásnak* nevezik. Ezeket a megosztásokat szerverek esetén a tartomány rendszergazdája, munkaállomás esetén a helyi rendszergazda állítja be. A hálózat gépei és a gépeken megosztott mappák, eszközök a *hálózat tallózásakor* jelennek meg.

Alapértelmezettként léteznek az úgynevezett *adminisztratív megosztások*, melyek a hálózat tallózásakor a felhasználók számára nem jelennek meg. Ezek a megosztások csak a megosztásnév pontos ismeretében érhetők el, nevük kötelezően a $-jelre végződik, például C$ vagy admin$. Ez utóbbi megosztás mindig a WINNT nevű mappát jelenti bárhol is legyen rendszerünkben. Az adminisztratív megosztások tehát csak adminisztrátori jogosultságokkal és a megosztásnév pontos ismeretében érhetőek el. Ha szeretnénk egy winchestert teljes egészében megosztani, akkor a főkönyvtárra létre kell hozni egy új megosztást amihez beállítjuk a megfelelő jogokat, hiszen az alapértelmezett – pl. D$ - megosztáshoz csak adminisztrátorként férünk hozzá.

A megosztásokhoz rendelhető jogosultságok

A Windows 9x, Windows NT és Windows 2000 esetén a megosztásokhoz a következő jogosultságokat rendelhetjük.

Windows 9x	*Windows NT*	*Windows 2000*
Csak olvasásra	Nincs hozzáférés	Olvasás
Teljes	Olvasás	Módosítás
Jelszófüggő	Módosítás	Teljes hozzáférés
	Teljes hozzáférés	és a fentiek tagadása

A megosztásokhoz beállított jogok a FAT és az NTFS fájlrendszer használata esetén is érvényesek, de kizárólag egy másik gépről való elérési kísérletnél fejtik ki a hatásukat. Hiába állítottunk be csak olvasási jogot a megosztáshoz, ha a felhasználó leülhet a megosztást tartalmazó gép elé, akkor már teljesen más

jogosultságokkal is rendelkezhet. FAT fájlrendszer esetén ez teljes hozzáférést jelent, mivel a FAT nem tárol védelmi információkat a fájlokról, mappákról.

A sajátgépben vagy az intézőben egységes jele van annak, hogy a mappa vagy a meghajtó megosztott vagy sem, a megosztás jele az ábrán látható kéz. A képek nevű mappa a hálózat minden felhasználójának elérhető, feltéve, hogy rendelkeznek a megfelelő jogosultságokkal.

A megosztott mappa használata

A megosztott mappa többféleképpen is elérhető. Láttuk, hogy megjelenik a *hálózat tallózásánál*, de hivatkozhatunk rá UNC névvel is. Példaként tegyük fel, hogy a *Install* nevű megosztott mappa a *Viktor* nevű gépen van, ekkor az UNC hivatkozás: \\viktor\install,

A hálózat egy hasznos lehetősége, hogy a megosztást mint önálló meghajtót is kezelhetjük, ez főleg akkor kényelmes, ha egy megosztást gyakran használunk. Természetesen a hálózati meghajtók esetén a formázás értelmetlen művelet. Az ábrán is látható példánk szerint az *Install* néven megosztott mappára a felhasználó a gépéről *S:* meghajtó néven hivatkozhat.

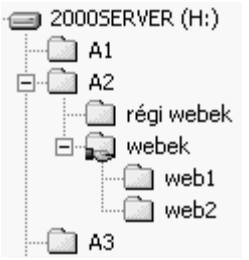
Hálózati meghajtót kétféleképpen is beállíthatunk, legegyszerűbben az *Intéző* program *Eszközök* menüpontjában csatlakoztathatunk, illetve választhatunk le hálózati meghajtót. A másik lehetőség, hogy a parancssorba beírjuk a NET USE S: \\VIKTOR\INSTALL utasítást. Ha az előbbi hozzárendelést szerverünkön (vagy munkaállomásunkon) megtettük, akkor pl. egy programot kétféleképpen indíthatunk el a gép előtt ülve. Szemléletesebben látjuk a különbséget, ha parancssorból kiadandó utasítást nézzük meg.

C:\INSTALL\SETUP.EXE

S:\SETUP.EXE

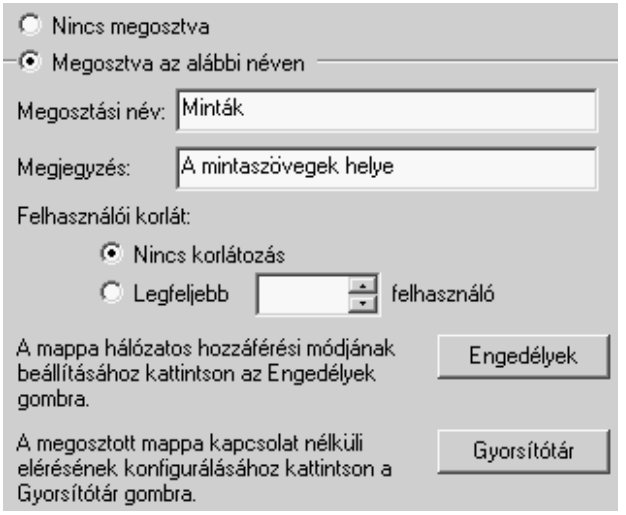
Érdekes lehet, hogy a szerver előtt ülve hogyan közelítünk a C: meghajtóhoz. Ha helyi winchesterként, akkor meg is formázhatjuk, ha hálózati meghajtóként, akkor nem formázhatunk, viszont leválaszthatjuk a meghajtót. A gépünkben lévő winchesterek automatikusan megkapják a C$ D$ … nevet, mint adminisztratív megosztások.

Felmerül a kérdés, hogy a hálózaton át láthatunk-e olyan mappát, ami nincs megosztva? A láthatóság a mappa elhelyezkedésétől (és természetesen a megfelelő jogosultságoktól) függ. Az ábra szerint a *webek* nevű mappát és minden almappáját elérjük, de az azonos és magasabb szinten található mappákat már nem.



Mappa megosztása

Egy mappát a következő módon oszthatunk meg. Jelöljük ki a megfelelő mappát, majd a tulajdonságlapon válasszuk a *Megosztás* fület. Értelemszerűen az alapértelmezett *Nincs megosztva* helyett válasszuk a következő lehetőséget:



Megosztva az alábbi néven: itt adhatjuk meg a megosztás nevét. Kitöltése kötelező, alapértelmezésként ez a mappa eredeti neve lesz. A névadásnál legyünk tekintettel arra az operációs rendszerre, amelyikről a felhasználók el akarják érni a megosztást. Lényeges, hogy *a hálózaton át az itt megadott néven hivatkozhatunk a mappára és nem a mappa eredeti* nevével. Természetesen két megosztásnév nem lehet azonos egy gépen.

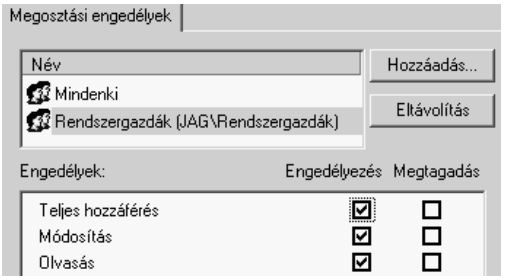
Megjegyzés: rövid megjegyzést fűzhetünk a megosztáshoz, kitöltése nem kötelező.

A *Felhasználói korlát* részen belül a következő beállításokat tehetjük meg:

Nincs korlátozás: ekkor nem korlátoztuk a csatlakoztatható felhasználók számát. Annyi kapcsolat lehet egyszerre, amennyit a szerver elbír.

Legfeljebb □ *felhasználó*: egyszerre csak □ darab felhasználó csatlakozhat, a többi csatlakozni próbáló felhasználó hibaüzenetet kap, mely szerint több kapcsolat nem létesíthető.

Engedélyek: Itt állíthatjuk be a hozzáférési jogokat. Az *engedélyek* gombra kattintva a megosztáshoz rendelt jogosultságokat látjuk. Megtekinthetjük a kiválasztott elem hozzáférési jogosultságát és akár módosíthatjuk is. Az *Eltávolítás* gombbal távolíthatunk el elemet a listából, a *Hozzáadás* gombbal, pedig bővíthetjük a jogosultak listáját. A gomb lenyomására kapott ablak egy pici eltéréssel megegyezik a csoporttagok bővítésénél kapott ablakkal. Megválaszthatjuk, hogy honnan kívánunk válogatni, majd a megjelenő listából kiválaszthatjuk a nekünk tetsző felhasználókat, illetve csoportokat.



Az *Új megosztás* gombbal (ha már megosztott volt a mappa) egy újabb megosztási nevet rendelhetünk egy mappához, újabb korlátokkal és újabb engedélyekkel. Ha pl. egy adatok nevű winchester gyökérkönyvtárát szeretnék elérhetővé tenni az egyszerű felhasználók számára is, akkor így kell eljárnunk.

A megosztáshoz való effektív hozzáférési jog

Vizsgáljuk meg a következő helyzetet. Mézga Géza nevű diákunknak a JATEK nevű megosztáshoz csak olvasási joga van, mint a *diákok* csoport tagjának. Mézga Géza viszont tagja a *karbantartók* nevű csoportnak is, akik viszont teljes hozzáféréssel rendelkeznek a kérdéses mappához. Mit tehet meg Mézga Géza amikor a JATEK nevű megosztáshoz csatlakozik? A válasz megértéséhez tekintsünk át néhány példát a JATEK nevű megosztással kapcsolatban!

Diák csoport	*Karbantartók csoport*	*Effektív jog*
Olvasás	Teljes	Teljes
Olvasás	Módosítás	Módosítás
Teljes	Módosítás	Teljes
Teljes	Nincs	Nincs
Teljes	– (nem tag)	Teljes

A táblázatot megtekintve megállapítható, hogy eltérő megosztási jogok esetén a különböző jogok uniója érvényes egyetlen kivételtől eltekintve, a *Nincs hozzáférés* jog mindennél erősebb. Figyeljünk arra, hogy aki nincs a hozzáférési listában semmilyen úton sem (saját jogon vagy csoporttagságok útján) annak effektív a joga a *Nincs hozzáférés.*

A megosztáshoz való hozzáférési jogok öröklődése

Az ábrán a *Játékok* nevű megosztáshoz *Teljes hozzáférése* van a felhasználónak, míg a *Logikai* nevű megosztáshoz csak *Olvasási jogot* kapott. Mit tehet a felhasználó a sakk nevű mappában, ha megosztások útján éri el? Erre a kérdésre a válasz helyzettől függő.

