Informatika – Hálózati ismeretek

Hálózati menedzsment

TÁMOP 2.2.3-09/1-2009-0010

SZÉCHENYI ISTVÁN

Térségi Integrált Szakképző Központ

Szerkesztette: Vinnai Zoltán

Lektorálta: Domonkos Sándor

A kiadvány a Széchenyi István Térségi Integrált Szakképző Központ fejlesztése TÁMOP 2.2.3-09/1-2009-0010 projekt keretén belül készült.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg

– 2011 –

TARTALOMJEGYZÉK

1. A modul célja

A modul célja, hogy a hallgató ismereteket szerezzen a hálózati eszközök, számítógépek, felhasználók menedzselésének lehetőségeivel kapcsolatban, és ismerkedjen meg a címtárszolgáltatások fogalmával. A tanuló a modul elsajátítása után képes lesz a windowsos környezetben leggyakrabban alkalmazott Active Directory szolgáltatás használatára. Ismereteket szerez a biztonsági másolatok készítésével kapcsolatban. A tanuló a modul elsajátítása után képes lesz különböző rendszerek teljes és részleges másolatának elkészítésére, megérti a dokumentálás fontosságát. A modul elsajátítása után képes lesz továbbá a hálózat fizikai és logikai szerkezetének dokumentálására, a licence nyilvántartás vezetésére, valamint képes lesz a szervereket hálózaton keresztül is kezelni.

2. Előzetes feltételek

A modul elsajátításához szükség van a Hálózati alapismeretek és a Hálózati operációs rendszerek modul sikeres teljesítésére.

3. Előzetes tudás elismerésének és beszámításának módja

A tanuló előzetes tudását a tananyagban található témazáró feladatsorok és a tananyag végén található Összegző felmérés segítségével mérjük. Amennyiben az Összegző felmérést első próbálkozásra legalább 60%-os eredménnyel végzi el, a tanuló számára a modul elvégzése alól felmentés adható. Amennyiben nem éri el a 60%-os eredményt, a sikeres közbenső témazáró feladatsorok alapján az órák meghatározott részeinek látogatása alól adható felmentés. Ebben az esetben a tanuló számára kötelező az Összegző felmérés ismételt kitöltése.

4. 1. lecke: Címtárszolgáltatások (NDS, LDAP, AD)

4.1 Részcélkitűzések

A tanuló ismerje meg a címtárak szerepét, funkcióját, legfontosabb típusait, kialakulásának okait. Ismerje az Active Directoryval kapcsolatos alapfogalmakat. Ismerje a windowsos környezetben használható címtárszolgáltatást, felépítését, alapelveit, objektumait és elnevezési rendszerét.

4.2 Címtárak szerepe

Nagyobb méretű hálózatok esetén a nyilvántartás és az eszközök központi kezelése, menedzselése nagyon fontossá válik. A címtárszolgáltatások pontosan ezeket a célokat szolgálják.

A címtár gyakorlatilag egy adatokat rendezett formában tároló adatbázis, ami rugalmasan bővíthető. Mivel a hálózaton elérhető eszközök nevei, azonosítói, esetleg konfigurációs adatai is „csak” adatok, ezért ezeket is könnyedén lehet tárolni egy címtárban. Ugyanúgy a felhasználók nevei, elérhetőségei, korlátozásai is „csak” adatok, ezért ezeket is el lehet tárolni egy címtárban. Szintén „csak” adatok azok az információk is, amelyekkel az egyes erőforrásokhoz való hozzáférési jogokat lehet szabályozni.

Ha a számítógépeket is felkészítjük a címtárak használatára, akkor egy nagyon könnyen kézben tartható központi irányító rendszert kapunk. Ez azt jelenti, hogy a felügyeletet ellátó rendszergazda egyetlen adatbázis módosításával szabályozhatja a hálózati erőforrások elérhetőségét, befolyásolhatja azok működését, felhasználókat vehet fel, módosíthatja azok adatait, korlátozásokat és engedélyeket állíthat egyetlen központi felületen keresztül.

4.3 Címtárak típusai

A nagyobb cégeknél igényként merült fel egy telefonkönyvhöz hasonló adatbázis létrehozása, ami a faxszámokat tenné kereshetővé, ráadásul nemzetközi szinten. Volt is ilyen kísérlet (British Telecom), de a hatalmas adminisztrációs igény miatt nem vált be.

Elindult két szabványosítási projekt is, aminek végül az *X.500* lett az eredménye. Ez az első szabvány a címtárakkal kapcsolatban; a mai, gyakorlatban használt címtárrendszerek is ezt vették alapul.

A legelső címtár funkciókat ellátó működő rendszert a Novell készítette a saját szervereihez. Itt minden szerveren különálló adatbázis volt, ahova rögzíteni lehetett a felhasználók és a hardvereszközök (számítógép, nyomtató) adatait is. Ezt a különálló adatbázisrendszert a Novell *Bindery elv*nek nevezi.

A Novell a Bindery elv hiányosságait kiküszöbölve alakította ki az *NDS*-t (*„Novell Directory Services”* – ma már *eDirectory*-nak nevezik), ami már többszintű, elosztott adatbázisrendszer. A mai napig fejlesztik, és sok helyen alkalmazzák is.

A Microsoft saját címtárrendszere az Active Directory (AD), ami a windowsos környezetek egyik leghatékonyabb címtárrendszere.

Azonban a Novell és a Microsoft terméke is komoly pénzbe kerül. Létezik egy teljesen ingyenes megoldás is, amit csak *LDAP*-nek neveznek. Az LDAP az X.500 bonyolult, nehézkes kezelését hivatott könnyíteni, még a neve is erre utal: *„Lightweight Directory Access Protocol”* (egyszerűsített címtár-hozzáférési protokoll). Az LDAP eredetileg csak egy címtárak, címjegyzékek elérésére és karbantartására szolgáló protokollcsalád, nem foglalkozik magával a címtárral, annak felépítésével. Ezért aztán el lehet érni mind az NDS-t, mind az AD-t is LDAP-n keresztül. Az LDAP protokollhoz létezik egy ingyenes, nyílt forráskódú megvalósítás is, az *slapd*, ami képes az objektumadatok tárolására egy helyi adatbázisban. Ezzel biztosítható, hogy Linux alatt is használhassunk ingyenes címtárszolgáltatást.

4.4 AD alapfogalmak

Az *Active Directory* a Microsoft saját fejlesztésű címtárszolgáltatása, ami több millió objektum hierarchikus rendszerben történő tárolására és jellemzőinek gyors visszakeresésére szolgáló elosztott adatbázisrendszer. A segítségével alapvetően felhasználók, felhasználói csoportok, számítógé-

pek és nyomtatók egységes felületen keresztüli nyilvántartását lehet könnyedén megoldani.

Az *AD* egyik fontos feladata a központi bejelentkeztetés, vagyis azoknál a számítógépeknél, amelyek az *AD* részei (tartományi tagok), a felhasználó bejelentkezési folyamatában az *Active Directory* végzi a felhasználói azonosítást.

A hierarchikus felépítés azt jelenti, hogy vannak erőforrás-objektumok (felhasználók, gépek stb.), és vannak tároló objektumok, amelyekben lehetnek erőforrás-objektumok és újabb tároló objektumok, hasonlóan a fájlok tárolására használt könyvtárszerkezethez. A tároló objektumokat AD környezetben szervezeti egységeknek (*„Organizational Unit”*, röviden *OU*) nevezik.

Ennek megfelelően az objektumok elnevezési rendszere is többszintű. Az *Active Directoryval* felügyelt hálózatok alapvető adminisztrációs egysége a *tartomány* vagy *domain*, aminek jellemzően van egy egyedi neve, utalva az intézményre. A tároló objektumoknak is van nevük, és az erőforrás-objektumoknak is. Ha egy objektumot azonosítani szeretnénk, akkor – hasonlóan, mint a fájlrendszerben – megtehetjük relatív és abszolút módon is. Az abszolút megadásnál először az objektum nevét írjuk le, majd ponttal elválasztva a tároló objektumokat, végül a tartomány nevét, például a *nagyi.penzugy.ceg* megadásban *nagyi* a felhasználó, *penzugy* a tároló és a *ceg* a tartomány neve.

Ez a felépítés nagyban hasonlít az interneten használt domainnév rendszerre (DNS). A hasonlóság itt nem ér véget, mivel az adatok tárolására az Active Directory is a DNS szolgáltatást használja.

Minden objektumnak van egy rendszeren belüli, automatikusan generált, egyedi azonosítója, amit *GUID* (*„Globally Unique Identifier”*)-nak, vagyis globálisan egyedi azonosítónak neveznek. Ez az egész világon egyedi szám. Egy objektumra való hivatkozáskor a rendszer ezt használja.

A felhasználóknak, felhasználói csoportoknak és a számítógépfiókoknak van még egy SID („*Security Identifier*”), biztonsági azonosító száma is. A jogosultság szempontjából a SID azonosítja a felhasználót.

Egy hálózatban több tartomány is lehet. Az AD biztosítja azt is, hogy az egyes tartományok között is ki lehessen alakítani alá-, fölérendelési viszonyokat, vagyis a tartományok is hierarchiába szervezhetők. Ha a fában van egy kiinduló, úgynevezett gyökértartomány, akkor tartományfáról beszélünk. Ha több gyökértartomány van, akkor már erdőről beszélhetünk.

5. 2. lecke: AD telepítése a kiszolgálóra

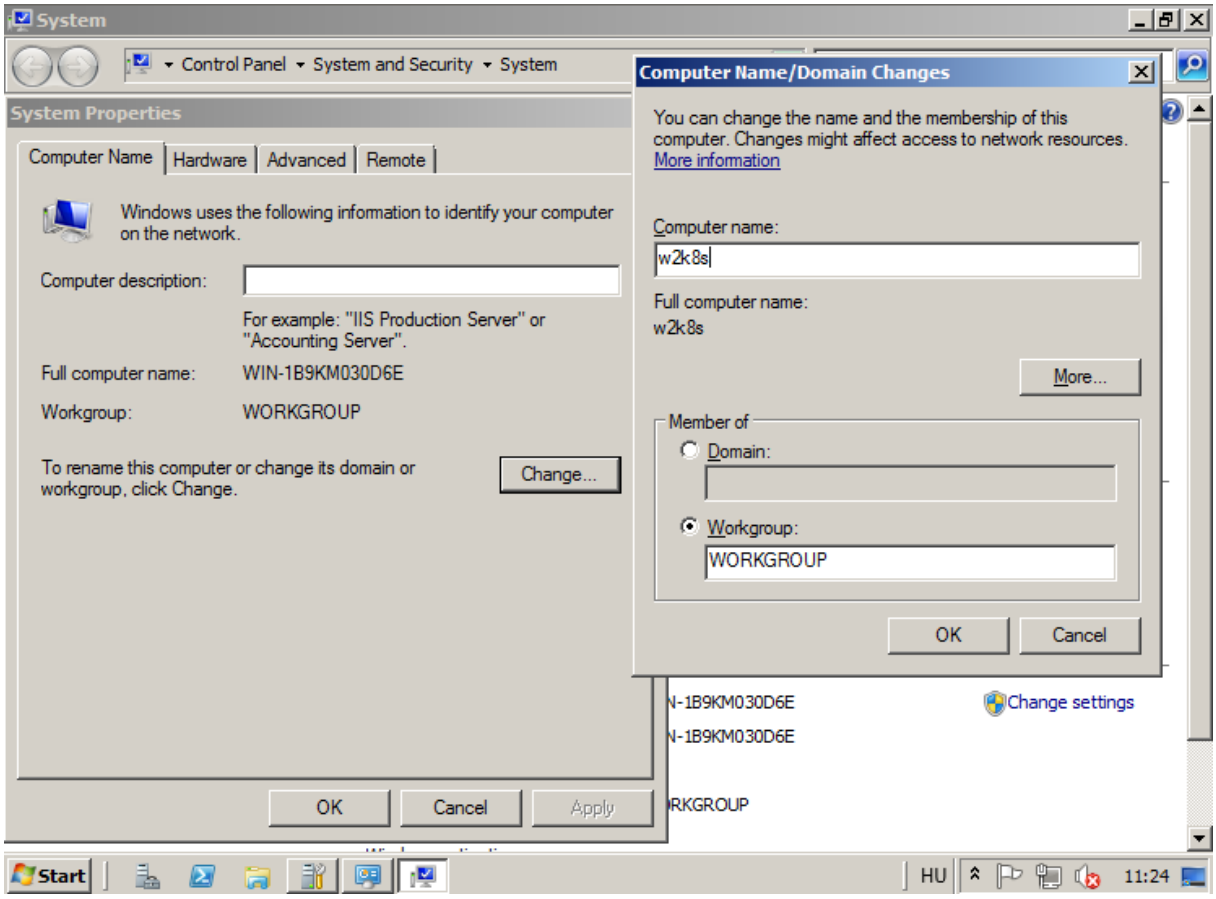
5.1 Részcélkitűzések

A tanuló legyen képes telepíteni a hálózaton Active Directory szolgáltatást, és beállítani a helyes működését.

5.2 Telepítés előtti feladatok

5.2.1 A számítógép átnevezése

A telepítés során a szerver egy véletlenszerűen generált nevet kapott, amit célszerű módosítani egy könnyebben megjegyezhető névre: a bejelentkezéskor automatikusan elinduló „*Initial Configuration Tasks*” program „*Provide Computer and Domain*” linkjére kattintva vagy a *Computer* ikon jobb egérgombbal elérhető gyorsmenü *Properties* menüpontját kiválasztva, és jobb oldalt lent a „*Change Settings*”-re kattintva. Ugyanez elérhető a vezérlőpulton („*Control Panel*”, „*System and Security*”, *System*) keresztül is.

