5. Active Directory alkalmazása Win2003-as hálózatban (tartomány,stb.)

1. Az Active Directory

A Windows 2003 Server tartalmazza az Active Directory címtárszolgáltatást. A címtár a hálózat minden erőforrását azonosítja, és elérhetővé teszi azokat a felhasználók és az alkalmazások számára. A címtár a hálózat fizikai felépítését és protokolljait átláthatóvá teszi, ezáltal a hálózat bármely felhasználója elérheti a hálózat bármely erőforrását anélkül, hogy tudná hol találhatóak azok valójában, vagy hogyan is kapcsolódnak egymáshoz fizikailag. A Windows 2003 Server által bevezetett Active Directory egy teljes egészében bővíthető és méretezhető címtárszolgáltatás. Az Active Directory a hálózat minden egyes publikált erőforrásának egy helyben történő adminisztrálási lehetőségét nyújtja, amibe beleértendők a fájlok és megosztások, perifériák, host kapcsolatok, adatbázisok, felhasználók, csoportok és egyéb tetszőleges objektumok és szolgáltatások.

Az Active Directory előnye a hálózati rendszergazdák, fejlesztők és felhasználók számára a címtárszolgáltatásban áll, amely:

- Lehetőséget ad a hálózatba való bejelentkezés és a hálózati felügyelet egyetlen helyről történő megvalósítására.
- Integrálja mind az Internetes és intranetes környezetet.
- Méretezhető a kisebb cégektől a nagyobb vállalatokig.

2. Csoportok

A csoportok az Active Directory vagy egy helyi számítógép olyan objektumai, amelyek felhasználókat, számítógépeket és más csoportokat tartalmazhatnak.

A csoportok használatának célja:

- felhasználók és számítógépek megosztott erőforrásokhoz (például az Active Directory objektumaihoz, azok tulajdonságaihoz, hálózati megosztásokhoz, fájlokhoz, címtárakhoz, nyomtatási várólistákhoz stb.) való hozzáférésének kezelése
- csoportházirend-beállítások szűrése, valamint
- elektronikus levelezési címzési listák létrehozása.

A csoportok két fő típusba sorolhatók:

- biztonsági csoportok és
- címzési csoportok.

A **biztonsági csoportok** felhasználók, számítógépek és más csoportok kezelhető egységekbe gyűjtésére szolgálnak. Az erőforrásokra (fájlmegosztás, nyomtatók stb.) szóló engedélyeket célszerűbb biztonsági csoportokhoz rendelni, mint egyéni felhasználókhoz, így az egész csoporthoz egyszerre rendelhető az engedély, és nem szükséges azt minden felhasználóhoz külön hozzárendelni. A csoporthoz rendelt engedélyekkel a csoporthoz hozzáadott összes fiók rendelkezik. Az egyéni felhasználók helyett csoportokra történő hivatkozás egyszerűsíti a hálózat karbantartását és felügyeletét.

A **címzési csoportokat** csak elektronikus levelezési terjesztési listaként lehet használni, csoportházirend-beállítások szűrésére nem alkalmazhatók. A címzési csoportoknak nincs biztonsági funkciójuk.

3. Az Active Directory felhasználói és számítógépfiókjai

Az Active Directory felhasználói számítógépfiókjai egy-egy valóságos személyt vagy számítógépet jelölnek. A felhasználói fiókokat és a számítógépfiókokat (valamint a csoportokat) rendszerbiztonsági tagoknak hívják. A rendszerbiztonsági tagok a címtár azon objektumai, amelyekhez a rendszer automatikusan biztonsági azonosítókat rendel. A biztonsági azonosítóval rendelkező objektumok bejelentkezhetnek a hálózatra és hozzáférhetnek a tartomány erőforrásaihoz.