Ha a sakk nevű mappát a *Játékok* megosztáshoz csatlakozva éri el a felhasználó, akkor bármit tehet benne, még le is törölheti.

Ha a *Logikai* megosztáshoz csatlakozik, akkor csak olvasni tudja a sakk tartalmát és természetesen le sem törölheti a mappát.

A megosztott mappára beállított jogok automatikusan érvényesek az összes alkönyvtárra is feltéve, hogy a kérdéses megosztáson keresztül érjük el az alkönyvtárakat.

Kapcsolat nélküli elérés

A kapcsolat nélküli elérés azt jelenti, hogy a szerver valamely megosztásán lévő fájlt akkor is használhatjuk a munkaállomáson, ha a kettő közötti kapcsolat valamilyen ok miatt szünetel. Ez természetesen azt jelenti, hogy az ilyen fájloknak a munkaállomáson is jelen kell lenniük, ha a felhasználó az adott fájlt módosítja, a kapcsolat helyreállításakor lezajlik a szinkronizálás és automatikusan frissül a szerveren lévő változat. Ez a folyamat a felhasználó kilépésekor is lezajlik. Fontos, hogy a folyamat automatikus, a felhasználó mindvégig úgy dolgozhat, mintha a kapcsolat élne.

Egy megosztás tartalmának kapcsolat nélküli elérését a mappa tulajdonságlapján a *Gyorsítótár* nevű gomb alatt érhetjük el. Fontos, hogy itt csak a lehetőség engedélyezése történhet meg, de hogy ténylegesen mely állományok lesznek elérhetőek kapcsolat nélkül is, azt a megosztáshoz való csatlakozás után a felhasználó döntheti el. Ehhez a jobb gombbal az objektumra kell kattintania és a megjelenő menüből a *Kapcsolat nélküli elérés* pontot kell kiválasztania. Ekkor a fájl ikonja – a bal alsó sarokban - kiegészül egy jelzéssel.

Ha kapcsolat nélküli módban szerkeszthetünk egy fájlt, akkor szinkronizáláskor problémát okozhat, hogyha többen is szerkesztették az adott fájlt. Ilyen esetekben a szinkronizálás alatt egy kérdést kapunk, hogy melyik változat maradjon meg. Természetesen megtarthatjuk mindkét változatot. Ekkor automatikusan egy kiegészítést kap a fájl neve, ami jelzi, hogy melyik változatot ki készítette.

Egész mappát is elérhetővé tehetünk kapcsolat nélküli módban, de a túl sok szinkronizálásra váró fájl elég nagy feladatot ad gépünknek.

A megosztott mappákkal kapcsolatban a munkaállomásokon az *Eszközök* menü *Mappa beállításai* pont, *Kapcsolat nélküli fájlok* pontja alatt tehetünk

további beállításokat. Egy hasznos lehetőség hogy megtekinthetjük az összes kapcsolat nélkül elérhető állományunkat bármely mappában is legyenek azok.

DFS (elosztott fájlrendszer)

Az elosztott fájlrendszer (DFS, Distributed File System) *segítségével a különböző szervereken elhelyezkedő megosztásokat egy egységes rendszerbe foglalhatjuk.* Segítségével a megosztások átláthatóbbak, egyszerűbben kezelhetőek.

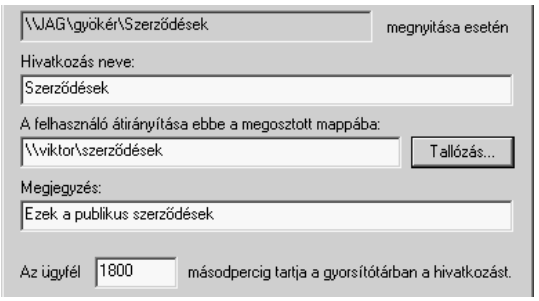
Az ábrán egy már létrehozott DFS-t látunk, a DFS gyökere ezúttal a *gyökér* nevű mappa a tartományvezérlőn. Ez alá a gyökér alá vehetjük fel a DFS nyilvántartásába a már létező megosztásainkat. Az ábra jelzi az egyes megoldásokkal kapcsolatos információkat is, most például a *hj* állapota ellenőrzött és elérhető, az *xy* állapota ellenőrzött és nem érhető el, az *ovix* állapota nem ellenőrzött.

Miért lesz ez a szerkezet előnyös? Példánkban az ábra szerinti *ovix* mappára a következő módon hivatkozhatunk: \\jag\gyökér\ovix, tehát a felhasználónak nem kell tudnia, hogy fizikailag hol található a megosztás. Az ábra szerinti 3 megosztásból 2 a szerveren van, de az xy nevű egy Windows 2000 munkaállomáson. A megosztásoknál látottak szerint engedélyezhetjük a kapcsolat nélküli elérést is.

A \\jag\gyökér hivatkozás „csak" a DFS gyökeret csatlakoztatja, így egy helyen látjuk a DFS által nyilvántartott összes megosztásunkat. Ez a hivatkozás azonban elviekben is lényegesen különbözik a szokásos \\gépnév\megosztásnév hivatkozástól. A DFS-ben a hivatkozás a következő módon nézhet ki: \\tartománynév\gyökérnév\hivatkozásnév. A hivatkozásnév a megosztás DFS hivatkozási neve, ami lehet akár más is, mint a megosztási név.

A DFS létrehozása

A DFS felépítését a *Felügyeleti eszközök* programcsoport *Elosztott fájlrendszer* pontja alatt kezdhetjük meg. Elsőként meg kell adni, hogy melyik mappa lesz a DFS gyökere.



A gyökér alá a következő módon vehetjük fel a hivatkozásokat. Ki kell jelölnünk a gyökeret, majd a *Műveletek* menü vagy a helyi menü *Új DFS hivatkozás* pontját választva az ábrát kapjuk. Meg kell adnunk a DFS hivatkozási nevet, majd a mappa szoká-

sos elérési útját, amit akár tallózás útján is megtehetünk.

Az ügyfél 1800 másodpercig tartja a gyorsítótárban a hivatkozást rész annyit jelent, hogy a DFS hivatkozás törlése után még 30 percig el fogja érni a megosztott mappát.

Szerverünk meghibásodása esetére egy másik szervert megnevezhetünk a DFS gyökér replikációs partnerének, ami azt jelenti, hogy szükség esetén a replikációs partner automatikusan átveszi a DFS-sel kapcsolatos teendőket és mindezt úgy teszi, hogy a felhasználók nem is fogják érzékelni.

Ha a rendszergazda szeretne egy megosztást áthelyezni, akkor csak a régi DFS hivatkozást kell törölnie és az új hivatkozást azonos néven létre kell hoznia. Ilyenkor figyelnie kell a gyorsítótárban tartás idejére is, mert a felhasználó akkor fogja az új tartalmat látni, ha az idő lejárt és frissít.

Feladatok

40. *Azonos nevű megosztások*
Megoldható e, hogy két azonos – pl. iratok – nevű mappánk egyszerre látható legyen a hálózaton?

41. *A C$ megosztás*
Egyik diákunk nem tud adminisztrátori jogosultsághoz elegendő jelszót, mégis látja egy adott Windows 2000-es munkaállomás winchesterének gyökérkönyvtárát. Hogyan lehetséges ez?

42. *Nincs megosztva*
Elérhetünk olyan mappát a szerveren, ami nincs megosztva?

43. *Windows 95 és NTFS*
Mint ismeretes a Windows 95 nem látja az NTFS formátumú partíciókat. Miért látják Windows 95-ös gépek mégis a szerver NTFS fájlrendszerű partícióján a megosztásokat?

44. *DOS és NTFS*
Egy munkaállomáson csak NTFS fájlrendszerű partíciók vannak és mégis működik rajta a régi DOS-os fájlkezelőnk. Miért? Milyen problémákkal kell szembenéznünk?

45. *Megosztás megszüntetése*
Milyen különbségeket tapasztalhatunk a megosztás megszüntetése és a DFS hivatkozás megszüntetése között?

46. *DFS hivatkozás?*
Egy szerver két azonos nevű mappájára mutathat e DFS hivatkozás?

Az NTFS fájlrendszerben a hozzáférési jogok

A FAT és az NTFS attribútumai

FAT	*NTFS*
Írásvédett	
Rejtett	
Archiválandó	
Rendszer	
	Tömörített
	Titkosított
	Indexelt

Látható, hogy az NTFS fájlrendszer esetén új attribútumként jelenik meg a *Tömörített*, *Titkosított* és *Indexelt* lehetőség.

A két fájlrendszer között alapvető eltérés, hogy a FAT fájlrendszer nem tárol jogosultsági információkat, az NTFS viszont igen, így használata esetén a fájlrendszer szintjén védhetőek az állományok. A Windows 2000 Professional és Server változata is telepíthető FAT fájlrendszerre, de ekkor az előbbiek miatt, nem tudjuk a fájlrendszer szintjén védeni az állományainkat.

Fontos, hogy ne keverjük össze az attribútumokat és a jogosultságokat. Az *attribútum* csak egy fájlhoz, vagy mappához fűzött jelzés, míg a *jogosultság* a fájlrendszerben tárolt hozzáférés-szabályzó „eszköz". Azért van jelentőségük az attribútumoknak is, hiszen pl. az archiváló programok a megfelelő attribútumból állapítják meg, hogy kell-e menteni egy fájlt vagy sem. A FAT fájlrendszer esetén tetszés szerint állíthatjuk az attribútumokat, az NTFS fájlrendszerben pedig jogosultsági beállításokkal védhetjük az attribútumokat is. Az attribútumokat a FAT és az NTFS is ismeri, de a jogosultsági információkat csak az NTFS képes tárolni.

Elemi jogok az NTFS fájlrendszerben

Az NTFS fájlrendszer a következő 13 elemi jogot ismeri.
Mappa bejárása, fájl végrehajtása
Mappa listázása, adatok olvasása
Attribútumok olvasása
Kiterjesztett attribútumok olvasása
Fájlok létrehozása, adatok írása
Mappák létrehozása, adatok hozzáűzése
Attribútumok írása

Kiterjesztett attribútumok írása
Almappák és fájlok törlése
Törlés
Engedélyek olvasása
Engedélyek módosítása
Saját tulajdonba vétel

A fájlokhoz, mappákhoz való hozzáférési jogosultságok beállításának egyik módja, hogy a védendő objektumok tulajdonságlapján minden érintett csoporthoz (felhasználóhoz) egyesével állítjuk be a fenti elemi jogokat. Ez csak nagyon gyakorlott, a jogosultsági kérdéseket pontosan ismerő rendszergazdáknak javasolt. Sokkal egyszerűbb *az elemi jogokból előre összeállított kombinációk, az ún. standard jogok* használata, amikről a későbbiekben részletesebben olvashatunk.