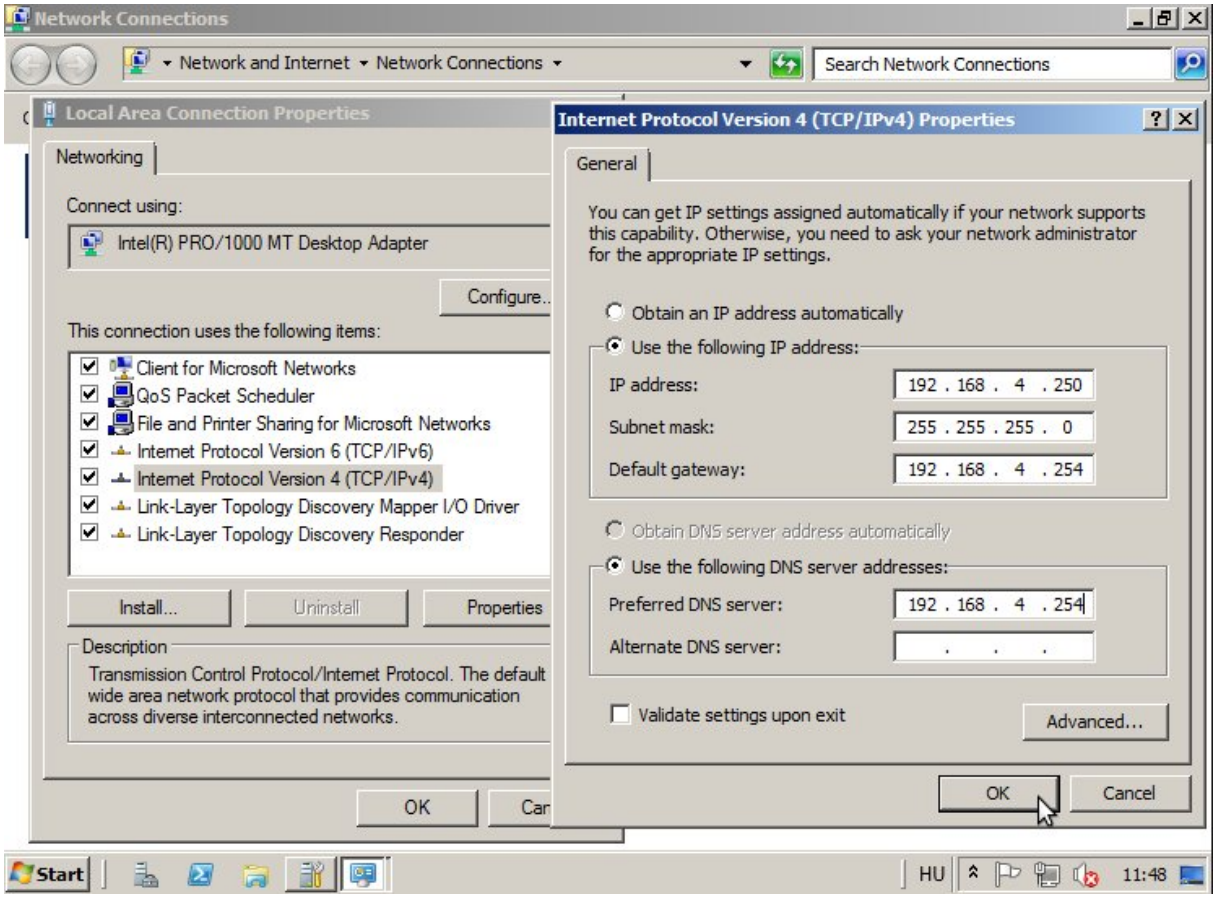


1. ábra. A számítógép nevének módosítása

A megjelenő ablakban a *Change* gombot kiválasztva egy újabb ablakban módosítható a számítógép és a munkacsoport neve is. A módosítás után újra kell indítani a számítógépet, hogy a változások érvényre is jussanak.

5.2.2 Fix IP-cím megadása

Egy kiszolgáló esetén alapvető elvárás, hogy a gép IP-címe ne változzon, ezért választani kell egy állandó címet a hálózatunkon belül. A beállításokat az adott környezet határozza meg. Ez beállítható az *„Initial Configuration Tasks”* program *„Configure networking”* linkjére kattintva megnyíló *„Network Connections”* programban. Ugyanez elérhető a vezérlőpulton keresztül is (*„Control Panel”*, *„View Network Status and Tasks”*, *„Change adapter settings”*). Itt a *„Local Area Network”* ikonra jobb egérgombbal kattintva, majd a gyorsmenüből *Propertiest* választva, megjelenik a hálózati protokollok listája.



2. ábra. Fix IP-cím beállítása

A listában az *„Internet Protokoll Version 4”* soron duplán kattintva a megjelenő ablakban megadhatók a hálózati adatok (IP-cím, netmask, átjáró, DNS szerver címe).

A beállítás után ellenőrizzük is le, hogy minden rendben van-e a hálózaton!

5.2.3 Rendszergazdai jelszó beállítása

Ha a telepítésnél nem adtunk meg a rendszergazdának (*Administrator*) jelszót, mindenképpen adnunk kell neki, különben nem fog települni az AD.

A telepítés lépeseit csak rendszergazdai jogokkal rendelkező felhasználó végezheti el, ezért jelentkezzünk is be rendszergazdaként!

5.3 Telepítési folyamat

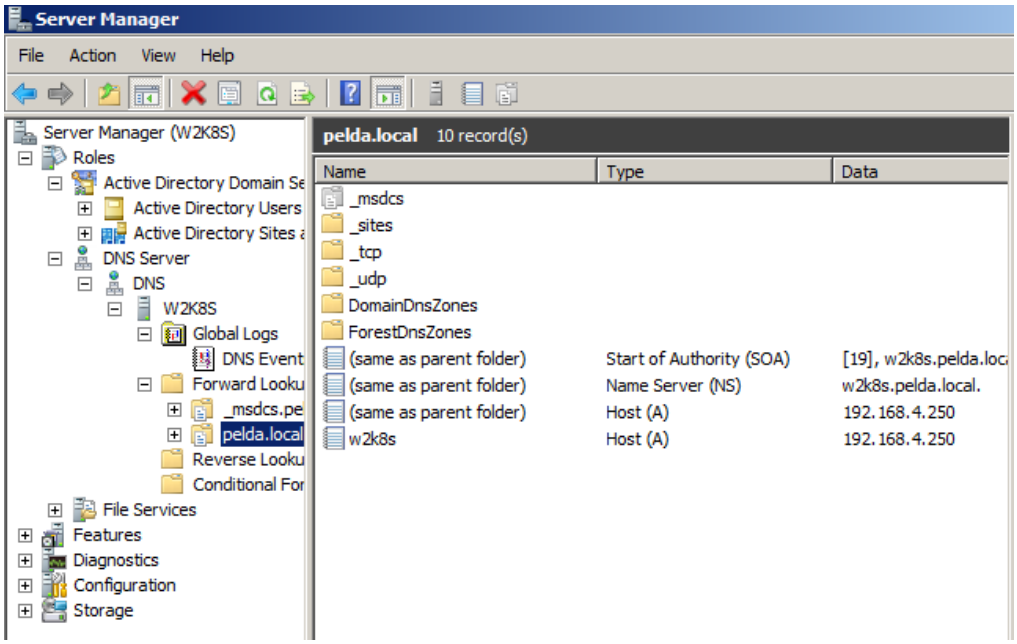
1. **dcpromo.exe** elindítása, a *Run…* (Futtatás) ablakban, egyszerűen írjuk be.
2. A rövid idő múlva megjelenő ablakban kapcsoljuk be a speciális módot (*„Use advanced mode installation”*), majd *Next*, *Next*.

3. Még nincs tartományunk, ezért egy újat hozunk létre („*Create a new domain in a new forest*”), majd Next.
4. Meg kell adni a szerver gyökerének teljesen meghatározott DNS nevét (*FQDN*) (a példában *pelda.local*), majd *Next*.
5. Meg kell adni vagy el kell fogadni a felajánlott tartomány *NETBIOS* nevét (a példában *PELDA*), majd *Next*.
6. Ki lehet választani a tartományi erdők kompatibilitási rendszerét. Ha van a hálózatunkban vagy elképzelhető, hogy lesz egy 2003-as tartományvezérlő, akkor az alapértelmezett beállítást válasszuk, majd *Next*.
7. Ha az előző pontban 2003-as szintet választottunk, akkor itt a saját tartományunkra vonatkozó szintet határozhatjuk meg, majd *Next*.
8. Ha a kiszolgálónkon nincs beállítva DNS szolgáltatás, akkor itt automatikusan felajánlja a telepítését, hagyjuk is meg, vagyis legyen pipa a *DNS server* előtt, majd *Next*.
9. Ha most nem tudja létrehozni a DNS beállításokat, akkor egy üzenetben figyelmeztet, hogy kézzel is el lehet végezni azokat. Itt válasszuk a *Yes*-t!
10. Meghatározhatjuk az Active Directory adatbázis fájljainak („*Database folder*”), a naplófájloknak („*Log files folder*”) és a rendszerfájlok („*SYSVOL folder*”) helyét. Az alapértelmezés is megfelelő, így *Next*.
11. Meg kell adnunk a címtár szolgáltatás helyreállításához tartozó rendszergazdai jelszót.
12. Az összefoglaló oldalon ellenőrizni lehet a beállításokat, majd *Next*.
13. A beállítások végén a DNS-sel kapcsolatos üzenetet olvashatjuk, majd *Finish*.
14. Újra kell indítani a rendszert (*Restart*).

5.4 Telepítés utáni feladatok

Ellenőrizzük a *„Server Manager”* programban a telepített szolgáltatásokat a *Roles* (Szerepkörök) elemnél. Meg kell hogy jelenjen az *„Active Directory Domain Services”*, a *„DNS Server”* és a *„File Services”* elem is a listában. Kiválasztva az egyes szolgáltatásokat, egy-egy összefoglaló oldal jelenik meg, ahol az utolsó eseményekről kapunk egy kis összefoglalót.

Ha a telepítés rendben lezajlott, akkor a DNS elemben meg kell jelennie a szerverünk nevének (most *W2K8S*) és a *„Forward Lookup Zone”*-nál a *pelda.local* bejegyzésnek is. Azon belül pedig szerepelnie kell a *w2k8s* név mellett az IP-címnek is, ami a példában *192.168.4.250*.



3. ábra. Active Directory DNS-sel

A telepítőnek szintén módosítania kellett a hálózati beállításokat is, konkrétan a hálózati kapcsolatoknál a DNS beállításokat *127.0.0.1*-re kellett átírnia, ezzel biztosítva azt, hogy az adott gépen a névfeloldást a saját DNS szervere végezze. Ellenőrizzük ezt is!

6. 3. lecke: Tartományba léptetés

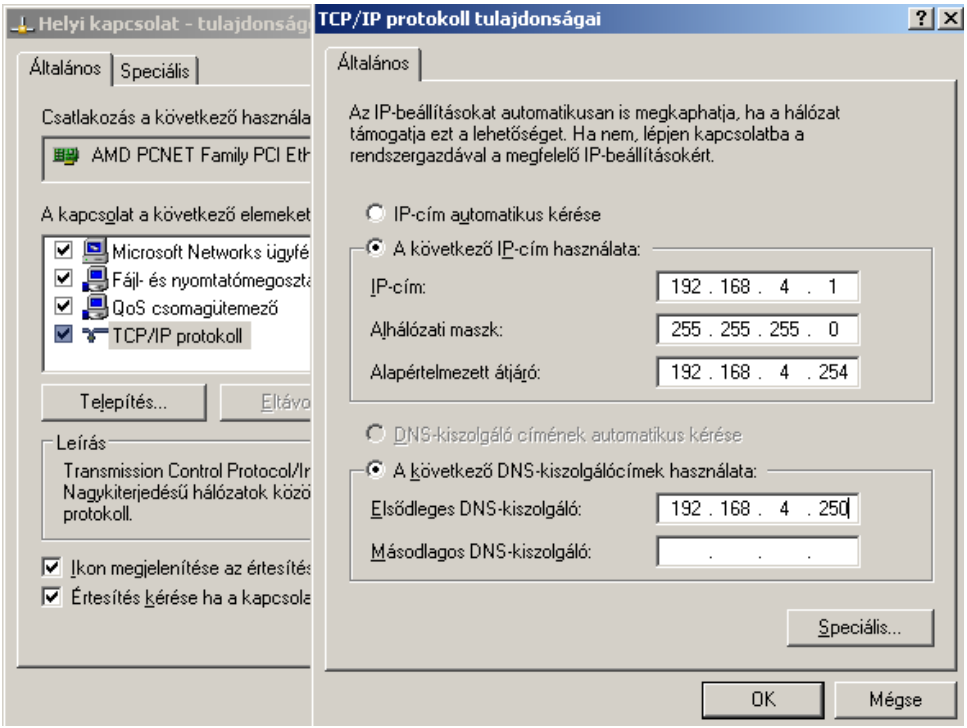
6.1 Részcélkitűzések

A tanuló legyen képes windowsos számítógépek tartományba léptetésére.

6.2 Előfeltételek

Ahhoz, hogy egy számítógépen a bejelentkezés során a tartományi kiszolgálóhoz forduljon a rendszer, a számítógépet a tartomány tagjává kell tenni. A legtöbb windowsos operációs rendszer alkalmas tartományi munkára, kivéve a Windows XP Home változatát.

A beléptetéshez a kliens gépen a hálózatot is be kell állítani úgy, hogy a gép az Active Directory által is használt DNS szervert használja, jelen példában ez magán a szerveren van, a 192.168.4.250-es IP-címen. Módosítani kell tehát a kliens gép DNS beállítását. Ez Windows XP esetén a *Vezérlőpult*, *„Hálózati és Internetes kapcsolatok”*, *„Hálózati kapcsolatok”*, majd a *„Helyi hálózat”* ikonon jobb egérgomb és *Tulajdonságok*, majd a *„TCP/IP protokoll”*-on dupla kattintás.

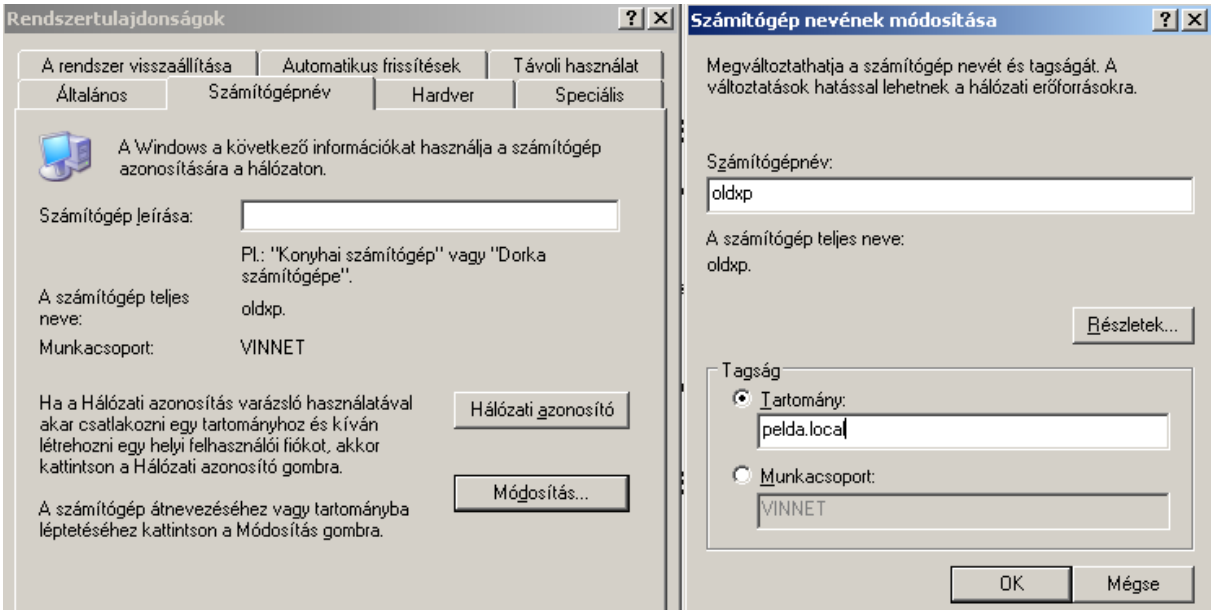


4. ábra. XP hálózati beállítása tartományi munkára

6.3 Beléptetés

A módosításhoz rendszergazdai jogokra van szükség, vagyis a sikeres művelethez rendszergazdaként jelentkezzünk be.