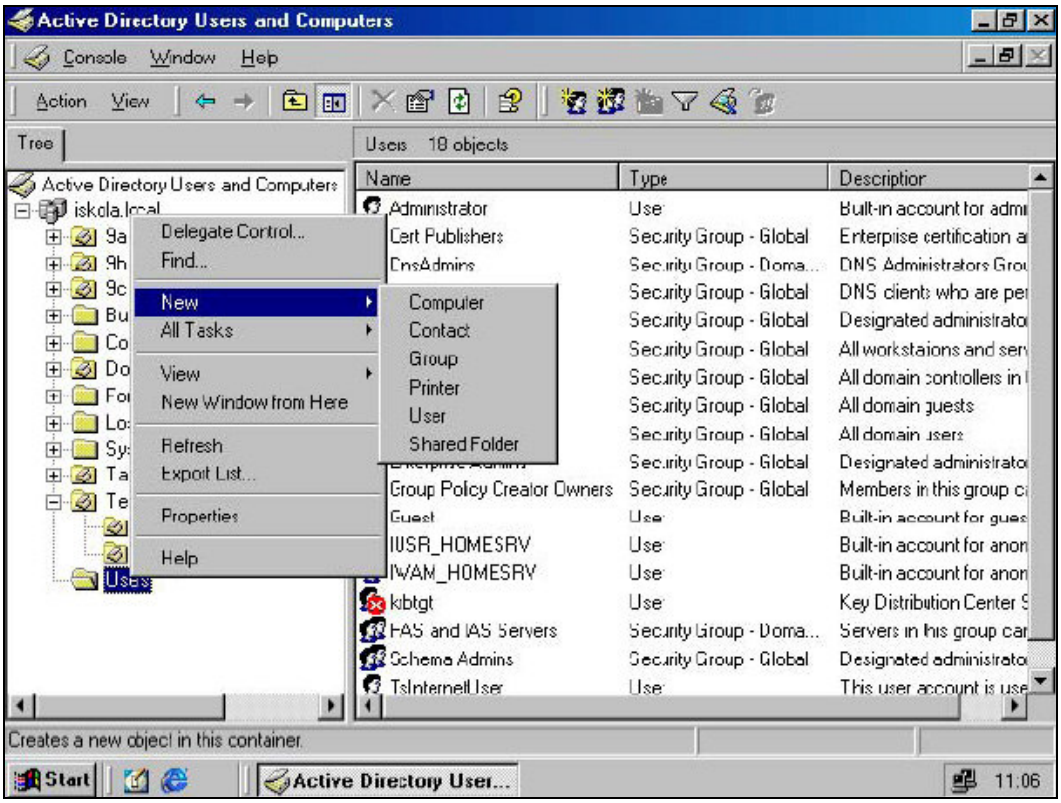
A felhasználói és számítógépfiókok az alábbiakra alkalmasak:

- A felhasználó vagy a számítógép azonosságának hitelesítése
- Tartomány erőforrásaihoz való hozzáférés engedélyezése vagy letiltása
- Egyéb rendszerbiztonsági tagok felügyelete
- A felhasználói vagy számítógépfiókok használatával kapcsolatos események naplózása

Felhasználói és számítógépfiókokat az Active Directory – felhasználók és számítógépek segítségével lehet hozzáadni, letiltani, alapállapotba állítani, illetve törölni.

4. Munka a címtár objektumaival

Az ablak baloldali részében a tartományban (iskola.local) található beépített (pl. Built-in, Computers) ill. általunk létrehozott szervezeti egységeket (pl. 9a, Titkarsag) és egyéb fontos beépített tárolókat (Computers, Users) láthatunk, míg a tárolók tartalma a jobb oldali részben jelenik meg. Egy új elem, pl. egy felhasználói fiók felvételéhez a hierarchia általunk kiválasztott pontján (pl. a Titkarsag OU-n) a jobb gombbal kattintva és a New… opciót kijelölve az 1. ábrán láthatóak közül választhatunk.



1. ábra *A címtárban létrehozható objektumok típusai*

4.1 Felhasználói fiók létrehozásának lépései

Új felhasználói fiók létrehozásakor megjelenő panelen a következő dolgokat lehet beállítani:

- A Full Name (Teljes név) mező a First Name (Vezetéknév) és a Last Name (Keresztnév) kitöltése után automatikusan megjelenik.

- A User logon name a felhasználó tartományi bejelentkezéséhez használt neve, amelyet praktikusan ékezet nélkül adunk meg, rövidítve. Célszerű a következő karaktereket sem használni: = + \ / < > [ ] * ? : ; , és a szóköz.

- A panel alján a nem Windows 2003 tartományba való bejelentkező név megadása történhet, ez alapesetben (ha betartjuk az előző bejelentkezési névvel kapcsolatos kritériumokat) megegyezhet az előző bejelentkezési névvel.

- A következő panelen a fiók jelszavát adhatjuk meg (kötelező megerősíteni a második mezőben), és/vagy választhatunk az alábbi opciókból:

    - ***User must change password next logon:*** ebben az esetben nem adunk meg jelszót, hanem a felhasználóra bízzuk az első tartományba belépése alkalmával.
    - ***User cannot change password:*** a felhasználó nem jogosult a jelszó megváltoztatására.
    - ***Password never expires:*** A jelszó soha nem „jár le”, azaz nem kell a rendszergazda által előírt időközönként megváltoztatni.
    - ***Account is disabled:*** a fiókot ezzel a kapcsolóval letilthatjuk, pl. ha még nem akarjuk, hogy a felhasználó igénybe vegye, vagy ha ideiglenesen fel kell függeszteni.