Ha egy fájlra egyetlen jogot sem kap meg a felhasználó, akkor az annyit jelent, hogy nem fér hozzá. Az elemi jogok neve eléggé beszédes, de fontosságuk miatt az utolsó kettőt vizsgáljuk meg tüzetesebben.

Az engedélyek módosítása jog

Az engedélyek módosítása elemi jog birtokában az adott objektum hozzáférési jogosultságait meg tudjuk változtatni. Például egy felhasználó számára írásvédett mappához nem „jár" az engedélyek módosítása elemi jog, hiszen ha járna, akkor a felhasználó megváltoztathatná a neki nem tetsző állapotot.

A Saját tulajdonba vétel elemi jog

A *Saját tulajdonba vétel* jog megértéséhez gondoljuk át a következő helyzetet. A rendszergazda beállításai után egy mappa tartalmát a diákok csak olvashatják. Az említett mappára nézve a tanárok pedig az utolsó két elemi jog kivételével mindegyikkel rendelkeznek. Ebben a helyzetben a tanár nem veheti el a diáktól a mappa megtekintésének jogát, de a saját tulajdonba vétel jog birtokában önmagát tulajdonossá teheti, majd teljes hozzáférés jogot ad magának és végül azt tesz a kérdéses mappával amit akar. Vegyük észre, hogy *Az engedélyek módosítása* elemi jog birtokában is már teljes hozzáférést adhat magának a felhasználó!

A saját tulajdonba vétel elemi jog bizonyos értelemben a „legerősebb" elemi jog hiszen ezzel a joggal rendelkezve az objektumokat saját tulajdonommá tehetem. Ha egy objektum saját tulajdonomban van, akkor tetszőleges dolgot művelhetek vele, tehát e jog osztogatásával óvatosan kell bánni. Ha tetszőleges jogok mellé a felhasználó megkapja a tulajdonjog átvételének lehetőségét is, akkor gyakorlati szempontból nem túl hatásosak a beállításaink, hiszen a felhasználó a tulajdonjog átvétele után bármit beállíthat önmagának.

Fontos megjegyezni, hogy tulajdonjogot csak átvenni lehet és átadni nem. Ennek megértéséhez gondoljuk át a következő helyzetet. Egy felhasználó tiltott

fájlokat tárol egy mappában. Ha átadható lenne a jog, akkor nyilvánvalóan azt mondaná a tilosban járó felhasználó, hogy a kérdéses fájl „nem az enyém” azaz beállítana egy másik tulajdonost. Ha egy fájl tulajdonjogát szeretnénk átadni, csupán annyit tehetünk, hogy a megfelelő felhasználónak megadjuk a saját tulajdonba vétel jogot. Ezek után kizárólag a felhasználótól függ, hogy él e jogával vagy sem.

A rendszergazda egyik legfontosabb privilégiuma, hogy bármely fájl vagy mappa tulajdonjogát átveheti. Ez a hálózat működése szempontjából már csak azért is fontos, mert a véglegesen eltávozott felhasználó mappáit esetleg csak így távolíthatja el, mert az új fájloknak illetve mappáknak a tulajdonosa a létrehozó felhasználó lesz.

A standard jogok fájlok esetén

Az elemi jogból képezve az alábbi standard hozzáférési jogot találjuk meg fájlok esetén.

Olvasás
Olvasás és végrehajtás
Írás
Módosítás
Teljes hozzáférés

Nézzük meg egy kicsit tüzetesebben, hogy mit is jelentenek ezek a jogok.

Nincs hozzáférés: Ilyen nevű jogosultság nincs ugyan, mert ez az állapot a jogok teljes hiányát jelzi, ez gyakorlatilag a hozzáférés megtagadását jelenti. Ekkor minden elemi jog hiányzik, az ilyen felhasználók látják ugyan a kérdéses fájlt, de nem tehetnek vele semmit.

Egy felhasználó, mint tulajdonos megtagadhatja a hozzáférést fájljaihoz, még a rendszergazdától is. Ebben az esetben egy hozzáférési kísérletre az operációs rendszer a rendszergazdát is figyelmezteti, hogy nincs joga a művelethez. A rendszergazda viszont ezt meg tudja kerülni, hiszen a tulajdonjog átvételével bármit megtehet az állományokkal.[19]

Olvasás: Az *Olvasás* jog esetén megtekinthető a fájl tartalma. A fájl lemásolható, de nem nevezhető át, nem törölhető, nem helyezhető át és tartalma sem módosítható.

Kezdő felhasználók meg szoktak ijedni akkor, ha írásvédett fájlt megnyitnak, módosítanak, majd menteni akarnak és a mellékelten látható üzenetet kapják. Természetesen ez nem azt jelenti, hogy nem menthető a dokumentum, csak annyit, hogy nevét esetleg a mentés helyét meg kell vál-

[19] A tulajdonjog átvétele még a rendszergazdának sem megy nyomtalanul, mert a fájl tulajdonságlapján látható a tulajdonos, és a tulajdonjog csak átvehető, de vissza nem adható.

toztatnunk. A futtatható állományok nem indíthatók el, ha a felhasználó csak olvasás joggal rendelkezik a kérdéses állomány tekintetében.

Olvasás és végrehajtás: Futtatható állományokat már el tudunk indítani a jog birtokában, szöveges dokumentumokra pedig ez a jog gyakorlatilag az olvasási jogot jelenti. Ha egy felhasználónak megadtuk az olvasás és végrehajtás jogot, akkor a jogok között automatikusan „kiválasztódik" az olvasási jog is.

Írás: Ha csak az *Írás* joggal rendelkezik egy felhasználó, akkor nem nézhet bele egy szövegfájlba, nem indíthat futtatható állományt, nem is törölhet állományokat, viszont beállíthatja a kérdéses állomány attribútumait. Sokkal használhatóbb állapothoz jutunk, ha az írási jog mellé az olvasási jogot is megadjuk. Ekkor egy szöveges dokumentumot már meg tudunk nyitni, a változtatásokat el tudjuk menteni, de a fájlt törölni nem tudjuk[20].

Módosítás: Ez a jog majdnem mindent megenged. A fájl tartalma megtekinthető, módosítható, a fájl átnevezhető, áthelyezhető és törölhető is. Látszólag a módosítás jog birtokában bármit megtehetünk. Lényeges, hogy nem változtathatjuk meg más felhasználóknak az adott fájllal kapcsolatos jogosultságait és a tulajdonjogot sem vehetjük át.

Teljes hozzáférés: Az összes elemi jogot tartalmazza. Ezen jog birtokában valóban minden megtehető a kérdéses állománnyal.

Ezek a fájlokra adott jogok az esetek legnagyobb részében elegendőek. Az elemi jogok felhasználásával azonban újabb kombinációkat is előállíthatunk. Ezt a lehetőséget csak akkor alkalmazzuk, ha nem felelnek meg az előre összeállított változatok. Kellően át nem gondolt kombinációkat állítva áttekinthetetlenné válhat rendszerünk. Végezetül ne feledkezzünk meg az NTFS egyik adatvédelmi erősségéről, a titkosításról, hiszen hiába adunk például olvasási jogot a felhasználóknak, ha a fájl titkosított.

Standard hozzáférési jogok könyvtárak esetén

Olvasás
Olvasás és végrehajtás
Mappa tartalmának listázása
Írás
Módosítás
Teljes hozzáférés

Tekintsük át röviden, hogy melyik mit is jelent.

Nincs hozzáférés: A fájloknál látottak szerint ez az eset a jogok teljes hiányát jelzi. Látjuk a mappát és ezzel ki is merültek lehetőségeink. Még bele sem tudunk nézni.

[20] Ha egy TXT fájl tartalmát töröljük, akkor 0 bájt hosszal is menthetjük, de a fájl nevét a tartalomjegyzékből nem tüntethetjük el.

Olvasás: Látható a mappa, megnézhető a tartalma, de nem törölhető és újabb objektum sem hozható létre a mappán belül, a futtatható fájlok sem indíthatók el. A mappa átnevezése ebben az esetben is megengedett. A mappa által tartalmazott fájlok és almappák beállítástól függően örökölhetik a szülő jogait vagy egyedi jogok oszthatók részükre.

Olvasás és végrehajtás: Az előbbiekhez még hozzáadódik a fájlok futatásának joga is.

Mappa tartalmának listázása: Ugyanazokat az elemi jogokat tartalmazza, mint az olvasás és végrehajtás jog.

Írás: Ha csak ezzel a joggal rendelkezik egy felhasználó, akkor nem nézheti meg a mappa tartalmát, nem is törölheti a kérdéses mappát, viszont beállíthatja az adott mappa attribútumait. Lényeges tudni, hogy új mappákat és fájlokat létrehozhat a felhasználó a kérdéses mappán belül.

Felmerül a kérdés, hogy hogyan hiszen hozzá sem fér a mappához? Ilyen jogosultságú mappába természetesen nem is menthetünk például egy szövegszerkesztőből, hiszen a mentéshez el kellene menni a kérdéses mappáig és az írás jog birtokában ez lehetetlen. Közvetlen a kérdéses mappán belül nem is hozható létre új objektum, de egy más helyen található fájl vagy mappa már elhelyezhető az említett mappában. Sőt, ha felhasználónk egyszer már elhelyezett az említett mappában egy fájlt vagy almappát, akkor azt nem törölheti és nem is módosíthatja[21].

Módosítás: Ez a jog a fájloknál látottakhoz hasonlóan majdnem mindent megenged. A mappa tartalma megtekinthető, módosítható, a mappa átnevezhető, áthelyezhető és törölhető is. Nem változtathatjuk meg más felhasználóknak az adott fájllal kapcsolatos jogosultságait.

Teljes hozzáférés: Az összes elemi jogot tartalmazza. Ezen jog birtokában már valóban mindent megtehetünk a kérdéses mappával.

A fájloknál látottak szerint mappákra is összeállíthatunk új jogosultságokat az elemi jogokból, de ezzel a lehetőséggel óvatosan bánjunk.