A tényleges beléptetéshez a számítógép nevének módosításánál kell megadni a tartományt. Ehhez indítsuk el a vezérlőpultot, majd *„Teljesítmény és karbantartás”*, majd *Rendszer*, a megjelenő *Rendszertulajdonság* ablakban pedig a *Számítógépnév* fület válasszuk ki. Kattintsunk a módosítás gombra, és adjuk meg a tartomány nevét, a példában ez *pelda.local* volt.



5. ábra. XP beléptetése tartományba

Ezután meg kell adnunk egy tartományi rendszergazda felhasználói nevét és jelszavát. Majd újra kell indítani a számítógépet.

6.4 Újraindítás után

Az újraindítást követően ki kell választani, hogy ne helyi bejelentkezés legyen, hanem tartományi. Ha nem látszik a *„Bejelentkezés ide”* elem, akkor a *Beállítások* gombot kell kiválasztani. Jelen példában ez a *PELDA* nevű tartomány kiválasztását jelenti.

6. ábra. Tartomány kiválasztása bejelentkezéskor

A kiválasztás után a felhasználónévnek már tartományban létezőnek kell lennie, különben sikertelen lesz a bejelentkezés.

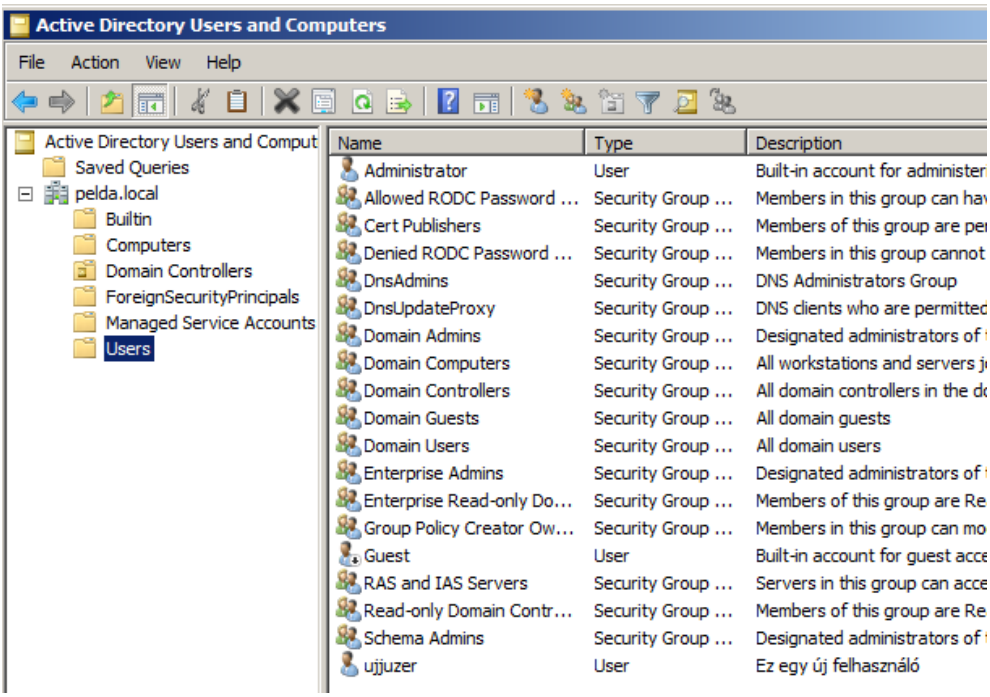
7. 4. lecke: Tartományi felhasználókezelés

7.1 Részcélkitűzések

A tanuló értse a helyi és a tartományi felhasználókezelés közötti különbséget. Legyen képes kialakítani tartományi felhasználói hierarchiát. Tudjon egyszerűen felhasználókat felvenni, adataikat módosítani. Legyen képes felhasználói csoportokat létrehozni, kezelni.

7.2 Active Directory Users and Computers

A tartományi felhasználók kezelését az *„Administrative Tools”* menüből elérhető *„Active Directory Users and Computers”* programmal célszerű elvégezni. A programot elindítva látszik, hogy baloldalt több elemet is tartalmaz, amelyeket nem lehet törölni és átnevezni se. Ezek a típus nélküli tároló objektumok, amelyekbe alapértelmezés szerint az új felhasználók és a beléptetett számítógépek kerülnek. Ha kiválasztjuk a *Computers* elemet, akkor a jobb oldalon megjelennek a már beléptetett számítógépek, a *Users* elemnél pedig megjelennek a felvett felhasználók és csoportok, melyek között vannak újabb alapértelmezett csoportok is.



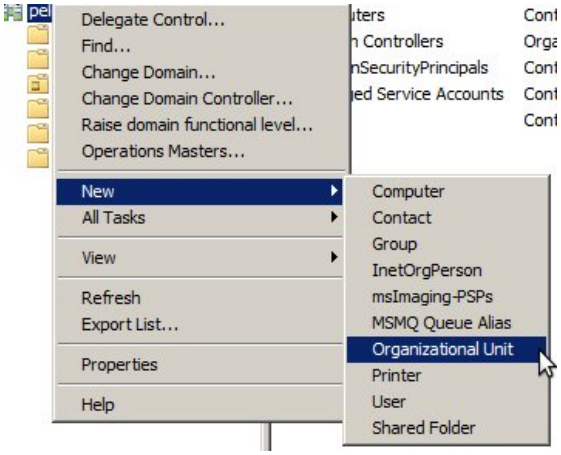
7. ábra. Alapértelmezett tartományi felhasználók és csoportok

Egy objektummal sokféle műveletet el lehet végezni, a lehetőségek a jobb egérgombbal megjelenő gyorsmenüből érhetők el. A *Properties* menüponttal lehet állítani a tulajdonságokat, de például egy felhasználó esetén itt lehet törölni, átnevezni, másolni, jelszavát alaphelyzetbe állítani stb.

Új felhasználót célszerűen a *Users* tárolóban hozhatunk létre úgy, hogy jobboldalt egy üres területen (vagy magán a *Users* tárolón) jobb egérgombbal kattintunk, majd a gyorsmenüből *New* és *User*. Itt megadhatjuk a nevét, jelszavát, bejelentkezési nevét (*„User logon name”*), a további adatokat azonban csak a létrehozás után, a tulajdonság lapokon adhatjuk meg.

7.3 A szervezeti egységek (Organizational Unit – OU)

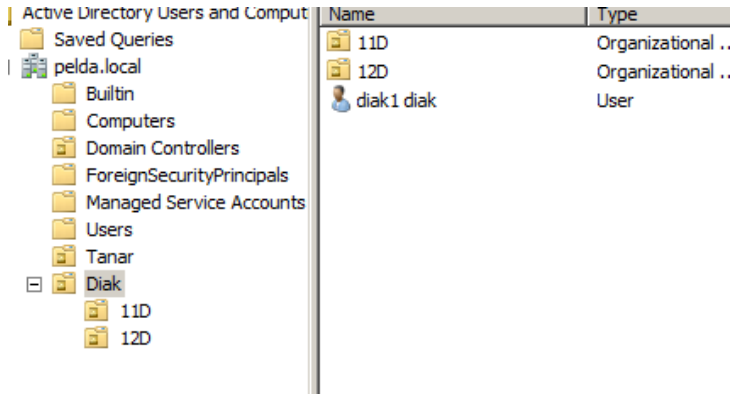
A felhasználóink és számítógépeink azonban különböző szervezeti egységekbe csoportosíthatók egyszerűen úgy, hogy a tartományban létrehozzuk azokat, majd azon belül hozzuk létre vagy másoljuk oda felhasználóinkat. Új szervezeti egység létrehozásához a tartomány nevén jobb egérgombbal előhívható menüből a *New*, majd az *„Organizational Unit”* elemet kell kiválasztani.



8. ábra. Új szervezeti egység létrehozása

Ezek után egyszerűen meg kell adni a nevét. Hozzunk létre egy *Tanar* és egy *Diak* szervezeti egységet. A *Diak*-on belül pedig létrehozhatunk további egységeket, például osztályokat. Most hozzunk létre mondjuk egy *11D* és egy *12D* szervezeti egységet. A tanár felhasználókat a *Tanar* szervezetbe, míg a tanulókat a *Diak* egységben mindig a megfelelő szervezeti egységen belül hozzuk létre. Most hozzunk létre egy *tanar1* és egy *diak1* felhasználót a megfelelő szervezeten belül!

Figyeljünk rá, hogy alapesetben a Windows 2008 szerveren szigorítva van a jelszómegadási mód, vagyis legalább 7 karakterből kell állnia, és tartalmaznia kell kis- és nagybetűt, számot, valamint egyéb speciális karaktert is.



9. ábra. Tartományi szervezetek és felhasználók

A létrehozott felhasználókkal már be is tudunk jelentkezni azon a számítógépen, amit már beléptettünk a tartományba.

10. ábra. Bejelentkezés tartományba

A felhasználók bejelentkezési neveinek egyedieknek kell lenniük a teljes tartományon belül, hogy felhasználóink egyszerűen tudjanak bejelentkezni.

7.4 Felhasználói csoportok

Ajánlatos létrehozni külön csoportokat (*Group*) a tanárokhoz és diák osztályokhoz is, amelyekbe fel is kell venni a felhasználókat. Most célszerűen a *Tanar* szervezetben egy *Tanarok*, míg a *Diak* szervezetben egy *Diakok* csoportot, valamint a *11D*-n belül egy *Diak_11D*, a *12D*-n belül pedig egy *Diak_12D* csoportot.

Tömeges felhasználó-létrehozásnál hasznos lehetőség az úgynevezett minta (template) felhasználó, ahol beállíthatjuk azokat a jellemzőket, amelyek közösek (pl. csoporttagság, bejelentkezési időszak), majd a többi felhasználót ennek alapján hozzuk létre a másolás (jobb egérgomb *Copy…*) segítségével.

8. 5. lecke: Tartományi erőforrás-kezelés

8.1 Részcélkitűzések

A tanuló legyen képes a hálózati megosztások tartományi környezetben történő, igény szerinti beállítására. Ismerje a rejtett megosztások lehetőségét, elérési módjaikat. Legyen képes rejtett megosztást létrehozni. Legyen képes felhasználókhoz hozzárendelni a szerveren egy home könyvtárat, és helyesen beállítani a hálózati elérhetőségét. Ismerje a csoportházirend fogalmát, jelentőségét.

8.2 Tartományi megosztások és elérésük

Itt elsősorban a megosztott mappák és nyomtatók központi kezelésére kell gondolni. Megosztásokat AD környezetben is ugyanúgy lehet létrehozni, és hálózaton keresztül elérni azokat, a különbség mindössze annyi, hogy tartományi felhasználóknak és felhasználói csoportoknak adunk hozzáférést a megosztáshoz. Fájlrendszer szinten és megosztás szinten is vigyázni kell, hogy kinek milyen jogosultságokat adunk. 2008 alatt erre figyel a rendszer is, vagyis ha a megosztásnál hozzáadunk egy felhasználót írási jogkörrel, akkor automatikusan fájlrendszer szinten is beállításra kerülnek a jogosultságai.

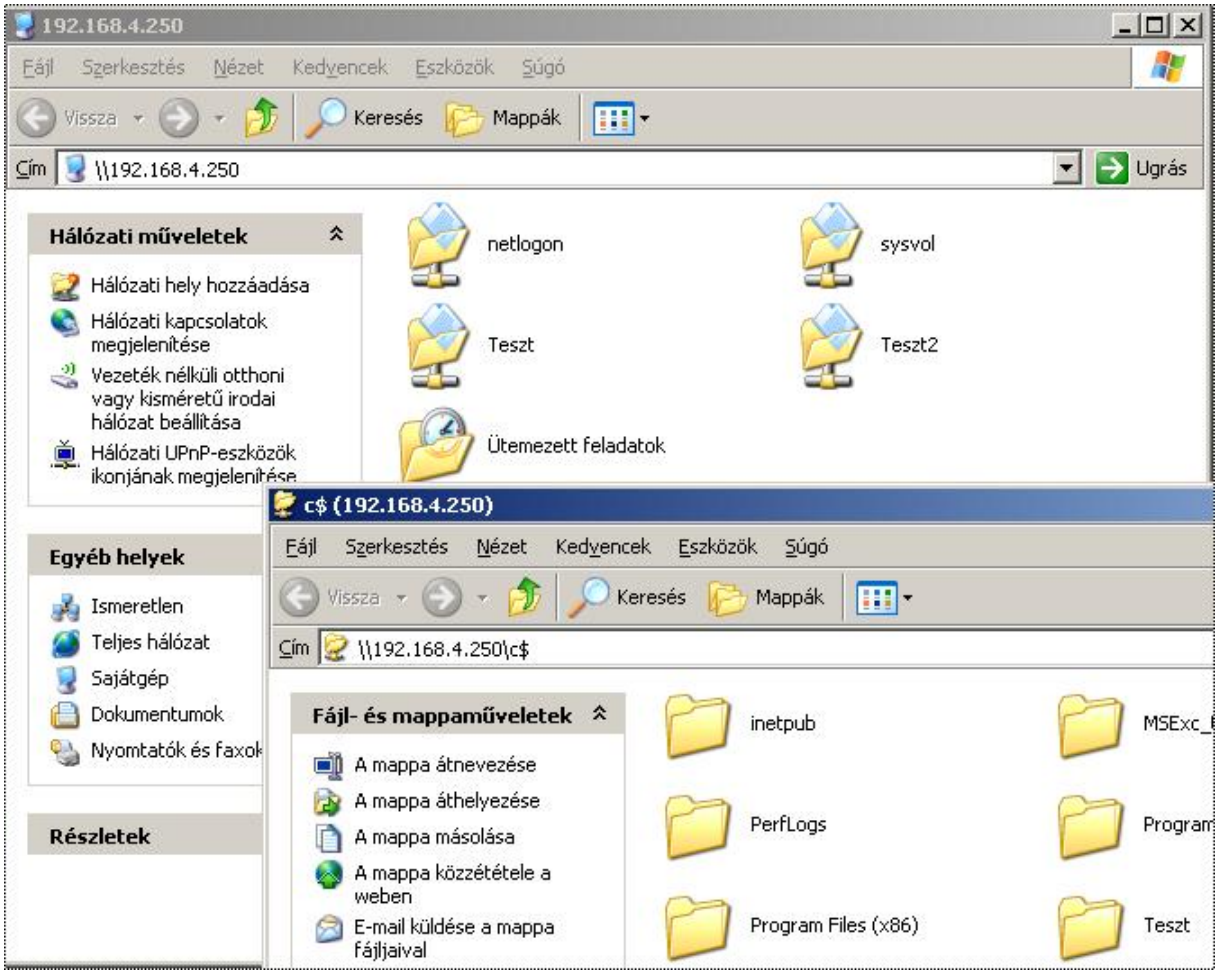
Tartományi környezetben azonban egy kicsit könnyebb a tallózás, vagyis a hálózati erőforrás elérése, ugyanis ha egy tartományi felhasználóval vagyunk bejelentkezve, akkor nem kell külön azonosítani magunkat ahhoz, hogy hozzáférjünk a megosztott könyvtárhoz.

8.3 Rejtett megosztások

A legtöbb Windows operációs rendszer segítségével lehetőség van rejtett megosztások létrehozásához is. A rejtett megosztás lényege, hogy hálózati tallózáskor nem látszik. Ha valaki nem ismeri a megosztás nevét, nem tudja használni azt.