Ezzel a felhasználói fiókok felvétele megtörtént, a létrehozás után a fiók nevére kattintva a jobb gombbal ezeket a jellemzőket akár meg is változtathatjuk, vagy rengeteg más leíró/előíró/korlátozó opciót is szabályozhatunk. Ezek közül kiemelném az Account fület, ahol fontos bejelentkezési időtartományokra, a fiók automatikus lejáratára és egyéb belépéssel és jelszóbiztonsággal kapcsolatos beállításokat találhatunk.

A *Profile* fülön a – felhasználói környezet beállításainak összességét jelentő – felhasználói profil állományainak az elérési útját, a bejelentkezéskor végrehajtódó parancsokat tartalmazó szkript (*Logon script*) nevét ill. a felhasználó számára a szerveren biztosított tárterület (*Home folder*) a helyét, illetve, mivel a felhasználó előtt ez a mappa egy meghajtóként jelenik meg, e meghajtó betűjelét állíthatjuk be. A *Member of* fülön a felhasználó csoporttagságát szabályozhatjuk.

4.2 A beépített felhasználói fiókok és csoportok

Visszatekintve az 1. ábrára, a jobb oldali ablakban látható a Users tároló rengeteg beépített csoportja és felhasználója, amelyek a telepítéskor jönnek létre. Amennyiben frissítünk NT4-ről, akkor ebben a tárolóban találjuk az összes eddigi felhasználónkat és csoportunkat, amelyeket aztán az általunk megtervezett hierarchia alapján átmozgathatunk az új szervezet egységekbe. A fontosabb beépített felhasználók a következők: Administrator (Rendszergazda, a hálózat/tartomány üzemeltetője, épp ezért minden ezzel kapcsolatos jog birtokosa.

Természetesen több rendszergazda jogosultságú felhasználót is felvehetünk (csoportjuk az Administrators, Domain Admins, Enterprise Admins) sőt célszerű beépített Administrator-t átnevezni és/vagy jogait lefokozni. A Guest (Vendég): alapértelmezés szerint tiltott fiók, a tartomány minimális jogkörű elérése céljából jön létre, használata biztonsági szempontból nem is javasolt, csak kizárólag speciális esetekben. IUSR_szervernév: a webszerverünk „Vendége", szintén minimális jogokkal rendelkezik, ennek a fióknak a nevében tekintheti meg az összes az Internetről „érkező" érdeklődő a weboldalainkat, természetesen megfelelő hitelesítés után (pl. ha üzemeltetői jogkörrel rendelkezünk a webszerver felett) a jogosultságaink a tartományon kívülről is nagyobbak lehetnek.

Automatikusan létrejön még jó pár csoport (pl. a Built-in tárolóban) a rendszergazdai feladatok el- ill. kiosztása céljából, pl. Account, Print, Server, Backup Operators, azon fiókok tulajdonosai, akik ezekbe a csoportokba kerülnek általában csak egy-egy objektum, erőforrás vagy felhasználócsoport felett rendelkeznek teljes jogkörrel.

4.3 További műveletek a felhasználói fiókokkal

A fiókokkal kapcsolatos műveleteket a jobb gombbal a fiókra kattintva érhetjük el, ezek közül is nézzük a fontosabbakat!

- ***Copy:*** a nyilvánvaló jelentése mellett ez az opció egy praktikus lehetőséget nyújt, nevezetesen azt, hogy egy mintafelhasználó elkészítése és az összes felhasználó közös jellemzőinek erre a mintára való „ráhúzása" után, a mintát másolva már csak az egyéni, specifikus jellemzőket kell megváltoztatnunk.

- ***Reset password:*** a felhasználó jelszavát a rendszergazda nem láthatja, viszont ezzel az opcióval megváltoztathatja, azaz egy újat generálhat.

Delete: a fiók törlése, fontos ismerni azt a körülményt, hogy a biztonsági azonosítók (SID: Security IDentifier) használata miatt, ha letörlünk egy fiókot, majd újra létrehozzuk, akkor sem „élnek" a fiók korábbi jogosultságai, hiszen a létrehozás közben új, mindig egyéni SID-et generál az operációs