Fájlok és mappák másolása, mozgatása

Az alábbiakban azt vizsgáljuk meg, hogy hogyan alakulnak a jogok új mappa, illetve fájl létrehozásakor, mappák, fájlok másolásakor és mozgatásakor.

Új mappa létrehozásakor az új mappa örökli a szülő mappa jogait. Másolásnál a mappák a célmappa jogosultságait veszik át. Áthelyezésnél két eset lehetséges. Ha partíción belül helyezünk át, akkor a mappa megtartja jogosultságait, ha partíciók között mozgatunk, akkor a célállomás jogait kapja meg a mappa.

Fájlok másolásánál illetve mozgatásánál hasonló a helyzet. A fájl vagy megtartja eredeti jogosultságait, vagy a célmappában érvényes jogosultságokat

[21] Ez az ideális dolgozatgyűjtő mappa.

veszi át. Fontos tudni, hogy FAT fájlrendszert tartalmazó partícióra másolva (mozgatva) bármit az a felhasználó szempontjából teljes hozzáférést jelent, hiszen a FAT fájlrendszer nem képes jogosultsági információk tárolására.

A megosztásoknál látott problémával itt az NTFS jogosultságok állításánál is találkozunk, ha a felhasználó több helyről szerzi be a jogosultságait. Nézzük meg, hogy az NTFS fájlrendszer jogosultságaival kapcsolatban mi lesz az effektív jog. Példaként tekintsük át a következő esetet. Marcipán Miklós nevű diákunknak a *diák* csoport tagjaként *olvasás* joga van a *versenyfeladatokat* tartalmazó mappához. A *versenyzők* csoport tagjaként viszont *teljes hozzáférés* joga van ugyanehhez a mappához. Mit tehet a felhasználó a kérdéses mappával? A kérdés megválaszolásához vizsgáljuk meg a következő táblázatot!

Diák csoport	*Versenyzők csoport*	*Effektív jog*
Olvasás	Módosítás	Módosítás
Módosítás	Olvasás	Módosítás
Teljes hozzáférés	Módosítás	Teljes hozzáférés
Módosítás	Nincs hozzáférés	Nincs hozzáférés
Módosítás	– (nem tag)	Módosítás

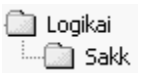
A megosztásokhoz hasonlóan NTFS jogok esetén is azt állapíthatjuk meg, hogy *a különböző utakon kapott jogok egyesítése lesz az effektív jog*. Itt is az egyetlen kivétel a nincs hozzáférés. Ha egyetlen úton sem kap hozzáférési jogot a felhasználó az adott objektumhoz, akkor az mindennél erősebb, azaz az effektív jog is nincs hozzáférés lesz.

A standard jogok összefoglalása

	Teljes hozzáférés	*Módosítás*	*Olvasás és végrehajtás*	*Olvasás*	*Írás*
Mappa átjárása /Fájl végrehajtása	×	×	×		
Mappa listázása /Adatok olvasása	×	×	×	×	
Attribútumok olvasása	×	×	×	×	
Kiterjesztett attribútumok olvasása	×	×	×	×	
Fájlok létrehozása /Adatok írása	×	×			×
Mappák létrehozása /Adat hozzáfűzése	×	×			×
Attribútumok írása	×	×			×
Bővített attribútumok	×	×			×

írása					
Almappák és fájlok törlése	×				
Törlés	×	×			
Olvasási engedélyek	×	×	×	×	×
Engedélyek módosítása	×				
Saját tulajdonba vétel	×				

Jogok öröklődése



Mit mondhatunk az ábra szerinti elrendezésben a *sakk* nevű mappáról, ha a logikai nevű mappára *olvasási* jogokat állítunk be? Erre a kérdésre a válasz a *sakk* mappa jogosultsági beállításától függ.

Az öröklődést az almappánál kell beállítani és élő kapcsolatot jelent. Ha módosítjuk a szülőmappa beállításait, akkor a megfelelő almappákra is automatikusan életbe lépnek a változtatások. Ha töröljük az alapértelmezett öröklődés engedélyezését a *sakk* nevű mappánál, akkor a *sakk* nevű mappa jogosultságairól semmit nem tudunk mondani.

Tekintsük át honnan kaphat egy felhasználó hozzáférési jogosultságokat egy mappához!

Megosztás: Különböző úton kapott jogok esetén az effektív jog a jogok egyesítése a nincs hozzáférés kivételével.

NTFS fájlrendszer: Különböző úton kapott jogok esetén az effektív jog a jogok egyesítése a nincs hozzáférés kivételével.

Mi lesz a felhasználó effektív joga, ha az NTFS fájlrendszer útján és megosztások útján is jogokat kap egy mappához? Például a *játék* nevű mappát megosztottuk szintén *játék* megosztásnéven. Kakaó Kázmér nevű felhasználónknak *olvasás* joga van a *játék* nevű megosztáshoz és *módosítás* joga van a *játék* nevű mappához az NTFS partíción. Mi lesz az effektív jog, ha megosztásként közelít a mappához? A kérdés eldöntéséhez vizsgáljuk meg a következő táblázatot!

Megosztás	*NTFS*	*Effektív jog*
Olvasás	Módosítás	Olvasás
Módosítás	Olvasás	Olvasás
Teljes hozzáférés	Módosítás	Módosítás
Módosítás	Nincs hozzáférés	Nincs hozzáférés
Módosítás	– (nem kapott jogot)	Nincs hozzáférés
– (nem kapott jogot)	Módosítás	Nincs hozzáférés

A táblázatot megvizsgálva megállapítható, hogy a megosztási és NTFS jogokból adódó effektív jog kivétel nélkül *a jogok metszete lesz*.

Összefoglalásként tekintsük át a következő táblázatot! A táblázat adatai egységesen a *játék* nevű mappára vonatkoznak és feltételezzük, hogy a kérdéses felhasználó mind a négy említett csoportnak tagja.

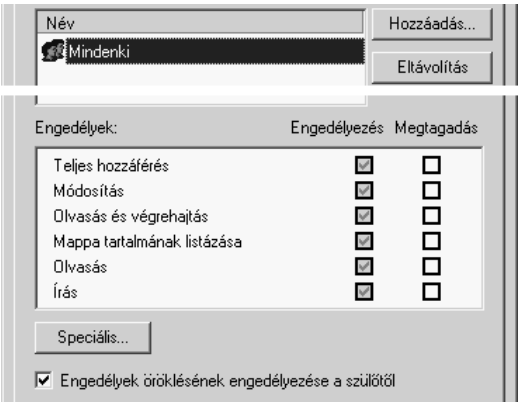
Megosztás		*NTFS*		*Effektív*
Diákok csop.	Info csop.	Játékos csop.	Szervező csop.	
Olvasás	Módosítás	Írás	Teljes	Módosítás
Nincs	Módosítás	Teljes	Teljes	Nincs

Jogok kialakítása hálózatos rendszerben

A megosztási jogokról és az NTFS jogokról írottak szerverek és munkaállomások esetén is érvényesek. Szerverek elé nem szokás leültetni a felhasználót, viszont a munkaállomások elé igen. Így előállhat az az érdekes eset, hogy más joga lesz a felhasználónak, ha a gép előtt ül és más, ha hálózaton át éri el a kérdéses mappát.

Célszerű *megosztásként* mindenkinek teljes hozzáférés jogot adni (alapértelmezésként automatikus) és az *NTFS fájlrendszerben* szabályozni a hozzáférési jogokat. Mivel a megosztási és az NTFS jogok közül a „gyengébb” érvényes így gyakorlatilag az NTFS fájlrendszer útján szabályozzuk a hozzáférést. Tehát mindegy, hogy milyen úton éri el a felhasználó a kérdéses mappát mindig azonos jogai lesznek. A rendszer áttekinthetősége érdekében célszerű betartani az előbb vázolt módszert a jogok osztására a szerveren is.

Nézzük meg hogyan állíthatjuk be a fájlok és mappák jogosultságait! Kattintsunk az egér jobb gombjával a kérdéses fájlra vagy mappára. A megjelenő helyi menüből válasszuk a *Tulajdonságok* pontot. A megjelenő panel *Biztonság* fülére lesz szükségünk és máris hozzákezdhetünk a jogosultságok beállításához.



A mellékelt ábra egy könyvtár jogosultságait ábrázolja. Fájlok esetén ez annyiban más, hogy az engedélyek listájában a fájloknál tárgyalt elemek jelennek meg.

Vizsgáljuk meg egy kicsit közelebbről az engedélyek öröklődését! Ha ezt bejelöltük, akkor a kérdéses mappánk átveszi a szülőmappára beállított jogosultságokat. Ezt kiegészíthetjük saját belátásunk szerint. Ha ezek után úgy döntünk,

hogy az öröklődést mégsem engedélyezzük, akkor csak a pipát kell eltávolítanunk. Ebben az esetben a következő lehetőségeket ajánlja fel a rendszer.

Másolás: Ekkor a szülőmappa jogosultsági beállításai átmásolódnak, ami annyit jelent, hogy azonos beállításokat látunk, mint az öröklődés engedélyezésekor, de már szerkeszthető állapotban.

Eltávolítás: Ekkor az összes szülőtől öröklött jogosultság eltávolításra kerül, csak az általunk kiegészítésként beállított jogosultságok maradnak meg. Ha ilyen kiegészítés nem volt, akkor a rendszer figyelmeztet arra, hogy a jogosultsági lista üres, tehát senki sem fog hozzáférni a mappához. Ilyen esetben még a rendszergazda is a hozzáférés megtagadva jelzést fogja kapni, de természetesen a rendszergazda jogosult a hozzáférési beállításokat megváltoztatni.

A kiválasztott felhasználó jogait a megfelelő jogosultságok *Engedélyezés és megtagadás* oszlopában a pipák elhelyezésével vagy eltávolításával szabályozhatjuk. Amíg az öröklődés érvényben van, addig az engedélyezés oszlop elemeit nem tudjuk megváltoztatni, de egy engedély megtagadását bejelölhetjük. Ha szeretnénk eltávolítani egy nevet a jogosultak listájából, akkor a kérdéses név kijelölése után csak az eltávolítás gombra kell kattintanunk. Ha az összes nevet eltávolítottuk a névlistából, akkor a rendszer figyelmeztet, hogy senkinek sem lesz hozzáférése a kérdéses mappához.