A Windows rendszerek alapértelmezésben automatikusan létrehoznak több rejtett megosztást is, mint például a gyökérpartíciók (pl. *C:*, *D:*), vagy a Windows rendszermappája (*C:\Windows*). Persze ezekhez a megosztásokhoz csak *administrator* felhasználóval lehet hozzáférni. A rejtett megosztásokat a szerveren a „*Share and Storage Management*” (a „*Start menü*”, „*Administrative Tools*” menüből elérhető) program segítségével is meg lehet jeleníteni, illetve ott is létre lehet hozni megosztásokat.

Ha egy rejtett megosztást el akarunk érni, akkor pontosan meg kell adni a megosztás nevét. Rejtett megosztásokat a név végén elhelyezett „*$*” jel segítségével lehet létrehozni, így a *C:* egység rejtett megosztási neve a „*C$*”, és ha hivatkozni akarunk rá, akkor *\\ipcím\C$* nevet kell használni.



11. ábra. Rejtett megosztás elérése

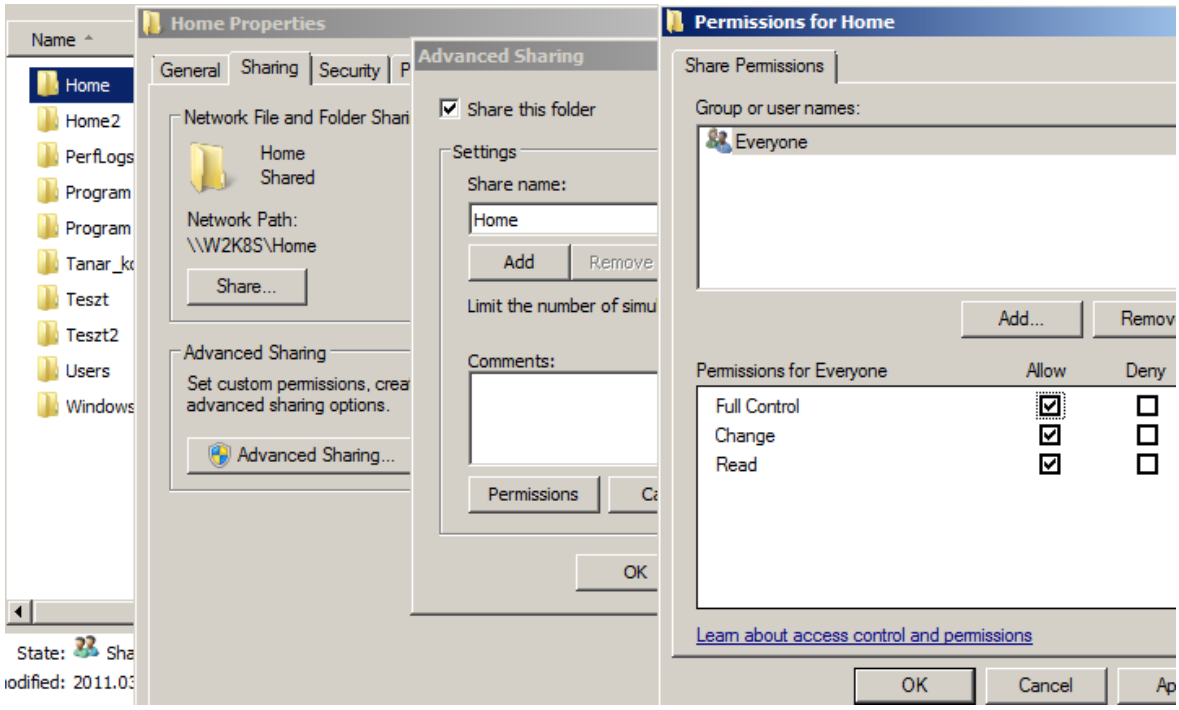
Rejtett megosztást felhasználó is létrehozhat nagyon egyszerűen, úgy, hogy a megosztás nevének a végére elhelyezi a „*$*” jelet. Ha például a „*teszt2*” nevű megosztást rejtetten szeretnénk létrehozni, akkor a „*teszt2$*” nevet kell megadni a megosztás nevének.

8.4 Home könyvtár beállítása

Az Active Directory segítségével a tartományi felhasználók részére könnyedén lehet *home* könyvtárakat készíteni a szerveren, majd hozzárendelni egy meghajtó betűjelet. A *home* könyvtár azt jelenti, hogy minden egyes felhasználónak lesz egy saját könyvtára a szerveren, amihez csak és kizárólag ő férhet hozzá.

Először létre kell hozni egy kiinduló könyvtárat a szerveren, ez most célszerűen a *Home* lesz. Majd meg kell osztani mindenki számára (*Everyone*) teljes jogkörrel. Ehhez válasszuk ki a *Home* könyvtárat a fájlkezelővel,

majd jobb egérgomb, *Properties*, *Sharing* fül, *„Advanced Sharing…”*, pipa a *„Share this folder”* elé, *Permissions*, végül pipa a *„Full Controll”* sor *„Allow”* oszlopába.



12. ábra. Home könyvtár megosztása

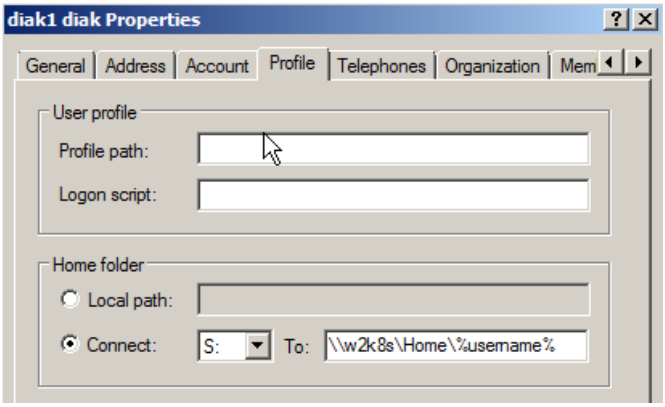
A felhasználók tulajdonságainál, a *Profile* fül *„Home folder”* részében, a *„Connect to”* mezőkben pedig meg kell adni a kívánt meghajtó betűjelet, valamint a home könyvtár hálózati elérhetőségét a ***\\szervernév\megosztásnév\%username%*** alakban, ahol a *%username%* mindig az aktuális felhasználót jelenti. A példában ez mondjuk az *S:* meghajtót és a *\\W2k8S\Home\%username%* beállítását jelenti.

A „%” jelek között megadott név egy környezeti változót takar. Több környezeti változó is elérhető egy windowsos rendszerben. A környezeti változóknak van nevük és van értékük. A környezeti változók nagy részét maga a rendszer állítja be, de lehetőség van arra is, hogy a felhasználó vegyen fel egyéni környezeti változókat. A változókat és értéküket a **set** paranccsal lehet megjeleníteni parancssorban. Bármelyik környezeti változó értéke felhasználható parancssorban vagy akár programparaméterként

is, ha „%” jelek között adjuk meg a nevét. A fontosabb környezeti változók listáját a következő címen lehet megtekinteni:

http://technet.microsoft.com/hu-hu/library/cc737438%28WS.10%29.aspx

A *%username%* megadási móddal megoldható az is, hogy egyszerre több felhasználó beállításait módosítjuk úgy, hogy előtte kijelöljük őket.

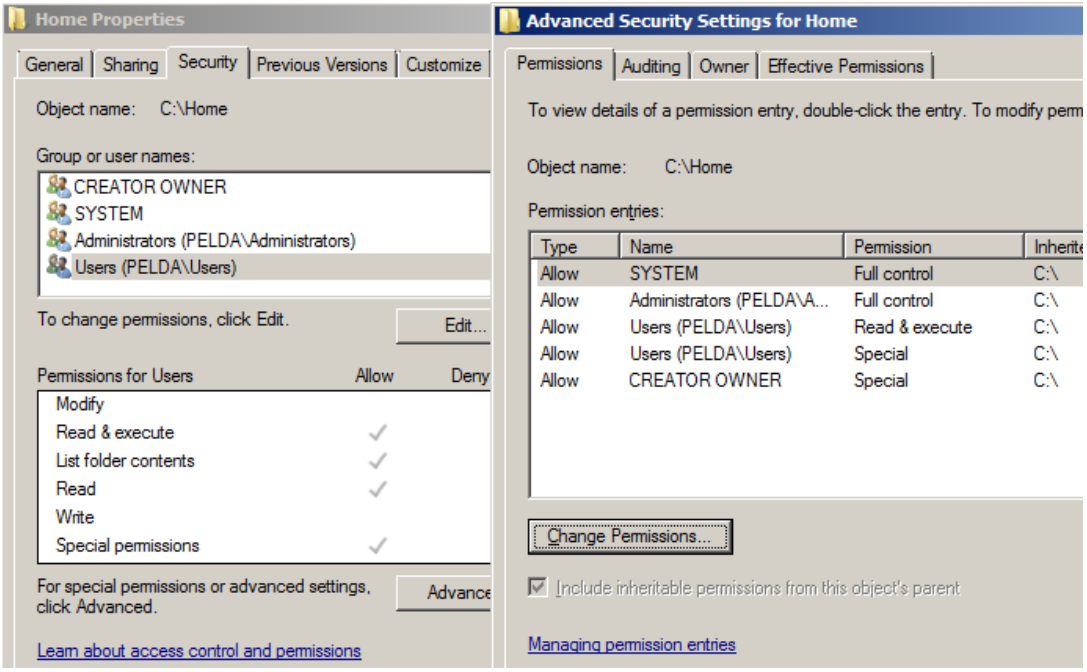


13. ábra. Home könyvtár beállítása

Ezzel a beállítással már a következő bejelentkezéskor meg fog jelenni a sajátgépen az *S:* meghajtó. Ha több felhasználónál állítottuk be, akkor mindenkinek lesz ugyan *S:* meghajtója, de mindenkinek más könyvtárra mutat.

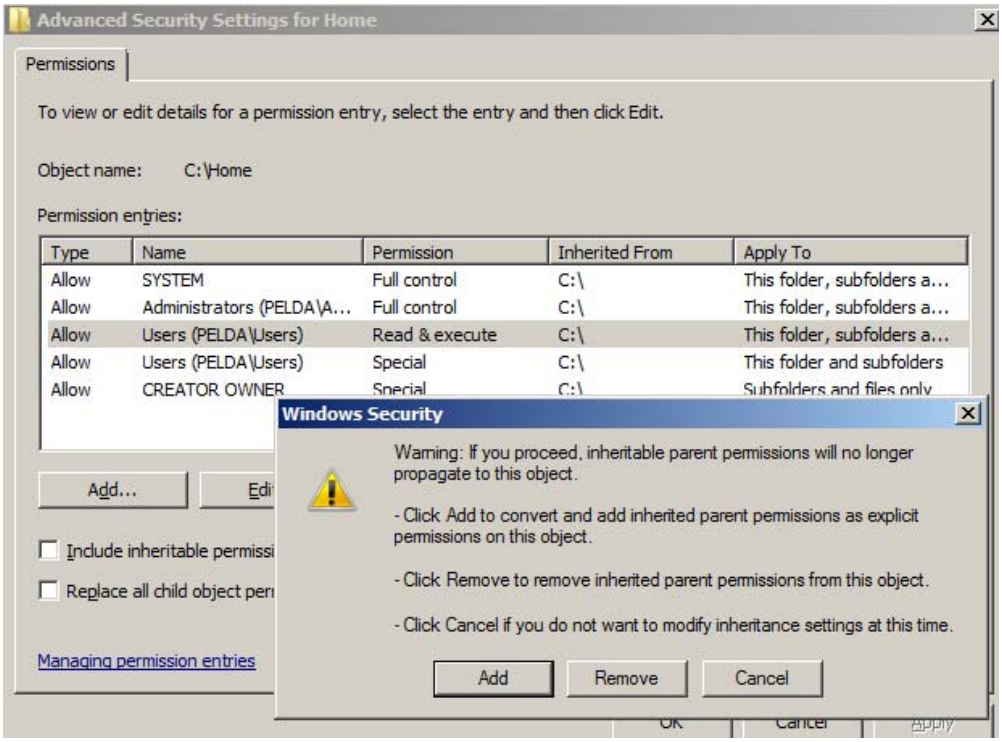
Van azonban még egy probléma a könyvtárakkal kapcsolatban. Ugyanis a megosztott *Home* könyvtár kitallózható bármely tartományi felhasználó részére, és mivel a megosztás mindenki számára engedélyezve van, így bárki home könyvtárában lehet garázdálkodni, módosítani, törölni, létrehozni stb. Ennek megakadályozásához el kell venni jogokat a *Home* könyvtárról. Konkrétan a *Users* csoporttól a *„Special permissions”* jogon kívül mindent el kell venni.

Fájlkezelőben a *Home* könyvtáron jobb egérgomb, *Properties*, majd *Security* fül, *Advanced* gomb.



14. ábra. Home könyvtár jogainak beállítása 1

Az *„Advanced Security Settings”* ablakban *„Change Permissions…”*, a megjelenő ablakban válasszuk ki a *„Users Read & Execute”* sort, majd vegyük ki a pipát az *„Include inheritable permissions from this object’s”* elől. A figyelmeztető ablakban az *Add* gombot válasszuk.



15. ábra. Home könyvtár jogainak beállítása 2

Ezután lehet csak eltávolítani a *Remove* gombbal a *„Users Read & Execute”* sorát. Innentől kezdve nem lehet majd tallózni a *Home* megosztást, a felhasználók csak és kizárólag az *S:* meghajtón keresztül férhetnek hozzá saját home könyvtáraikhoz.

9. 6. lecke: I. témazáró feladatsor

1. **Válassza ki, hogy melyik nem címtárszolgáltatás! Csak egy jó válasz van! (1 pont)**

    a) NDS

    b) VPN

    c) X.500

    d) LDAP

    e) AD

2. **Hogyan nevezik angolul az Active Directoryban a tároló objektumokat, amelyekben lehetnek erőforrás-objektumok és újabb tároló objektumok, hasonlóan a fájlok tárolására használt könyvtárszerkezethez? (1 pont)**

3. **Állítsa sorba az Active Directory telepítéséhez szükséges lépéseket! (3 pont)**

    a) Helyreállításra szolgáló rendszergazdai jelszó megadása.

    b) Új tartomány FQDN nevének megadása.

    c) A szerveren a hálózati beállításoknál a DNS címét módosítani kell 127.0.0.1-re.

    d) Meghatározható az AD adatbázisfájljainak, naplófájljainak és rendszerfájljainak helye.

    e) Újra kell indítani a szervert.

    f) Fix IP beállítása a szerveren.

g) dcpromo.exe elindítása.

h) Ha még nincs DNS a szerveren, most telepíthető.

4. Válassza ki azokat az elemeket, amelyek szükségesek ahhoz, hogy egy számítógép tartományba léptetése sikeres legyen! Több jó válasz lehetséges! (2 pont)

a) A beléptetni kívánt számítógépen Windows 7 rendszernek kell lennie.

b) A gép DNS beállításainál a szerver címének kell szerepelnie.

c) A számítógép újraindítása után a „Bejelentkezés ide” részben ki kell választani a tartományt.

d) A beléptetéshez rendszergazdai jogokkal kell bejelentkezni.

e) Az AD-ben fel kell venni egy felhasználót a „Tartományi beléptetés” csoportba.

5. Igaz-e a következő állítás? (1 pont)

Egy új felhasználó felvételekor megadható a bejelentkezési neve, jelszava, meghatározható, hogy jelszava soha nem jár, valamint korlátozható a bejelentkezés időtartama.

6. A home könyvtár hálózati megosztásakor milyen megosztási jogokat kell adni az *Everyone* beépített felhasználói csoportnak? Válassza ki a helyes megoldást! (1 pont)

a) Csak olvasási jog.

b) Olvasási és írási jog.

c) Teljes hozzáférési jog.

d) Módosítási jog.

e) Olvasási és végrehajtási jog.

7. **Mit jelent a home könyvtár meghatározásakor a *„\\W2k8S\Home\%username%”* adatban a %username%” meghatározás? A választ két szóban írja le! (1pont)**

10. 7. lecke: Csoportházirend (Group Policy)

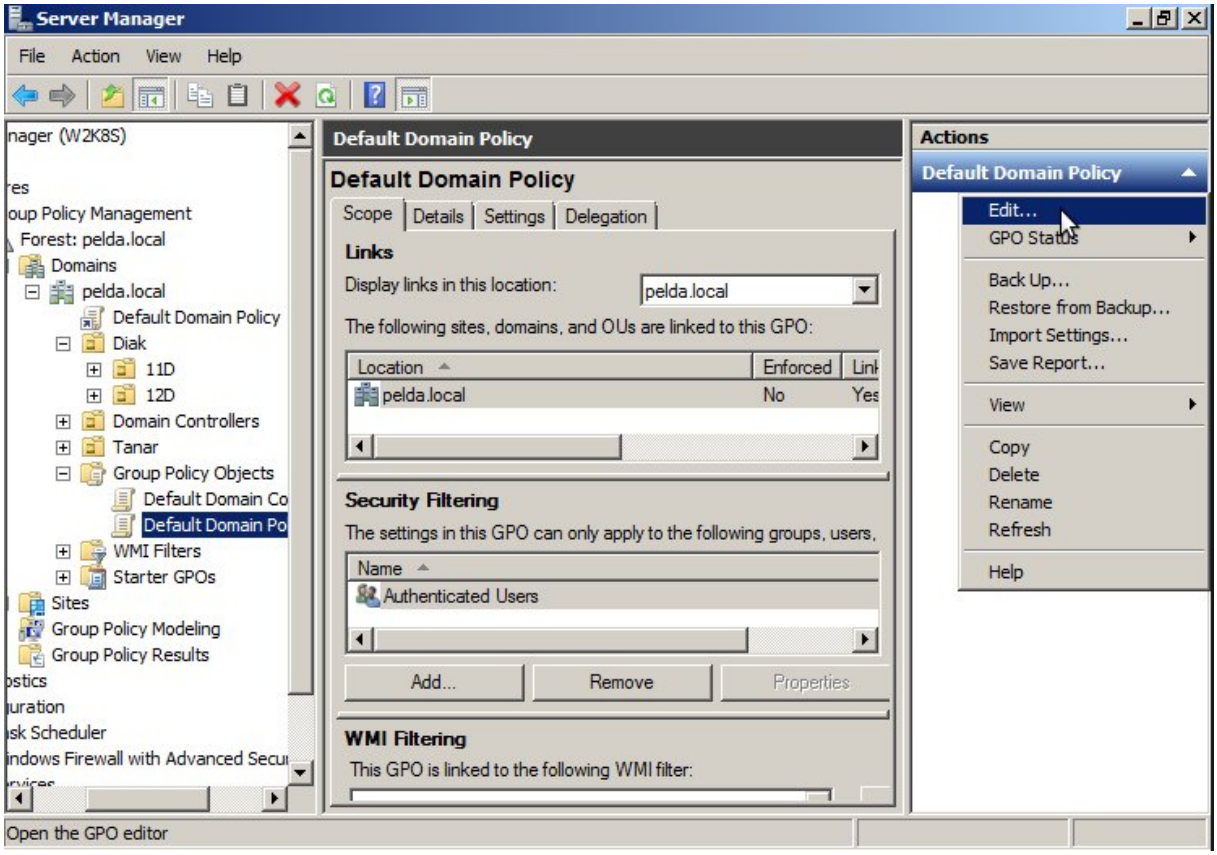
10.1 Részcélkitűzések

A tanuló legyen képes csoportházirendek kialakítására, módosítására különböző felhasználói csoportok részére. Ismerje a csoportházirenddel elvégezhető korlátozások és beállítások legfontosabb lehetőségeit, és legyen képes be is állítani azokat.

10.2 Alapfogalmak

Ez az Active Directory egyik leghatékonyabb eszköze a központi felügyelethez. Segítségével megoldható, hogy felhasználótól függően más és más beállítások legyenek érvényben egy windowsos számítógépen. Felhasználói csoportok vagy akár az összes felhasználó esetén letiltható a vezérlőpult, vagy beállítható az asztal háttere, vagy automatikusan csatolhatók hálózati meghajtók, elindíthatók tetszőleges programok, sőt telepíthetők is, illetve eltávolíthatók különböző alkalmazások is. Ráadásul mindezt úgy, hogy a rendszergazdának nem is kell leülnie a felhasználók számítógépe elé, néhány kattintás egy egységes felületen, és minden meg van oldva.

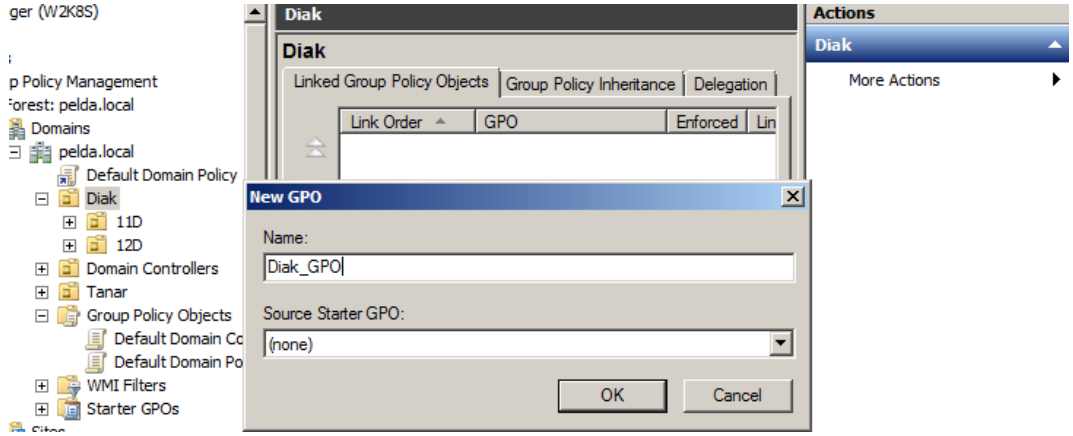
A csoportházirendek kezelését a *„Server Manager”* program segítségével lehet elvégezni. Az AD telepítésekor a *Features* elemek közé telepítésre került ez a szolgáltatás is. Használatához tudni kell, hogy minden szervezeti egységnek saját csoportházirendje (Group Policy Object – GPO) lehet, és a hierarchiában lejjebb lévők örökölhetik is a beállításokat. A legfelső szintű korlátozások mindenkire érvényesek lesznek, még a rendszergazdákra is. Ezt nevezik *„Default Domain Policy”*-nek, és módosítani (*Edit*) az alábbi ábrán látható módon lehet:



16. ábra. Default Domain Policy műveletek

Érdemes megjegyezni, hogy ezek a lehetőségek minden windowsos számítógépen rendelkezésre állnak, itt azonban a tartományi gépekre központilag lehet beállítani őket.

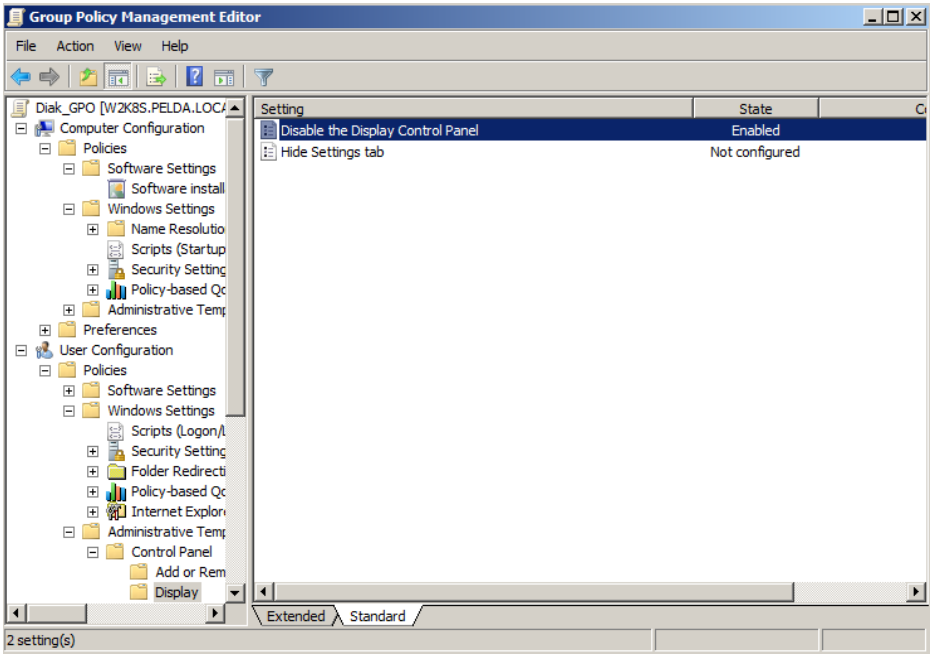
Ha szervezeti egységenként egyedi beállításokat szeretnénk, akkor először létre kell hozni egy GPO-t a szervezeti egységhez, és nevet kell adnunk neki. A létrehozáshoz válasszuk ki baloldalt a szervezeti egységet, majd jobboldalt a *„More Actions”* ikonra bal egérgombbal kattintva, a megjelenő menüből a *„Create a GPO on this Domain”* menüpontot. A megjelenő ablakban meg kell adni a GPO nevét.



17. ábra. GPO létrehozása egy szervezeti egységhez

Bármely GPO módosításához válasszuk ki baloldalt a *„Group Policy Objects”* listából, majd rajta jobb egérgomb és Edit. Ekkor elindul a *„Group Policy Management Editor”*, amelynek segítségével mindent be lehet állítani. Két fő csoportra oszlanak a beállítások, az egyikbe a számítógéphez kapcsolható („*Computer Configuration*”), a másikba a felhasználókhoz kapcsolható („*User Configuration*”) beállítások tartoznak.

A következő ábrán a GPO editor képernyője látható, ahol már le lett tiltva a *Diak_GPO*-n keresztül a *Vezérlőpult Display* beállítása. Ezek után, ha egy tartományi gépről a *Diak* szervezeten belüli felhasználóval jelentkezik be valaki, akkor ő már nem fogja tudni módosítani a Megjelenítés vezérlőpultot.



18. ábra. GPO editor munkában

Egyszer érdemes rászánni az időt, és végigböngészni a lehetőségeket, esetleg ki is próbálni azokat. Sok hasznos beállítást lehet találni, főleg az *„Administrative Templates”*-ek között.

11. 8. lecke: Login script

11.1 Részcélkitűzések

A tanuló legyen képes Login és Logout scriptek készítésére és beállítására. Legyen képes hálózati megosztások GPO-n keresztüli automatikus csatlakoztatására, meghajtóhoz való hozzárendelésére.

11.2 A login script (bejelentkezési parancsfájl) fogalma

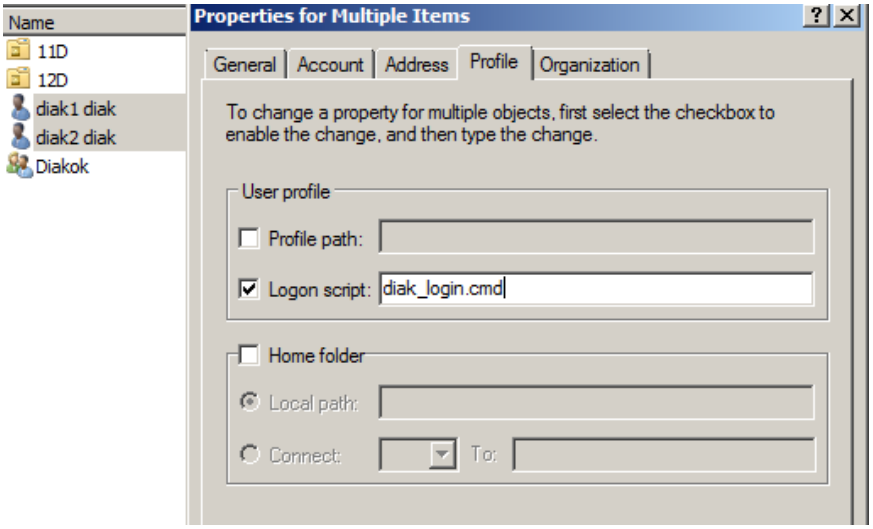
Sokszor előfordul, hogy bejelentkezéskor (*Login*) vagy kijelentkezéskor (*Logout*) automatikusan el kellene indítani egy programot a felhasználónál. Ebben tud segíteni a *„Logon/Logout Scripts”* lehetőség.

A script itt egy olyan szöveges fájlt jelent, amit a Jegyzettömbbel is szerkeszteni lehet. Tartalmazhat minden olyan utasítást, amit parancssorban is ki lehet adni. Elindíthat programokat, módosíthat fájlokat, törölhet, másolhat, bármit elvégezhet.

A parancsfájl maga a szerveren kerül tárolásra, de a végrehajtás a munkaállomáson történik, így a fájl tartalmának a munkaállomás környezetéhez kell igazodnia. Persze az is elképzelhető, hogy a végrehajtandó program vagy programok valamelyik kiszolgálón helyezkedik, helyezkednek el.