A standard jogokon túl

Ha standard jogok nem felelnek meg, és új jogokat szeretnék előállítani az elemi jogokból, akkor azt a *Speciális* gombra kattintva tehetjük meg. A megjelenő névlistából a kiválasztott elemre duplán kattintva már válogathatunk is az elemi jogosultságok között. A speciális gomb lenyomása után megjelenő panel tulajdonos fülén nézhető meg, hogy ki a mappa vagy fájl jelenlegi tulajdonosa és megfelelő jogosultságok birtokában átvehetjük a kiválasztott objektum tulajdonjogát. Ha eredetileg nem volt hozzáférésünk a kérdéses objektumhoz, akkor is átvehető a tulajdonjog, de ekkor figyelmeztet a rendszer, hogy az összes jogosultsági beállítását elveszti az adott objektum. A tulajdonjog átvételénél eldönthető, hogy csak a mappa tulajdonjogát szeretnénk átvenni vagy az összes almappáét is.

Ha új nevet szeretnénk felvenni a jogosultak közé, akkor a *Hozzáadás* gombra kattintva tehetjük ezt meg. Ahogy a csoporttagság beállításánál láttuk megadható, hogy honnan szeretnénk válogatni, majd a megjelenő névlistából válogathatjuk ki a megfelelő felhasználókat és csoportokat. Végül az újonnan kiválasztott nevekre is állítsuk be a hozzáférési jogokat.

Feladatok

47. *„Elérhetetlen” megosztás*
Hálózatunk egyik munkaállomásának egy megosztásához Mekk Eleknek nincs hozzáférési joga megosztásként. Elek barátunk a hálózat ismeretében viszont megoldotta hozzáférését. Hogyan? Tegyük fel, hogy Elek barátunk azonosítója csak „vendég” jogú, nem tud más jelszavakat és nem használt illegális eszközöket!

48. *Hozzáférés megtagadva*
Egy felhasználónak csak olvasási joga van egy mappára. Milyen különbséget tapasztalhatunk a minden jog megtagadása és a hozzáférési listából való törlés között?

49. *Home könyvtárak áthelyezése*
Home könyvtárakat tároló winchesterünk kezd betelni, viszont a másik szerver merevlemezén van bőven hely. Átmozgatjuk a home könyvtárakat. Mi a baj?

50. *Nyom nélkül?*
Kollégánk a dolgozatok mappára úgy állította be a jogosultságokat, hogy kizárólag ő férjen hozzá, más ne. A rendszergazdai jogokkal rendelkező diák meg tudja e nézni a dolgozatok kérdéseit? Lesz ennek nyoma?

51. *Helyi és hálózati elérés*
Hogyan kell beállítani a jogosultságokat egy munkaállomáson, ha azt szeretnénk, hogy egy mappára nézve több joga legyen a felhasználónak, ha leül a munkaállomáshoz, mintha hálózaton át közelít? Mi a teendő, ha a fordított esetet szeretnénk megvalósítani?

52. *Effektív jogok*
Adjuk meg Mézga Géza effektív jogait az alábbi táblázatban. A megadott nevek csoportokat takarnak és ahol nincs megadva jog ott nem tagja a csoportnak Mézga Géza.

NTFS jogok		*Megosztási jogok*		*Effektív*
9b	tagozat	9b	tagozat	
Olvas	módosít	olvas	teljes	
Nincs	teljes	olvas	olvas	
	teljes	olvas	olvas	

Nyomtatókezelés

Nyomtató és nyomtatási sor

Elsőként két fogalmat szükséges tisztázni a félreértések elkerülése végett.

Printer: az operációs rendszer és a hardvereszköz közötti felület, egy logikai nyomtató. Valójában ezt szokás *nyomtatási sor* névvel illetni.

Printer device: ez a hardvereszköz, ami fizikailag a nyomtatást végzi.

Legtöbb esetben *egy printer (nyomtatási sor) tartozik egy nyomtató eszközhöz*, ezért látszólag félreértések nélkül keveredhetnek a fogalmak. A nyomtatási sor és a nyomtató eszköz egymáshoz rendelése azonban nem mindig jelent kölcsönösen egyértelmű kapcsolatot. Példaként tekintsünk át két egyszerű esetet. Egyik esetben egy nyomtatási sor két nyomtató eszközre dolgozik, míg a másik esetben két nyomtatási sor egy nyomtató eszközre nyomtat.

Egy nyomtatási sor két nyomtatóeszközre nyomtat. Ez a változat használatos abban az esetben, ha rengeteg nyomtatási kérés érkezik egy adott géphez és gyorsítani szeretnénk a nyomtatás folyamatán. Ilyenkor a nyomtatási sor megpróbálja szétosztani a terhelést a két eszköz között, és váltakozva küldi a nyomtatnivaló dokumentumokat az eszközökhöz. Egy dokumentumot természetesen nem fog szétosztani a nyomtatási sor az eszközök között, hanem teljes egészében egyik eszközre küldi. E lehetőség használatához szükséges, hogy a, nyomtatási sorral képes legyen együttműködni mindkét eszköz. A felhasználók an??nyit fognak észlelni, hogy gyorsabban készülnek el a dokumentumaik, de továbbra is csak egy nyomtatót fognak látni a programjaik.

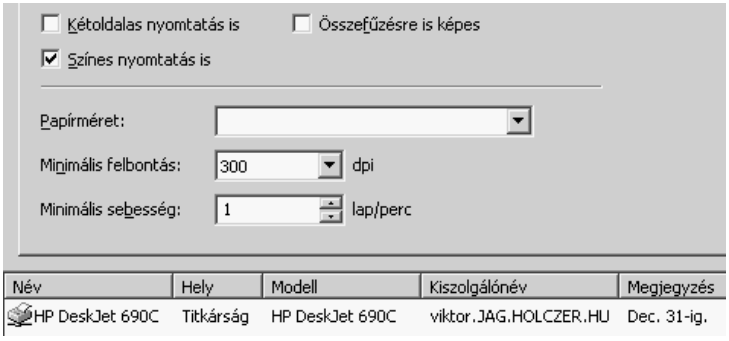
Két nyomtatási sor egy eszközt irányít. A következő típusú problémák megoldására használható ez a módszer. A számítógéphez egy nyomtató eszköz van illesztve, de szeretnénk, ha a főnök dokumentumai nem állnának be a nyomtatási sorba, hanem megelőznék a beosztottak sorban álló dokumentumait. Ehhez a vezérlőpulton kétszer kell telepítenünk ugyanazt a nyomtatót, ugyanarra a portra, majd a különböző nyomtatókhoz különböző prioritásokat kell rendelni. A vezetők által használt nyomtatási sor fogja a nagyobb prioritást kapni.

Ekkor az alkalmazottak dokumentumának nyomtatása nem fog megszakadni, hanem teljes egészében el fog készülni a nyomat. Ha azonban jön egy nyomtatási kérés a vezetők által használt nyomtatási sorból, akkor ez a kérés fog előbb teljesülni és nem a régebben sorban álló alkalmazotti kérés. Ennek a lehetőségnek a használatához a nyomtatási jogosultságokat is helyesen kell beállítanunk, hogy mindenki a megfelelő nyomtatási sorokba nyomtathasson. A felhasználók programjai két nyomtatót látnak miközben csak egyetlen eszköz van a számítógéphez kapcsolva. Azoknál a nyomtatóknál melyeket nem a vezérlő-

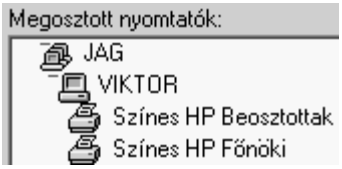
pulton át kell telepíteni, hanem pl. egy setup.exe programmal kell elindítani a telepítést előfordulhat, hogy nem használható ez a lehetőség.

A nyomtató telepítése

A vezérlőpult nyomtatók ablakában a nyomtató hozzáadása ikonra kattintva indul a telepítést irányító varázsló. Elsőként azt kell eldöntenünk, hogy hol található a hardvereszköz. Saját gépünkhöz kötve vagy egy másik számítógéphez kötve. Ha a hálózati nyomtató lehetőséget választjuk, akkor a tovább gombra kattintva meg kell adni, hogy hol található a csatlakoztatni kívánt nyomtató.



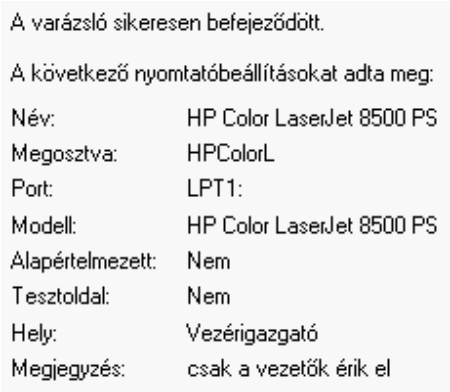
Ha a *Címtárban való keresést* választjuk, akkor ki is használhatjuk az active directory azon képességét, hogy sokféle szempont alapján lehet keresni benne az objektumokat. A fenti ábra szerint egy legalább 300 dpi felbontású színes nyomtatót kerestünk. A találatban az active directory-tól azt is megtudjuk, hogy hol található a nyomtató.



Ha *Megosztott nyomtatók közötti tallózás lehetőséget* választjuk, akkor megjelenik a számunkra elérhető számítógépek listája. A listát tallózva megkeressük a számunkra érdekes számítógépet és a + jelre duplán kattintva láthatóvá tehetjük a kiválasztott gépen található megosztott nyomtatót, ha van. Itt az OK gombra kattintsunk és a következő ablakban csak azt kell eldöntenünk, hogy ez a nyomtató legyen e az alapértelmezett a programok számára. Ekkor a tovább gombra kattintva már csak egy üzenetet kapunk, hogy a nyomtató telepítése sikerült.

A telepítés kezdetén a *Helyi nyomtató* lehetőséget választva egy kicsit hosszabb út áll előttünk. A tovább gombra kattintás után el kell döntenünk, hogy melyik portra telepítjük a nyomtatót. A következő lépésben meg kel adnunk a nyomtató gyártóját és típusát a Windows 2000 által ismert nyomtatók közül, vagy a nyomtatóhoz mellékelt meghajtó programot tartalmazó CD-t kell megadni a telepítő varázsló számára, majd megadhatjuk, hogy alapértelmezett lesz a nyomtatónk vagy sem. Ezután meg kell határozni, hogy megosztjuk-e az

új nyomtatót és ha igen, akkor milyen néven. A következő ablakban a felhasználók tájékozódását segítő hely és megjegyzés adatokat adhatjuk meg, majd eldönthetjük, hogy kérjük e a tesztoldal nyomtatását vagy sem. Utolsó lépésként a sikeres befejezésről kapunk értesítést és összefoglalva láthatjuk a nyomtatóval kapcsolatos beállításainkat.