11.3 Felhasználóhoz rendelt login script

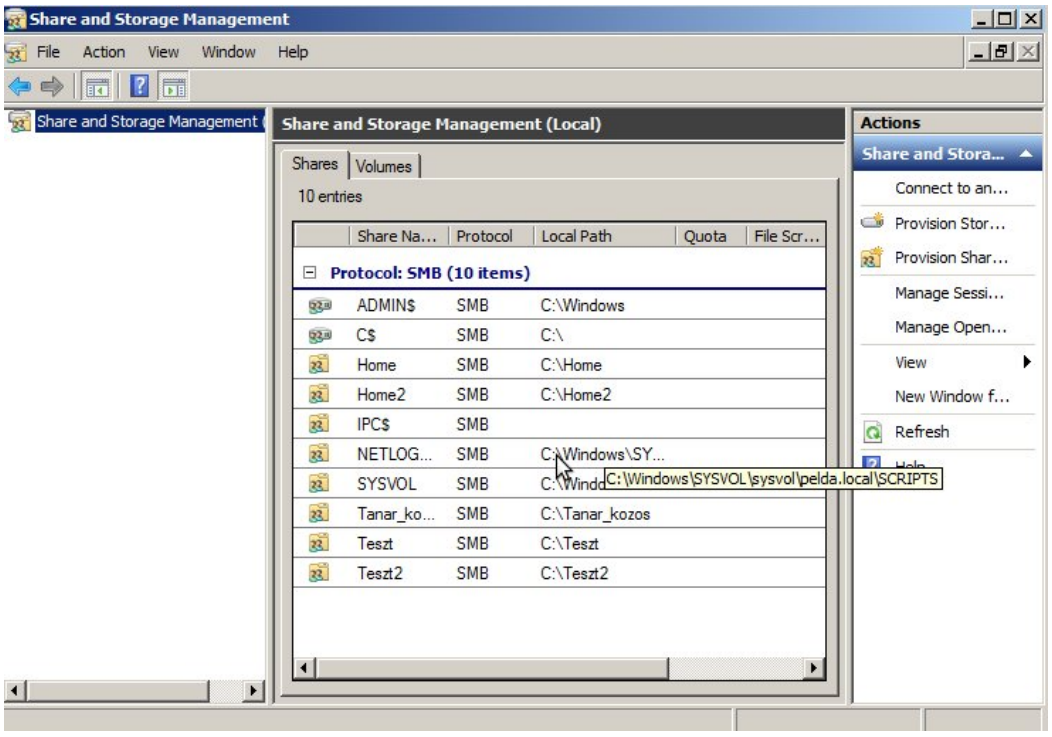
Minden egyes felhasználónak egyedi bejelentkezési parancsfájlt lehet készíteni. Persze nem kötelező, de ha szükséges, meg lehet oldani. Ezt a lehetőséget felhasználók csoportjainál is könnyedén lehet használni, a csoportos módosítási lehetőséget alkalmazva. Ha ugyanis több felhasználót jelölünk ki, majd ilyenkor állítjuk a jellemzőket (*Properties*), akkor egyszerre több felhasználónál is be lehet állítani a *„Logon script”*-et is. Persze egyszerre több felhasználót kiválasztva nem lehet minden jellemzőt módosítani.



19. ábra. Logon script beállítása egyszerre több felhasználónál

A példában mind a két diák felhasználóhoz a **diak_login.cmd** fájlnév került beállításra. A beállítás azt mondja meg, hogy a bejelentkezés után a kliens gép megkeresi a tartományi szerver *netlogon* megosztásában a **diak_logon.cmd** fájlt, letölti, majd végre is hajtja.

Ahhoz, hogy hol van a *netlogon* megosztás, ki is lehet tallózni, de egyszerűbb a szerveren megjeleníteni, vagy a „*Share and Storage Management*" programban, vagy parancssorban a „*net share*" paranccsal.



20. ábra. A *netlogon* megosztás megjelenítése

Ezen a szerveren a *netlogon* megosztás a következő könyvtárban van:

C:\\Windows\SYSVOL\sysvol\pelda.local\SCRIPTS

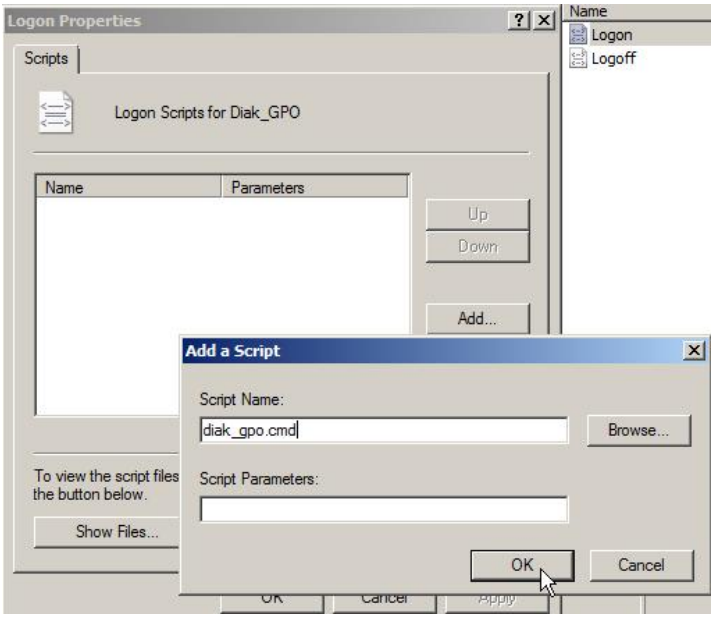
Ezek után már csak el kell készíteni a **diak_logon.cmd** fájlt a megadott könyvtárban. A fájlban csatolhatunk hálózati meghajtókat is, mint például a diákok közös elérési könyvtára (**Diak_kozos**). Ehhez a következőket kell a **diak_logon.cmd** fájlban elhelyezni:

net use K: *w2k8s**Diak_kozos*

11.4 Csoportházirendhez rendelt login script

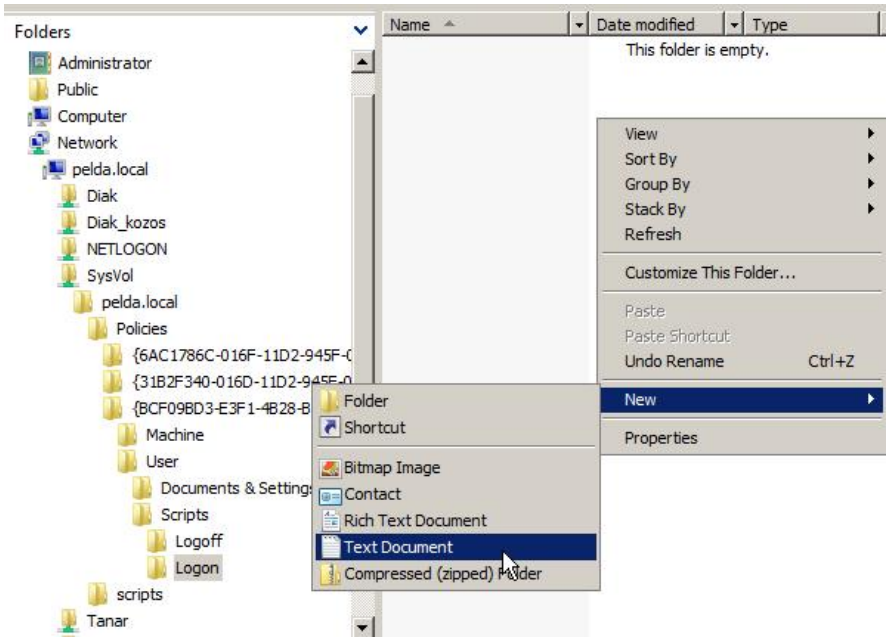
Kétféle login scriptet lehet állítani a csoportházirendben, az egyik magára a számítógépre vonatkozik, a másik a felhasználóra. Az első a *„Computer Configuration", Policies*, *„Windows Settings"* rész *Scripts* elemnél, a másik a *„User Configuration"*, *Policies*, *„Windows Settings"* rész *Scripts* elemnél található. A számítógépre vonatkozóan *Startup* és *Shutdown* scriptről beszélhetünk, míg a felhasználók esetén *Logon* és *Logout* scriptekről. A kettő között az a különbség, hogy *Startup* a számítógép elindulásakor hajtódik végre; míg a *Logon* a bejelentkezés után, a *Shutdown* a számítógép leállításakor, míg a *Logout* kijelentkezéskor.

A *Logon*-ra kattintva készíthetünk egy olyan parancsfájlt (.*cmd*), ami a bejelentkezés után automatikusan lefut a felhasználó számítógépén. Ehhez kattintsunk duplán a *Logon* szövegre, majd a megjelenő ablakban *Add…*, az újabb ablakban pedig adni kell egy nevet, jellemzően .*cmd* kiterjesztéssel. A példában a *Diak* szervezeti egység részére készítünk scriptet, ezért a neve **diak_gpo.cmd** lett.



21. ábra. Logon script készítése 1

Az *OK* gombbal bekerül a listába. Ezzel a lépéssel még nem készült el a script, csak a GPO-n belül vettük fel, mint hivatkozást. Létrehozni fájlrendszer szinten kell úgy, mint egy normál szöveges fájlt. Ehhez először a *„Show Files…"* gombot kell kiválasztani, majd a megnyíló fájlkezelőben létre kell hozni egy szöveges dokumentumot. A fájlkezelőben meg lehet nézni, hogy végül is hol kerül tárolásra a script.



22. ábra. Logon script készítése 2

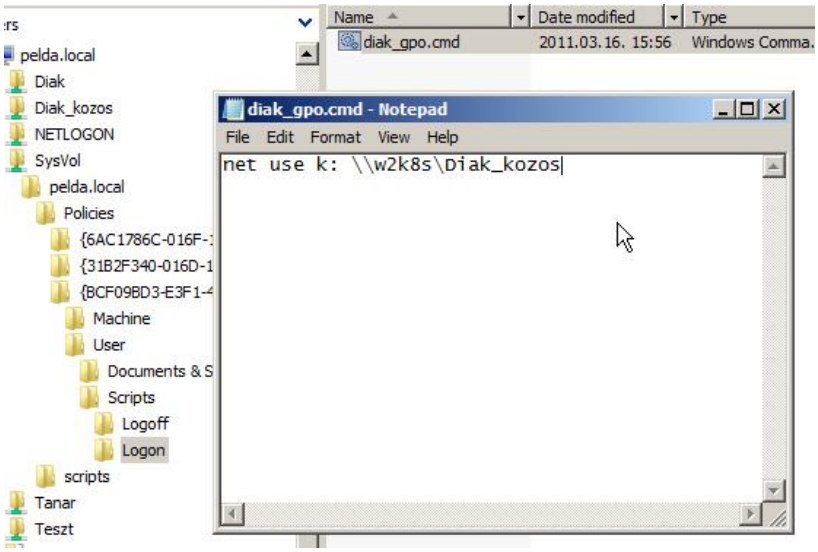
A létrehozás során figyeljünk oda, hogy a Windows 2008 se szakított azzal a csúnya megoldással, ami elrejti az ismert fájltípusok kiterjesztéseit. Így ha ezt nem kapcsoljuk ki, a létrehozott fájl neve **diak_gpo.cmd.txt** lesz, aminek az lesz a vége, hogy nem fog végrehajtódni, mert nem ezt állítottuk be. Kikapcsolni 2008 alatt is ugyanott lehet, mint XP alatt, a *Tools* menü, *„Folder Options”*, *View* fül, majd középen ki kell szedni a pipát a *„Hide extension for Known File Types”* sor elől.

A fájl szerkesztéséhez a fájl nevén jobb egérgomb, majd a gyorsmenüből *Edit*. A biztonsági figyelmeztető ablakban *Run*, majd a *Notepad* programmal szerkeszthetjük.

Az egyik leghasznosabb lehetősége a *Logon* scripteknek a hálózati meghajtók automatikus felcsatolása és meghajtóbetűjel hozzárendelése. Például ha azt szeretnénk, hogy a tanárok szervezet felhasználóinak minden bejelentkezés után legyen egy *K:* meghajtójuk, ami a kiszolgáló *Diak_kozos* megosztására mutat, akkor a következő sort kell elhelyezni a *Logon* scriptben:

net use k: \\w2k8s\Diak_kozos

Persze előtte meg is kell osztani a szerveren egy könyvtárat ilyen névvel, úgy, hogy a hozzáférési jogok is rendben legyenek.



23. ábra. Logon script készítése 3

A scriptben szerepelhet tetszőleges program indítása is, mint a Jegyzettömbbé (**Notepad.exe**) útvonal nélkül, csak a fájlnevet megadva. Ilyenkor a programnak valamelyik rendszerkönyvtárban kell lennie. De megadható teljes útvonallal bármilyen másik program is.

12. 9. lecke: Távtelepítés

12.1 Részcélkitűzések

A tanuló ismerje a távtelepítés fogalmát, lehetőségeit, jelentőségét, korlátait. Legyen képes **.msi** fájlok előállítására. GPO-n keresztül be tudja állítani a távtelepítést, adott számítógépcsoportok és felhasználók esetén.

12.2 Fogalma

A távtelepítés fogalma alatt két folyamatot is értünk. Egyik esetben úgy telepítjük fel magát az operációs rendszert, hogy nem használjuk a hagyományos telepítő CD-lemezt, helyette a hálózaton keresztül automatikusan hajtódik végre a telepítési folyamat. Ehhez vagy egy PXE-képes (hálózatról képes rendszert indítani) hálózati kártyára vagy egy speciális rendszerindító lemezre van szükség.

A másik jelentésében azt értjük távtelepítés alatt, amikor egy működő tartományi számítógépre úgy települnek fel alkalmazások, hogy a rendszergazda be se jelentkezik arra a gépre, ahol telepíteni kell. Minden csoportházirenden keresztül, automatikusan zajlik. A továbbiakban erről a lehetőségről lesz szó.

12.3 Jelentősége

Ha egy felhasználó több számítógépen is be szokott jelentkezni, akkor a távtelepítési szolgáltatással megoldható, hogy ahol bejelentkezik, automatikusan települjön egy alkalmazás.

Nagyon kényelmes megoldást jelent ez a szolgáltatás akkor, ha egyszerre sok számítógépre kell telepíteni egy programot.

12.4 Korlátai

A távtelepítési szolgáltatás csak és kizárólag ***msi*** fájlokat tud kezelni. Az *msi* kiterjesztésű fájlok csak olyan windowsos gépen futtathatók, ahol van

már telepítve *„Windows Installer”* szolgáltatás. Az *msi* fájlok gyakorlatilag telepíthető programok, csak önmagukban nem futtathatók.

Ha a telepítendő programnak nincs *msi*-s változata, akkor készíteni kell ilyet, ha a távtelepítési szolgáltatással szeretnénk telepíteni. Létezik erre a feladatra ingyenes program is:

http://www.advancedinstaller.com/downloads/advinst.msi

12.5 Beállítása

A távtelepítésre váró alkalmazásoknak készíteni kell egy könyvtárat, amit meg is kell osztani mindenki számára, célszerűen csak olvasásra. Ebbe a könyvtárba pedig bele is kell másolni az *msi* alkalmazásokat.