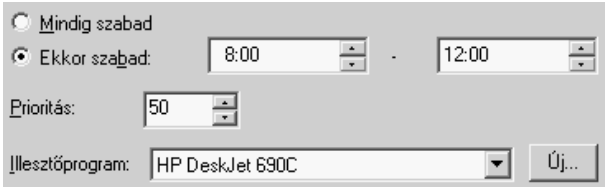


A nyomtató tulajdonságai

A nyomtató további beállítását a nyomtató tulajdonságlapján kell elvégeznünk. A tulajdonságlap *Megosztás* nevű fülének *További illesztőprogramok* gombjára kattintva adhatjuk meg, hogy mely egyéb operációs rendszerű gépek számára álljon rendelkezésre a nyomtató illesztőprogramja. Természetesen ekkor rendelkeznünk kell a másik operációs rendszerhez való illesztőprogrammal, ami rajta lehet a Windows 2000 Server CD-n, vagy bármely más helyen. A megosztás fülön találjuk a ☑ *Listázva itt: Címtár* lehetőséget. Csak ennek a beállításnak a megléte esetén tudják a felhasználók megkeresni a nyomtatót az active directory segítségével. A megosztott nyomtatónak tallózás útján való elérése természetesen ennek ellenére is megtehető.

A *Portok* nevű fülön a *Nyomtatók egyesítésének engedélyezése* lehetőség kiválasztásával tehetjük lehetővé, hogy egyetlen nyomtatási sor két (vagy több) fizikai nyomtatóeszközre tudjon dolgozni. Ekkor meg kell nevezni, hogy melyik portra van kötve a másik nyomtató.

A tulajdonságlap *Speciális* fülének egy részletét érdemes megnézni közelebbről. Meghatározhatjuk a nyomtató elérhetőségét időben. A nyomtató lehet állandóan elérhető vagy megadhatunk egy összefüggő időtartamot óra-perc pontossággal. Előállíthatunk olyan helyzetet, hogy egyik felhasználó nem tud



nyomtatni adott időben egy eszközre, míg a másik ugyanarra az eszközre igen. Ehhez a két sor egy eszköz változatot kell választanunk. A két nyomtatási sorra külön-külön megfelelően állítsuk be a jogokat és az elérhetőség idejét, beállíthatjuk a nyomtatási sor prioritását is. A két sor egy eszköz változatnál a nagyobb prioritású sorban várakozó dokumentumok előbb érik el a nyomtató eszközt, de természetesen a dokumentumok nem keveredhetnek.

A nyomtatással kapcsolatos jogosultságok

A nyomtatókra nem alkalmazhatóak a mappáknál és fájloknál használt jogok, hiszen például az olvasás jog nyomtató esetén értelmetlen lenne. A jogosultságok a következők:

Nem elérhető: A mappákhoz hasonlóan a nyomtatók esetén sem létezik ilyen nevű jogosultság. Ez minden jog hiányát jelzi.

Nyomtatás: Ezen jog birtokában nyomtathatunk a megfelelő nyomtatóra, de mást nem tehetünk. Meg sem szakíthatjuk a nyomtatást, ha meggondoltuk magunkat.

Dokumentum kezelése: Csupán e jog birtokán még semmit sem tehetünk. Ha legalább még egy nyomtatás jogunk is van, akkor a nyomtatási sor tartalmát is módosíthatjuk. Akár mások sorban álló dokumentumait is törölhetjük a nyomtatási sorból. A sorban álló dokumentumok őrzik eredeti jogosultságaikat. Ez azt jelenti, hogy ha nem volt jogunk törölni a nyomtatási sorból és egy felhasználó elküldött egy nyomtatást, majd ezután kaptunk dokumentumkezelési jogot, akkor ezt a kérdéses munkát nem törölhetjük a nyomtatási sorból.

Nyomtatókezelés: Ennek a jognak a birtokában már megváltoztathatjuk a felhasználók nyomtatással kapcsolatos jogosultságait. Mások munkáinak nyomtatási sorból való törlési kísérletére *A hozzáférés megtagadva* hibajelzést kapjuk, hiszen a nyomtatókezelés joghoz nem jár automatikusan a dokumentumkezelés jog. Természetesen a nyomtatókezelés jog birtokában megadhatjuk magunknak a dokumentumkezelési jogot is. Ebben az értelemben tehát a nyomtatókezelés jog jelenti a mappáknál látott teljes hozzáférés nyomtatásjogi megfelelőjét.

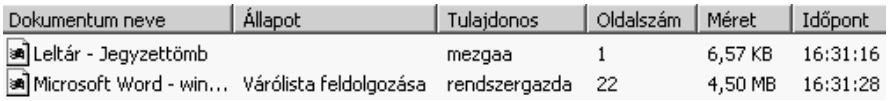
A nyomtatási jogok beállításához a vezérlőpulton át válasszuk ki a kérdéses nyomtatót, majd jobb gombbal kattintsunk rá. A megjelenő menüből válasszuk a *Tulajdonság* pontot. Az előálló ablakban válasszuk a *Biztonság* fület és elkezdhetjük beállítani a jogokat.

A kiválasztott felhasználó jogainak változtatását az NTFS jogok állításánál látottakkal azonos módon tehetjük meg, csak a beállítható jogosultságok lesznek mások. A jogosultak listájában látunk egy létrehozó tulajdonos nevű csoportot, mely a dokumentumok kezelése joggal rendelkezik. Ez annyit jelent, hogy a saját munkáit mindenki kiveheti a nyomtatási sorból annak ellenére, hogy csak nyomtatás jogot kapott. Egymás várakozó dokumentumait láthatják a felhasználók, de mindenki csak a sajátját kezelheti a nyomtatási sorban, feltéve, hogy nem rendelkeztünk másképpen.

A nyomtatási sor tartalma

A nyomtatási sor tartalma a nyomtatóra való dupla kattintással érhető el.

A nyomtatási sorban láthatjuk a dokumentum fontosabb adatait. A kép szerinti várólista feldolgozása állapot arra utal, hogy az alkalmazás – itt a Word – éppen küldi a nyomtatandó oldalakat a nyomtatási sor felé. A nyomtatást végző gépen ezen idő alatt látjuk a tálca jobb szélén a lapokat „dobáló" nyomtatóikont. Ha egy munkaállomásról nyomtatunk egy megosztott nyomtatóra, akkor a várólista feldolgozása állapot megszűnése után már akár ki is kapcsolhatjuk a munkaállomást.



Dokumentum neve	Állapot	Tulajdonos	Oldalszám	Méret	Időpont
Leltár - Jegyzettömb		mezgaa	1	6,57 KB	16:31:16
Microsoft Word - win...	Várólista feldolgozása	rendszergazda	22	4,50 MB	16:31:28

Ha a várólista feldolgozása állapot megszűnt, akkor a nyomtatásra váró dokumentum már a ténylegesen nyomtatást végző gépen van. A méretként jelzett érték nem a mentett fájl mérete a lemezen, hanem a nyomtatási sorban várakozó, a nyomtató számára értelmezhető adathalmaz mérete. A sorból kiválasztva egy dokumentumot, majd a dokumentum menüt választva a felfüggesztés, folytatás, újraindítás és megszakítás pontokkal lehetőségünk van - jogosultságainknak megfelelően – a dokumentumot kezelni.

Feladatok

53. *Dokumentumkezelési jog*

Hibás beállítások miatt a diákok egymás dokumentumait törölték a nyomtatási sorból, ezért mindenféle dokumentumkezelési jogot visszavont a rendszergazda. Mi lehet ezzel a beállítással a baj?

54. *Megosztott nyomtató*

Kollégánk megosztotta irodájának új nyomtatóját és mi telepítettük is saját irodánk gépére hálózati nyomtatóként. A munkaidő végén sürgős nyomtatnivalónk akadt. A tálcán meg is jelenik a nyomtató ikonja, rövid várakozás után pedig egy kérdőjel jelenik meg az ikonon. Az ikonra duplán kattintva előhívjuk a nyomtatási sor tartalmát, és azt látjuk, hogy „hiba…." Mi lehet a valószínű ok?

55. *Iskolai nyomtatók*

Egy iskola számítógéptermében találunk 2 színes tintasugaras nyomtatót és 1 fekete-fehér lézernyomtatót. Tegyünk javaslatot a nyomtatók beállításaira, feltéve, hogy az iskolában nincs több nyomtató és a tanári szobákban és az igazgatói irodában is van számítógép.

56. *Mókás Márton*

Mókás Márton diák a tanári gép megosztott nyomtatójára egy üres oldal nyomtatását elküldte ötvenszer. Kollégánk jelezte, hogy nem tudta leállítani a felesleges nyomtatást. Mit kell tennünk, hogy ezt máskor megtehesse?

57. *Lézernyomtató*

Rendszergazda kollégánk elkezdett rendet tenni a nyomtatási jogok terén és elkezdte beállítani a 9.a, 9.b… osztályokra a lézernyomtatónál a nyomtatási jogok megtagadását. Mi lehet ezzel az eljárással a baj?

Naplózás

A naplózás alapjai

A naplózás célja, hogy a szerver illetve a hálózat bizonyos történéseit körülményeivel együtt egy fájlban rögzítse és ezzel lehetővé tegye a működés későbbi elemzését.

Rendszerünk karbantartásában segíthet a jól beállított naplózás. A Windows 2000 az alábbi naplókat kezeli.

Rendszer
Alkalmazás
Biztonság
DNS server
Fájlreplikációs szolgáltatás
Directory Service

A Windows 2000 server változata mind a hat felsorolt naplót kezeli, míg a professional változat csak a Rendszer, Biztonság és az Alkalmazások naplóit kezeli.

A rendszer naplózása

Ebben a naplóban találjuk meg az operációs rendszer üzeneteit. Ilyen üzenetek például *a naplózó szolgáltatás elindult*, egy *szolgáltatás leállt*, *nyomtatót sikeresen telepítettük*, *hibás blokk* a CD-ROM-on és különböző eszközhibák, egy winchester kapacitásának határán van. Ezeknek az eseményeknek a naplózását nem kell külön előírni, mert ezeket az eseményeket automatikusan naplózza a rendszer.