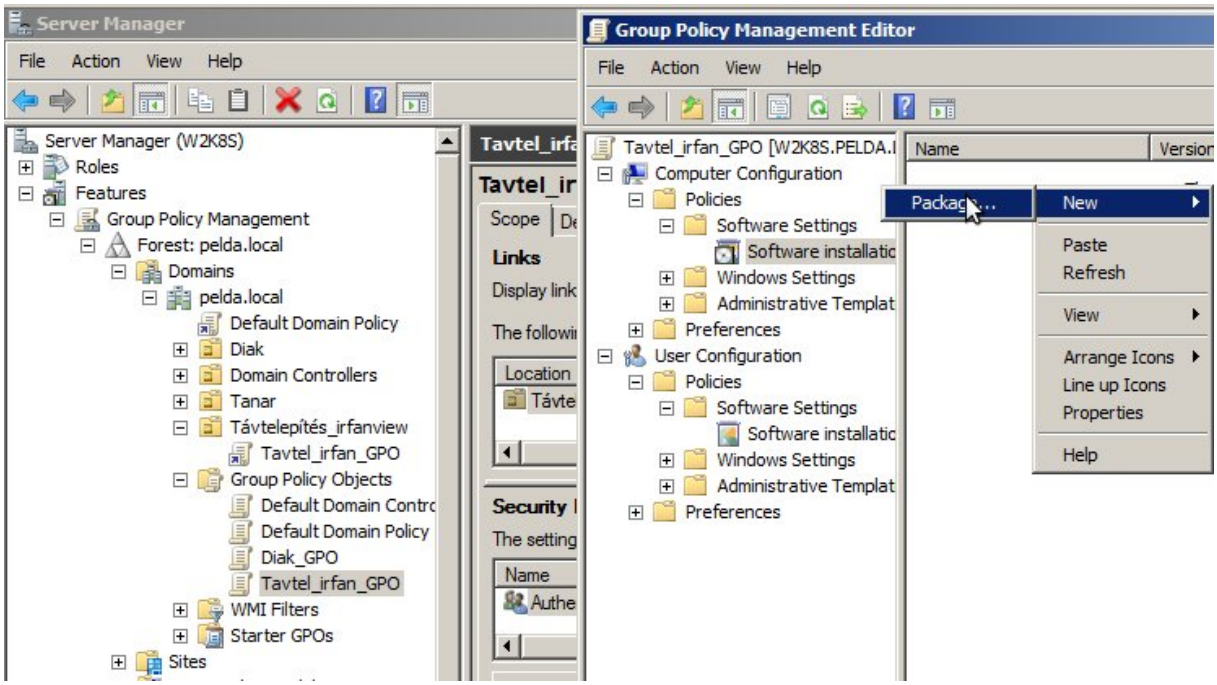
A példában készült egy **Tavtel** könyvtár a C: egység gyökerében, ahová bemásolásra került az *Irfanview* nevű program aktuális telepítője, átkonvertálva exe-ből msi-re, **irfanview_setup.msi** névvel.

A beállítás előtt el kell döntenünk, hogy számítógéphez vagy felhasználóhoz kívánjuk kapcsolni a telepítést. Mindkét esetben célszerű egy új szervezeti egységet létrehozni, és a szükséges elemeket (számítógépek, felhasználók) ebbe belemozgatni. Persze figyelni kell arra is, hogy volt-e más GPO beállítva az elemekhez. Sokkal kezelhetőbb az az eljárás, amikor a különböző korlátozásokat felhasználói objektumokhoz (felhasználókat tartalmazó szervezeti egységhez) kapcsoljuk, míg a távtelepítést kizárólag a számítógépekhez (számítógépeket tartalmazó szervezeti egységekhez). Ilyenkor ugyanis csak a számítógép-objektumokat kell mozgatni, és jó esetben azokhoz nincs külön GPO beállítva.

A *„Server Manager”* program *„Group Policy Management”* fülön belül ki kell választani a módosítani kívánt GPO-t, vagy ha nincs, akkor létre kell hozni.

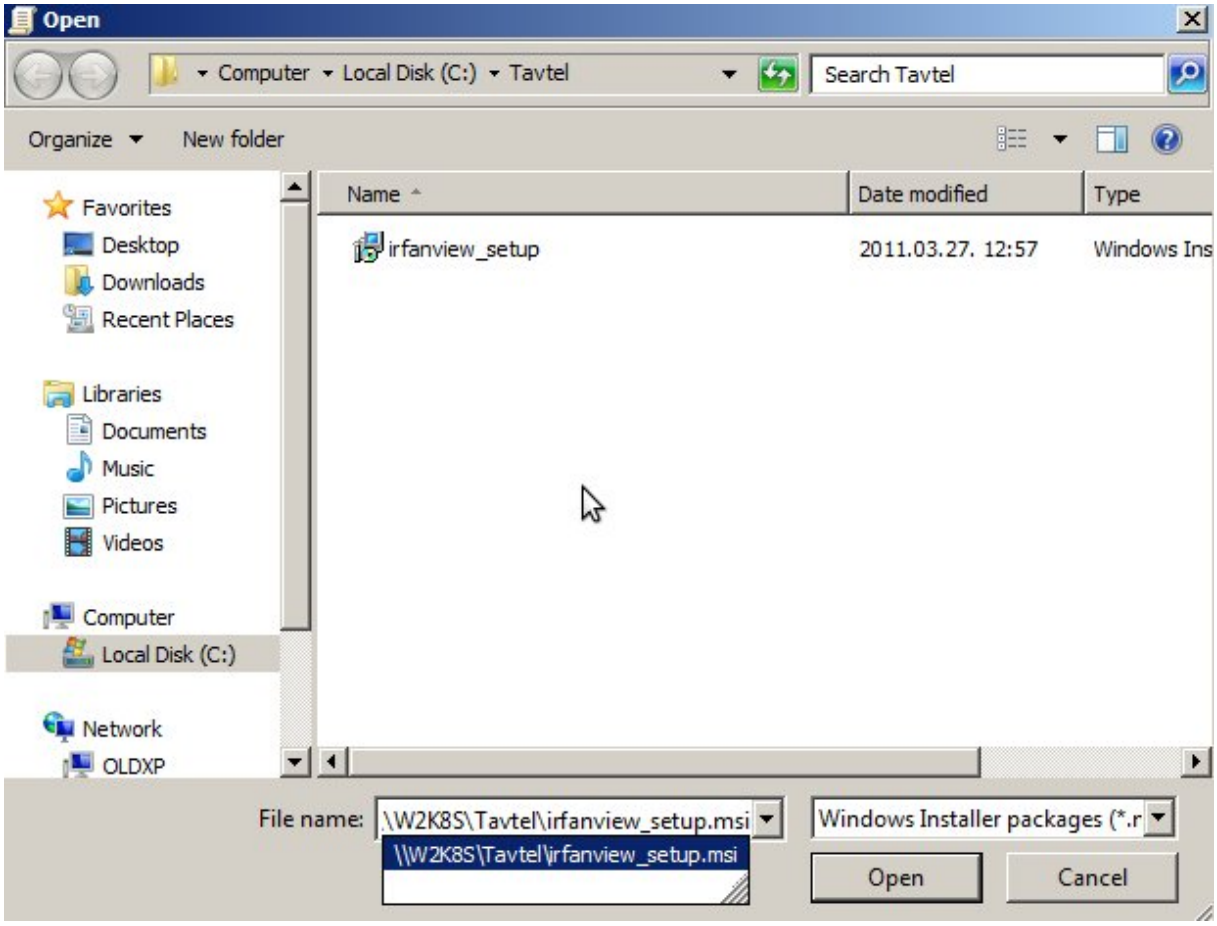
A példában létrehozásra került egy *„Távtelepítés_irfanview”* szervezeti egység, amelybe át lett mozgatva a tartományi számítógép, ahonnan a felhasználók bejelentkeznek. Valamint a szervezeti egységhez létre lett hozva egy *Tavtel_irfan_GPO* nevű GPO is.

Azt is el kell dönteni, hogy hogyan is szeretnénk telepíttetni az alkalmazást. Ha bejelentkezés előtt, akkor a *„Computer Configuration”*, *„Software Settings”*, *„Software Installation”* részben, ha konkrétan egy felhasználóhoz szeretnénk kötni, akkor a *„User Configuration”*, *„Software Settings”*, *„Software Installation”* részben kell beállítani úgy, hogy hozzáadunk egy új csomagot (*Package*).



24. ábra. Távtelepítés, új csomag hozzáadása

A következő lépésben ki kell választani a csomagot. Itt azonban figyelni kell arra, hogy hálózati elérési úttal határozzuk meg azt.



25. ábra. Távtelepítés, fájl kiválasztása

A következő lépésben válasszuk az *Assigned* (kijelölt) elemet. Ezután a rendszer készen áll arra, hogy az adott számítógépen a bekapcsolás után az *irfanview* alkalmazás automatikusan települjön. A telepítés minden esetben SYSTEM felhasználói fiókkal történik, vagyis független az aktuálisan bejelentkező felhasználótól.

Egy GPO esetén már az is beállítható, hogy milyen felhasználók esetén kerüljön érvényesítésre a GPO. Alapesetben a hitelesített felhasználók (*„Authenticated Users”*) esetén jut érvényre. Ha szükséges, ez módosítható, eltávolítható az *„Authenticated Users”,* és bármilyen felhasználó vagy felhasználói csoport hozzáadható a *„Security Filtering”*-nél.

13. 10. lecke: II. témazáró feladatsor

1. **Minek a rövidítése a GPO? (1 pont)**

2. **Válassza ki azt az elemet, amelyiken beállítva valamilyen korlátozást, az mindenkire érvényes lesz a tartományon belül! Egy jó válasz van! (1 pont)**

    a) Group Policy

    b) Server Manager

    c) Default Domain Policy

    d) Group Policy Object

    e) Root Policy

3. **Igaz-e a következő állítás? (1 pont)**

    Egy szervezeti egység létrehozásakor automatikusan létrejön egy GPO.

4. **Hogy nevezik azt a megosztást, ahol a felhasználóhoz kapcsolt Logon scriptet el kell helyezni? (1 pont)**

5. **Szeretnénk elérni, hogy a w2k8s tartományi szerver felhasználóinál bejelentkezés után automatikusan csatolásra kerüljön a C:\Közös, közvetlenül „Kozos” névvel megosztott könyvtár a Z: egységhez. Melyik az a parancs, ami ezt el tudja végezni egy login scriptben? Válassza ki a helyes megoldást! (1 pont)**

    a) net share Kozos Z:

    b) net use \\w2k8s\Közös Z:

    c) \\w2k8s\Kozos Z: Link

    d) net use Z: \\w2k8s\Kozos

6. **Melyik csoportházirend lehetőséget választaná, ha azt szeretné, hogy a script a felhasználó kijelentkezésekor fusson le? Egy jó válasz van! (1 pont)**

    a) A „Computer Configuration” rész „Startup” beállítást.

    b) A „Computer Configuration” rész „Logout” beállítást.

    c) A „User Configuration” rész „Startup” beállítást.

    d) A „User Configuration” rész „Logout” beállítást.

    e) A „Computer Configuration” rész „SShutdown” beállítást.

7. **Elindítható-e egy logout scriptből egy játékprogram? (1 pont)**

8. **Milyen alkalmazásokat lehet tartományi környezetben a távtelepítési szolgáltatással telepíteni? Válassza ki a helyes megoldást! (1 pont)**

    a) Azokat, amelyeket egyetlen .exe fájl segítségével lehet telepíteni.

    b) Csakis Microsoft Installer (MSI) formátumú programokat.

    c) Bármilyen Windows alkalmazást.

    d) Csakis olyan programokat, amelyeket nem kell külön telepíteni.

9. **Igaz-e a következő állítás? (1 pont)**

    A távtelepítési szolgáltatással telepített alkalmazások mindig azzal a felhasználóval települnek, aki aktuálisan be van jelentkezve.

10. **Válassza ki, hogy melyik beállításba kell elhelyezni a szoftver telepítést, ha azt szeretnénk, hogy bejelentkezés nélkül kerüljön telepítésre! Egy jó válasz van! (1 pont)**

    a) A *„User Configuration”*, *„Software Settings”*, *„Software Installation”* részben.

b) A Vezérlőpult „Távtelepítés szolgáltatás” programban a „Automatic Installation” beállításban.

c) A megfelelő GPO *„Authenticated Users” „Security Filtering” beállításnál.*

d) A *„Computer Configuration”*, *„Software Settings”*, *„Software Installation”* részben.

14. 11. lecke: Biztonsági másolatok

14.1 Részcélkitűzések

A tanuló legyen tisztában a biztonsági másolatok készítésének fontosságával, lehetőségeivel. Ismerje a teljes és növekményes mentés fogalmát, szerepüket, alkalmazásukat, a mentési stratégia kialakításának jelentőségét. Tudjon önálló mentési stratégiát kidolgozni, ismerje a mentésre szolgáló hardver- és szoftvereszközöket. Legyen képes Windows Server mentésének beállítására, automatizálására. Ismerje az Image fájl fogalmát. Ismerje a klónozás fogalmát. Legyen képes egy adott számítógépet klónozni. Ismerje a Linux rendszerekben használható mentési eljárásokat, használatukat.

14.2 Mentési eljárások

Egy számítógépes rendszerben bármikor előfordulhatnak olyan hardver- és szoftvermeghibásodások, akár szándékos rongálások is, amelynek során fontos és kevésbé fontos adataink is megsérülhetnek, akár el is veszhetnek. Pótolhatatlan adataink védelme érdekében ajánlatos rendszeresen biztonsági másolatokat készíteni róluk.

Egy másolat készülhet kézzel vagy automatikusan is. A **kézi másolat** készítésének lényege, hogy a rendszergazda vagy a felhasználó más helyre is elmenti a fontosabb állományokat. Ez a más hely lehet pendrive, CD/DVD lemez vagy egy másik számítógép a hálózaton.

Az **automatikus mentés** során előre beállított helyekről (könyvtárak), előre meghatározott célterületre, adott vagy rendszeres időközönként történik mentés.

A mentések során az **időközök** mellett még azt is el kell dönteni, hogy **teljes mentés** vagy **növekményes mentés** készül. A teljes mentés során minden alkalommal minden fájl mentésre kerül, függetlenül attól, hogy változott-e annak tartalma. Növekményes esetben pedig csak azok kerülnek mentésre, amelyek a legutolsó mentés óta megváltoztak. A gyakorlatban a két eljárás kombinációját érdemes használni. Mondjuk vasárnap éjjel készül egy teljes mentés, míg naponta csak növekményes mentéseket alkalmazunk.

Figyelembe kell venni azt is, hogy ha a csütörtöki állapotra van szükségünk ezekből a mentésekből, akkor egymás után vissza kell állítani a legutolsó vasárnapi mentést, majd utána sorban a hétfői, keddi és szerdai mentéseket is. Ez időigényes lehet, vagyis megfontolandó, hogy hogyan is alakítjuk ki a mentési stratégiát.

14.3 Mentési eszközök

A mentési eszközök között vannak szoftver- és hardvereszközök is. A „mivel” kérdésre „szoftverrel” a válasz, míg a „hova” kérdésre „valamilyen hardverre” a válasz.

A **szoftverek** között vannak az operációs rendszerbe épített eszközök, vannak külön megvásárolható professzionális programok, és vannak teljesen ingyenes programok is.

A **hardvert** tekintve a pendrive nem egy archiváló eszköz, nem ez az elsődleges feladata. A pendrive-ok elsősorban adatok hordozására valók, adatok biztonsági másolatait már nem célszerű hosszabb távon rajtuk tárolni.

Mentési célra azonban már használhatók a **CD/DVD/BlueRay lemezek**. A mentést végző szoftverek egy része is képes kezelni célként, azonban nagyobb mennyiségű adatok esetén már beavatkozást igényelhet a használata (lemezt kell cserélni).