Az alkalmazás napló

Az alkalmazás naplóba kerülnek az alkalmazások hibaüzenetei és figyelmeztetései. Például itt találjuk meg a Windows-hoz írt vírusellenőrzők üzeneteit, de itt találjuk meg a lemezellenőrzés eredményét és a közismert DrWatson üzeneteit is. Itt találunk bejegyzést ha a belépés folyamán probléma adódik például a profil elérésével vagy a házirend feldolgozásával. Ezt a naplózást sem kell külön előírni, a rendszer automatikusan kezeli.

A biztonság

Ez a napló alapértelmezés szerint üres, alapértelmezésben tehát nincs biztonsággal kapcsolatos naplózás. A naplózás beállítását *Csoportházirend Windows beállításainál* a *Biztonsági beállításoknál* a *Helyi házirendben* a *Naplórendnél* végezhetjük el.

A következő események naplózását írhatjuk elő: bejelentkezés, címtárszolgáltatás-hozzáférés, fiókbejelentkezés, fiókkezelés, folyamatok nyomon követése, házirendváltozás, objektum-hozzáférés, rendszeresemények, rendszerjogok használata. A naplózandó eseményekből minden esetben két típust találunk. Egy esemény lehet *Sikeres* vagy *Sikertelen*.

Megjegyzendő, hogy a naplófájlba rögtön bekerülnek a bejegyzések a kiválasztott esemény sikeres vagy sikertelen voltáról az objektum-hozzáférés kivételével. Az *Objektum-hozzáférés* naplózását a naplórendnél csak engedélyezni kell és a konkrétan naplózandó esemény beállítása a megfelelő objektum tulajdonságlapján történik meg. Ha a naplózást az objektum tulajdonságlapján bekapcsoltuk, de még nem engedélyeztük a házirendben, akkor az operációs rendszer egy üzenettel figyelmeztet bennünket erre. Ekkor természetesen hiába állítottuk be a naplózást, hiszen a biztonsági napló mindaddig üres marad, amíg házirendben nem engedélyezzük.

Egy mappa esetén a naplózást a következő módon állíthatjuk be. A mappára a jobb egérgombbal kattintunk, majd a megjelenő helyi menüből a *Tulajdonságok* pontot választjuk. A *Biztonság* fül *Speciális* nevű gombjára kattintunk és az előbukkanó panelen a *Naplózás* fület választjuk és nekiláthatunk a naplózás beállításának. A *hozzáadás* gomb alatt vehetünk fel új elemet a névlistába, az *eltávolítás* gombbal pedig csökkenthetjük a névlista méretét.

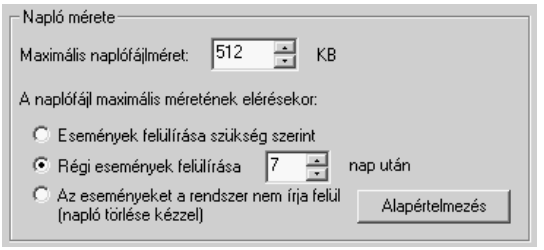
Természetesen meg kell határozni, hogy mit szeretnénk naplózni. A következő lehetőségek közül választhatunk: Mappa bejárása, fájl végrehajtása, mappa listázása, adatok olvasása, attribútumok olvasása, kiterjesztett attribútumok olvasása, fájlok létrehozása, adatok írása, mappák létrehozása, adatok hozzáfűzése, attribútumok írása, kiterjesztett attribútumok írása, almappák és fájlok törlése, törlés, engedélyek olvasása, engedélyek módosítása, saját tulajdonba vétel. A felsorolt összes eseményre a sikeres és sikertelen változat külön naplózható. Fájlok és mappák esetén a naplózás beállítása gyakorlatilag annyiban tér el, hogy a mappák esetén eldönthető, hogy csak az adott mappára vonatkozzon a beállítás vagy az alatta álló objektumokra is.

Hogyan öröklődnek a naplózási beállítások másolásnál és mozgatásnál? *Másolásnál* a mappák a célmappa naplózási beállításait veszik át. *Áthelyezésnél* két eset lehetséges. Ha partíción belül helyezünk át, akkor a mappa megtartja eredeti naplózási beállításait, ha partíciók között mozgatunk, akkor a célmappa beállításait kapja meg a mappa. Fájlok másolásánál és mozgatásánál is azonos változnak a naplózás beállításai. Ez a módszer a naplózási beállítások öröklődésére teljesen összhangban van az NTFS jogok öröklődésével.

A naplózás beállításai

A naplózás beállításait jól át kell gondolni, mert egy kellően át nem gondolt beállítással nagy terhet akaszthatunk szerverünk nyakába munkaigény és

lemezterület tekintetében is. Előnyösebbnek tűnik, ha szerverünk a hálózat kiszolgálásával foglalkozik és nem a naplózással.



A *Start* menü *Programok* pontjának *Felügyeleti eszközök* pontja alatt találjuk az *Eseménynapló* nevű alkalmazást, amivel a naplóállományokat megtekinthetjük és a naplók viselkedését szabályozó beállításokat tehetünk meg. Az eseménynapló alkalmazásban a kiválasztott napló tulajdonságlapját választva a mellékelt ábra szerinti képet láthatjuk. Meghatározhatjuk a napló méretét 64 kB-os lépésközzel.

A napló eseményinek felülírására három lehetőség adódik. A megadott naplóméret elérése esetén a legrégebben készült bejegyzések felülíródnak. A második lehetőség tulajdonképpen az előbbi esetnek a finomítása. Itt csak akkor írható felül a bejegyzés, ha régebben készült, mint a megadott napok száma. A harmadik esetben a naplót saját kezűleg kell kiürítenünk, a bejegyzések felülírása tiltott.

Ha betelik a napló, és a bejegyzéseket nem lehet felülírni, akkor egy erre utaló hibajelzést kapunk. Ilyenkor a naplózás már nem folyik tovább, azonban a napló kiürítése után minden rendben folytatódhat. A naplózás beállításait szabályozhatjuk a házirendek útján is a *Számítógép konfigurációja\Windows beállítása \Biztonsági beállítások\Eseménynapló* ágon.

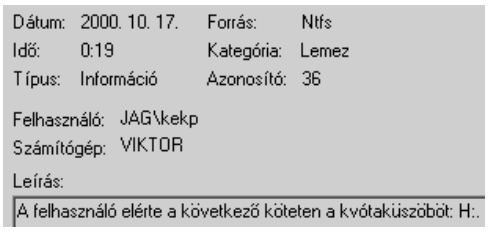
Tekintsük meg a naplófájl tartalmát! Az alábbi képen a rendszernapló egy részletét láthatjuk.

Típus	Dátum	Idő	Forrás	Kategória	Esemény	Felhasználó
Információ	2000. 10. 29.	0:36:01	Print	Nincs	13	mezgaa
Információ	2000. 10. 17.	0:19:25	ntfs	Lemez	36	kekp
Információ	2000. 10. 16.	22:45:58	ntfs	Lemez	37	ani
Hiba	2000. 10. 29.	15:38:36	W32Time	Nincs	62	-
Figyelmezt...	2000. 10. 29.	15:38:42	RSVP	Nincs	10047	-

A naplóban láthatjuk az esemény dátumát; pontos idejét; az esemény forrását; az esemény jellegére utaló rövid megjegyzést; az esemény azonosítóját az operációs rendszer számára; az eseményhez kapcsolható felhasználó azonosítóját, ha van ilyen; végül egy gépnevet látunk, amelyen az esemény történt.

Alapvetően három eseményfajta létezik. A kékkel jelölt (i) egy információt takar. Tehát nem is hiba valójában, csak tájékoztatás a számunkra. A sárgával jelölt (!) valamilyen közelgő hibalehetőségre vagy fontosabb üzenetre figyelmeztet. A piros kereszt (×) pedig valamilyen súlyosabb problémára hívja fel a figyelmet.

Ha szeretnénk az eseményről többet megtudni, akkor kattintsunk a kérdéses eseményre kettőt és egy – például a mellékelt ábra szerinti - bővebb leírást fogunk kapni az eseményről. Az előbbi ábrán látható 36-os azonosítójú esemény bővebb kifejtése látható az itt mellékelt ábrán.

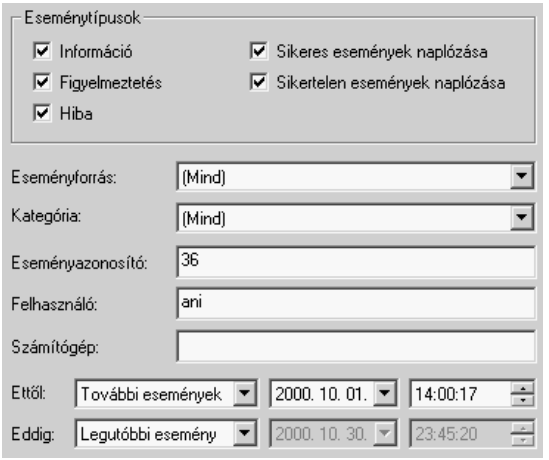


A naplók kezelése

A naplók kezelésére vonatkozó néhány menüpontot tekintsünk meg közelebbről. A naplónéző alkalmazás *Művelet* menüjében elmenthetjük az aktuális naplót vagy tanulmányozási célból megnyithatunk egy régebben elmentett naplót. A naplót elmenthetjük más programok számára is olvasható TXT formátumban a művelet menü lista exportálása pontjával. Nagyobb naplófájlok elemzéséhez segédprogramokat is találhatunk az Interneten.

Szintén a művelet menüben *törölhetjük* a napló tartalmát. Megjegyzendő, hogy a biztonsági napló törlés után sem lesz üres. Egyetlen sor lesz benne, amiben jegyzi a napló a törlés tényét és azt is, hogy mikor és ki törölte a naplót.

Ha a naplónéző alkalmazásban az eseménynapló nevű sor van kijelölt állapotban, akkor a művelet menü csatlakozás más számítógéphez pontján át az elérhető szerverek és munkaállomások bármelyikének a naplóját megtekinthetjük és még el sem kell menni a szerver elől.



A napló kiválasztása után a nézet menüben kétféle megjelenítés közül választhatunk. Az összes esemény megjelenhet, de szűrhetjük is az eseményeket. Terjedelmes naplófájlok tanulmányozásánál nagy segítséget jelenthetnek az

ábrán látható szűrési lehetőségek. Természetesen ilyenkor a többi esemény nem törlődik csak nem látszik. A minden esemény menüpont választása után újra láthatjuk az összes eseményt. A nézet menü keresés menüpontjában a mellékelt ábra időmeghatározás nélküli részét láthatjuk viszont két új lehetőséggel bővítve. Eldönthetjük, hogy lefelé, vagy felfelé szeretnénk keresni a naplóban az aktuális pozícióhoz képest.

A naplózás megfelelő beállítása nagy körültekintést igényel. Első próbálkozásainknál előfordulhat, hogy nem úgy működik a naplózás, ahogyan szeretnénk, hiszen elég sok helyen állíthatjuk a naplózást. Ilyen helyek a *Felügyeleti eszközök* között a *Helyi- és a Tartományi biztonsági házirend*, a *Tartományvezérlő biztonsági házirendje* és az összes szervezeti egység *Csoportházirendje*. A biztonsági házirendek a gép indulásakor értékelődnek ki. Arról se felejtkezzük el, hogy a házirendek hierarchikusan egymásra épülnek és pl. a bejelentkezések naplózásánál mást jelent a nincs naplózás és a nincs megadva érték. Az első esetben nincs naplózás, a második esetben pedig a felsőbb szintekről öröklött beállítások lesznek az érvényesek.

Feladatok

58. *Bejelentkezés naplózása*
Tartományi szinten bekapcsoltuk a bejelentkezések naplózását. A *vezetők* nevű szervezeti egység tagjainak bejelentkezését mégsem naplózza a rendszer, pedig már egy újraindítást is megtettünk. Mi történt?

59. *Mappa hozzáférésének naplózása*
Szeretnénk tudni, hogy a tanárok közül ki és mikor látogatta meg a szerződések nevű mappát ezért a tanárok szervezeti egység csoportházirendjében bekapcsoltuk az objektum-hozzáférés naplózását. A naplóban viszont semmilyen bejegyzés nincs a témával kapcsolatban. Hol a hiba?

60. *Bizalmas szerződések*
Bizalmas szerződéseinket tartalmazó mappánkra beállítottuk, hogy minden olvasási kísérletet naplózzon a rendszer és rendben megy is a naplózás. Félünk a szerződések megsemmisülésétől, ezért átmásoltuk az egész mappát a gépünkben található másik winchesterre. Milyen észrevételeket tehetnénk?

61. *Dolgozatok*
A dolgozatokkal kapcsolatos anyagokat egy *dolgozatok* nevű megosztott mappa megfelelő almappájában tárolják a tanárok. Dobos kolléga almappáját a rendszergazda ideiglenesen áthelyezte egy másik partícióra, de rövidesen visszakerült eredeti helyére. Mi történhetett a naplózási beállításokkal?

62. *Betelt naplófájl*
Túl gyakran kapunk üzenetet a szerveren, hogy betelt a biztonsági napló. Mit javasolhatnánk ebben az esetben?

63. *A bejelentkezés naplózása*
A biztonsági naplót megtekintve azt látjuk, hogy Balázsi úr hajnali 1-kor jelentkezett be a hálózatba. Nincs éjszakai műszak a cégnél. Mi lehet a megoldás?

64. *Windows 98*
A Windows 2000 szerver és munkaállomás változata is kiterjedt naplózási lehetőségeket kínál, de mi a Windows 98-ról a tartományunkba belépő felhasználók belépését is szeretnénk naplózni. Megoldható? Mit mondhatunk a Windows 98 alatt megosztott mappa hozzáférési kísérleteinek a naplózásáról?

65. *Kevés az eseménynapló*
A szerver előtt ülve kollégánk az eseménynaplót nézegeti. A monitoron a megszokottnál kevesebb naplót látunk. Hány naplót látunk és miért csak ennyit?

Összefoglaló feladatsor

66. *CD olvasó vagy RAM?*
20 számítógépet kap iskolánk. Választanunk kell, hogy minden gépbe legyen CD olvasó vagy inkább több memória legyen a gépekben. Elemezzük a választási lehetőségeket!

67. *Tartományi tagság*
Egy Windows 2000 Professionalt futtató számítógépet nem léptettünk be a tartományba. Ezen a számítógépen beléphetünk e tartományi nevünk és jelszavunk használatával? Miért? Ha egy hálózati erőforrást szeretnénk elérni erről a számítógépről, akkor mit tapasztalunk?

68. *Windows 2000 Professional telepítése*
Munkaállomásainkra Windows 2000 Professionalt szeretnénk telepíteni. Gépeinkben nincs CD-olvasó eszköz, de a telepítéshez szükséges állományok egy megosztáson elérhetőek. Hogyan érhetjük el ezt a megosztást, ha Windows NT4-ről szeretnénk frissíteni? Mit kell tennünk, ha még nincs semmilyen operációs rendszer a gépen? Mi a teendő, ha valaki szeretné megtartani a létező Windows 98-at és szeretné megtanulni a Windows 2000 használatát is?

69. *Windows 98, NT4 vagy 2000?*
Valaki számítógépet kap munkahelyén. Természetesen szeretné használni a hálózati erőforrásokat, a kérdéses gépen szeretne néhány anyagot elérhetővé tenni kollégái számára és a gépet mások is használnák. Melyik operációs rendszer mennyiben alkalmas ezen a munkahelyen?

70. *Windows 98, NT4 és 2000 egy gépen*
Egy 20GB-os winchesterre elsőként egy 6GB-os partícióra Windows 98-at telepítettek valamikor. A gép tulajdonosa szeretné a másik két operációs rendszert is a gépére telepíteni. Mit kell tennie?

71. *Mobil rack*
Három számítógépen rendre Windows 98, NT4 és 2000 operációs rendszer fut. Mobil rack segítségével valósítjuk meg az adatcserét. Mit javasolhatnánk a mobil rack fájlrendszerét illetően (előnyök, hátrányok)?

72. *Törölt felhasználó*
Tartományi rendszergazda kollégánk szabadságra ment és zárolás helyett töröltük felhasználói fiókját, de könyvtárait nem töröltük. Hogyan segíthetünk rajta?

73. *Jelszavak*
Mézga Géza úr munkahelyén a következő jelszavakat szokta használni: Paula, Aladár, AlAdÁr, PAlKri (a nevek első betűi), 2520815, 2765335, qw<df#5. Milyen észrevételeink lehetnének Mézga úr jelszavait illetően?

74. *Azonos felhasználók*
Azonos névvel és jelszóval létezik egy tartományi rendszergazda és egy munkaállomáson egy helyi rendszergazda. Egyenértékű a két rendszergazda vagy sem? Ha csak egyszerű felhasználókról van szó, akkor mit mondhatunk?

75. *A családi géppark bővül*
A család gépparkja két gépből áll. Ha hálózat kiépítése mellett döntünk, akkor koaxiális vagy UTP kábelt használjunk? Mennyiben befolyásolhatja döntésünket, ha a család kap egy harmadik gépet is?

76. *Elemezzük a jogosultságokat!*
Az alábbi táblázatban csak NTFS jogokat látunk. Feltételezzük, hogy Benton Péter 9.b. osztályos tanuló és ahol nincs bejegyzés a táblázatban, ott a kérdéses nevet nem tartalmazza hozzáférési lista.

Benton Péter	*9b*	*Mindenki*
olvas		
olvas	olvas	
	olvas	olvas
módosít	olvas	
olvas	módosít	teljes
teljes	módosít	olvas
nincs		teljes
teljes		nincs

77. *Törlési jog*
Miért van minden operációs rendszerben legalább egy olyan felhasználó, aki mindenkinek az anyagaihoz hozzáfér minimum törlési joggal?

78. *Biztonsági mentés*
Székelyi Szabolcs 9.a osztályos tanuló tud e biztonsági mentést készíteni a szerver egyik winchesteréről? Tegyük fel, hogy a szerveren van belépési joga, egyébként az osztálytársaival azonos jogai vannak.

79. *Diákrendszergazda*
Horváth Zoltán 11.a osztályos tanuló tagja a rendszergazdák csoportnak. Zoltán túl sok területet foglal el a winchesteren ezért a rendszergazda csökkentette az általa elfoglalható terület méretét, de mást nem állított be. Megkerülheti e Zoltán

ezt a beállítást? Mit tud tenni, ha a rendszergazda tiltott állapotba helyezte a felhasználói fiókját?

80. *A SID egyedisége*
Milyen problémákkal találkozhatnánk, ha két felhasználó is megkaphatná ugyanazt a SID-et?

81. *A biztonsági rendszer teljesítménye*
Mint ismeretes minden felhasználó és csoport egyedi SID-del rendelkezik. Az operációs rendszer minden hálózati erőforrásnál tárol egy SID listát (Access Control List) ami alapján ellenőrzi a hozzáférési kísérlet jogosságát. Mi köze van ennek az ACL-nek ahhoz, hogy a biztonsági rendszer teljesítményének érdekében is javasolják a csoportok használatát?

82. *Kíváncsi Kázmér*
Egy ügyvédi irodában egy bizalmas szerződéseket tartalmazó mappának mi vagyunk a tulajdonosai és csak néhány kollégánknak adtunk olvasási jogot a mappához. Kollégánk rövidesen érdeklődik, hogy miért vontuk meg olvasási jogát, pedig számítógép közelében sem jártunk. Ki lehet a Kíváncsi Kázmér?

83. *Cseregép*
Windows 2000 Professional operációs rendszert futtató gépünk sajnos meghibásodott. A javítás idejére kapott cseregépen Windows 98 fut. Mit tapasztalhatunk, ha megszokott hálózati nyomtatónkat használni szeretnénk?

84. *Nyomtatás naplózása*
Iskolánk igazgatója új nyomtatót kapott, ami a megfelelő jogosultsági beállításokkal meg is van osztva a hálózaton. A titkárság egyik dolgozója szeretné használni a nyomtatót és szeretné a naplózást is bekapcsolni. Mit mondhatunk az ötletéről?

85. *Feledékeny rendszergazda*
Egy Active Directory fában a teszt.bolt.cég tartomány rendszergazdája elfelejtette a jelszavát. Hogyan lehet rajta segíteni?

Irodalomjegyzék:

Belinszki Balázs: Windows NT 4.0 Server, 3D Computer Kft. , Budapest, 1997

Morten Strunge Nielsen: Windows 2000 és az Active Directory, Kiskapu, Budapest, 2000

Kis Balázs: Haladókönyv haladó szoftverhez, Szak Kiadó, Bicske, 2000