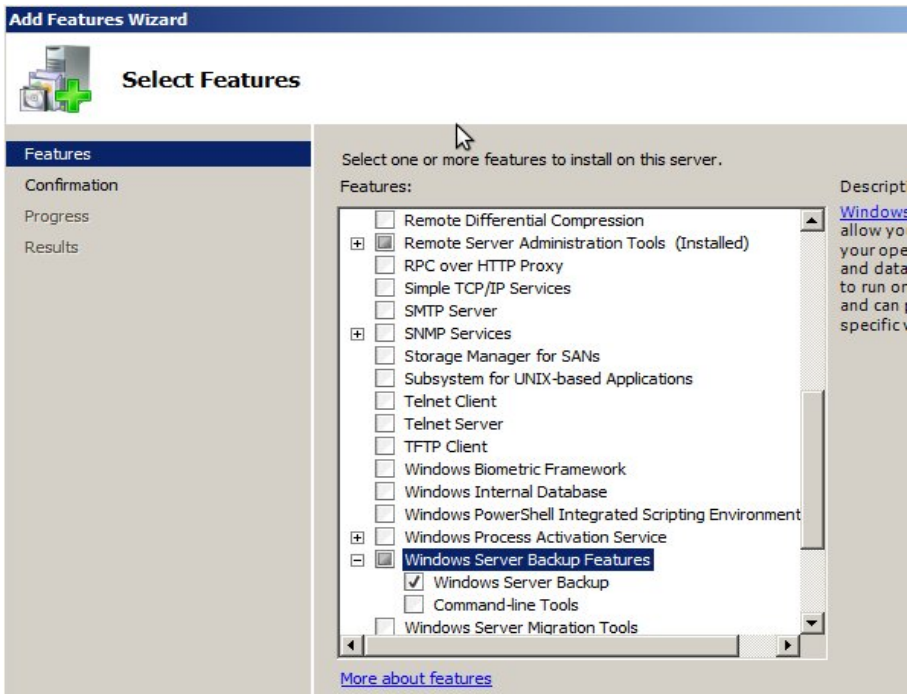
Menthetünk **merevlemez**re is, ami lehet akár ugyanabban a számítógépben is, amiről mentést szeretnénk készíteni. Azonban vegyük figyelembe, hogy biztonsági szempontból mentünk, és ebben az esetben, ha az adott számítógéppel történik valami, akkor a mentésnek is annyi. Ezért legalább másik számítógépre készítsük a mentést, vagy legalább másoljuk át máshova is. A szoftverek többsége erre is képes.

Hagyományosan a mentést **szalagos egység**ekre szokták elvégezni. A mai napig megbízható tároló eszköz. Maga a szalag viszonylag olcsó, azonban a szalagos egység elég drága. Ráadásul mindenképpen külön szoftverre van szükség ahhoz, hogy szalagos egységekre tudjunk menteni.

14.4 Beépített mentési szoftverek

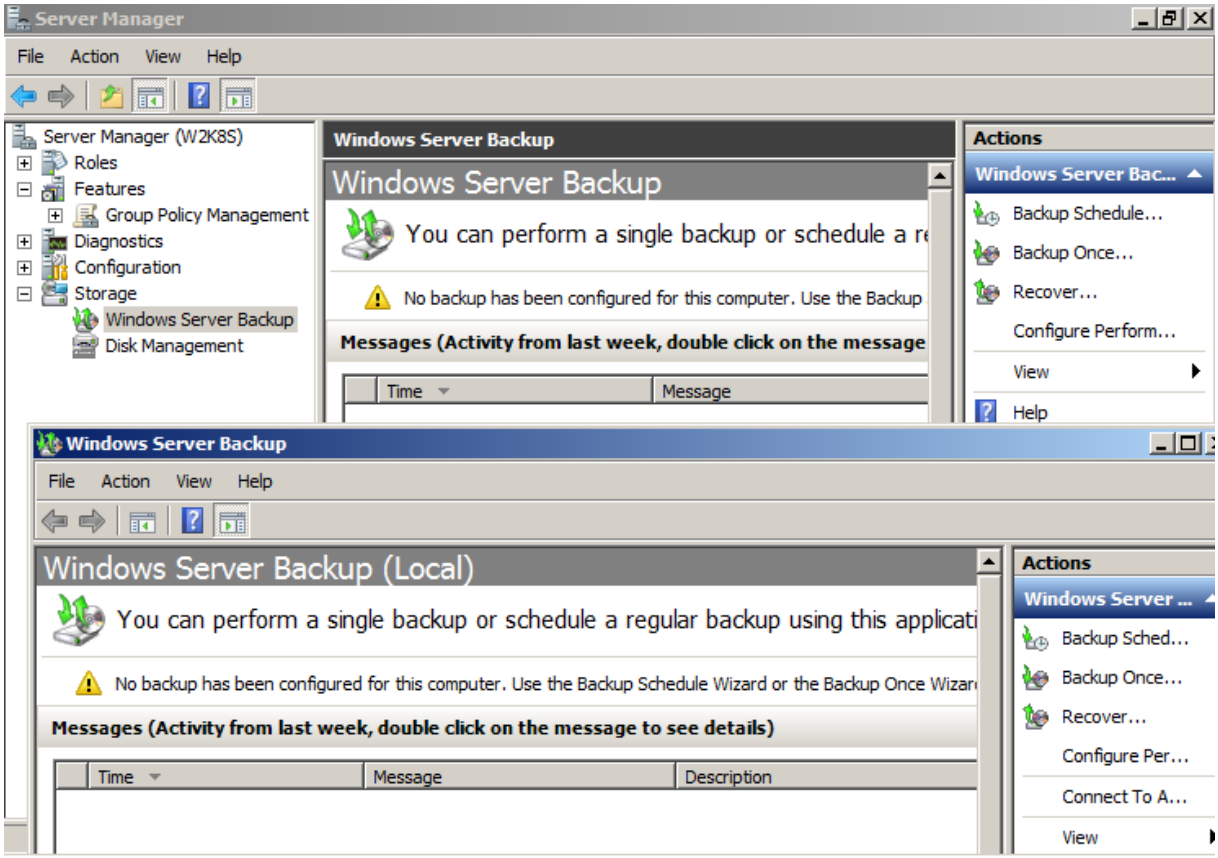
Az eddigi Windows változatokon a mentést és visszaállítást az ntbackup.exe program segítségével lehetett elvégezni. A Windows 2008 Server esetében azonban egy új alkalmazás vette át a szerepét, amit külön szolgáltatásként kell telepíteni.

A telepítést a „*Server Manager*” program segítségével végezhetjük el. A *Features* résznél, *Add* majd a listában ki kell választani a „*Windows Server Backup Features*” elemet.



26. ábra. Mentési szolgáltatás telepítése

A telepítés után a „*Windows Server Backup*” elérhető a „*Server Manager*” programból is, de külön is elindítható az „*Administrative Tools*” menü „*Windows Server Backup*” ikonnal.

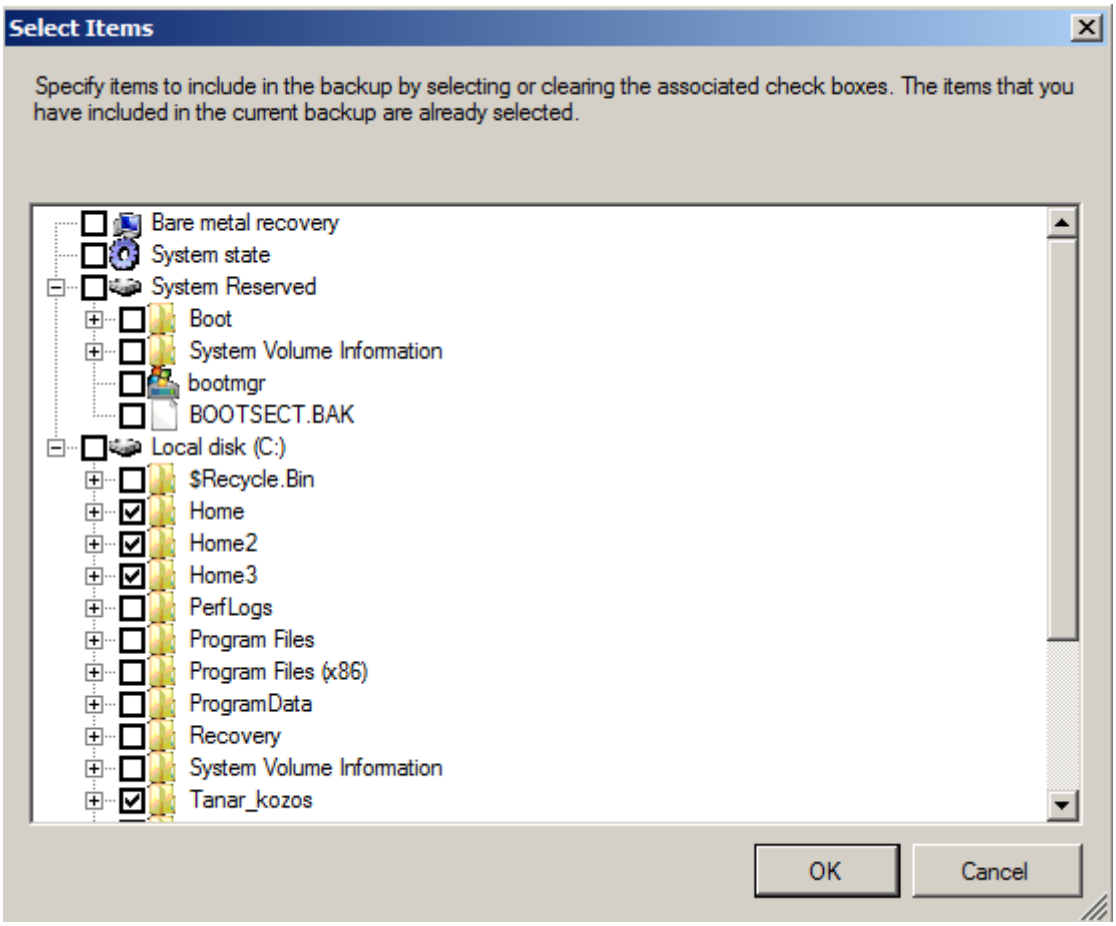


27. ábra. Windows Server Backup

Új mentés beállításához válasszuk ki jobboldalt a „*Backup Shedule Wizard…*” elemet. A megjelenő ablak végigvezet a legfontosabb beállításokon.

Választható a teljes szerver mentése is („*Full Server”*), amivel mindent, még a rendszerfájlokat is le lehet menteni. Az **ntbackup**-pal ezt nem lehetett. A *Custom* beállítás segítségével mi választhatjuk ki, hogy mely könyvtárak tartalma kerüljön mentésre.

Custom beállítás esetén a következő lépésben az „*Add Items*” gombbal a rendszer bármely könyvtárát, fájlját vagy akár külön kijelölhetjük a rendszer állapotának mentését is, illetve a rendszer védett részének mentését is hozzáadhatjuk a mentési listához.



28. ábra. Mentési elem hozzáadása

Ugyanott az „*Advanced Settings*” gombbal kivételeket vehetünk fel a listára, amiket a rendszer nem fog menteni.

Következő lépésben beállítható a mentés ideje („*Ones a day*”) vagy a rendszeres mentés („*More than once a day*”) időpontjai.

Ezután meghatározható a mentés típusa. Itt három lehetőség közül lehet választani:

- Külön merevlemezre mentünk, ami csak erre a célra van a rendszerben (ezt ajánlja) – „*Back up to a hard disk that is dedicated for backups*”.
- Egy adott könyvtárba ment – „*Back up to a volume*”. Figyeljünk rá, hogy nem lehet menteni arra a meghajtóra, ahol a rendszer van (C:, valamint csak NTFS-re formázott helyre menthetünk).
- Egy megosztott hálózati meghajtóra ment – „*Back up to a shared network folder*”.

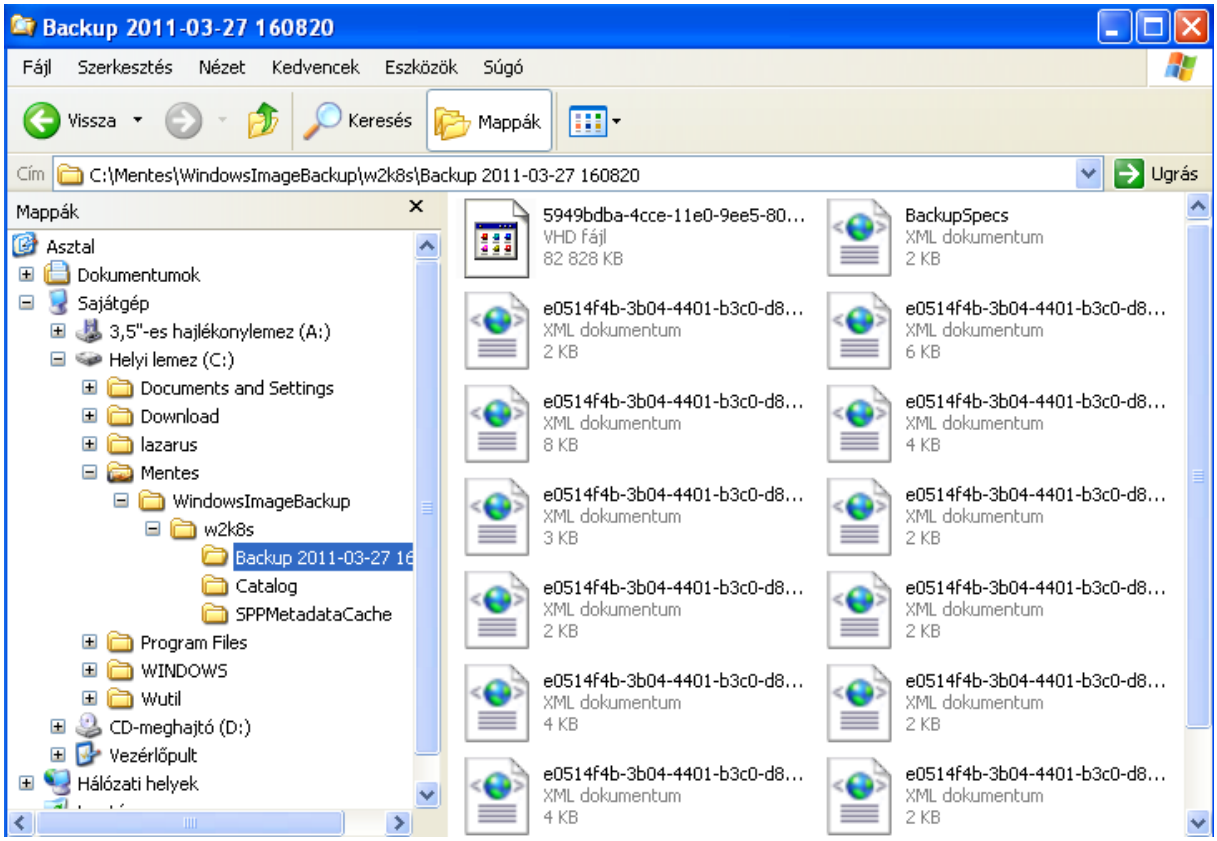
Végül megadható, hogy milyen felhasználóval hajtsa végre a mentést, illetve próbáljon meg csatlakozni a beállított megosztáshoz. Figyeljünk arra is, hogy a felhasználónak vagy az *Administrators* vagy a *„Backup Operators”* csoport tagjának kell lennie! A megosztott mappa jogosultságait is eszerint kell beállítani!

Készíthetünk egyszeri mentést (*„Backup Once…”*) is, ami a beállított konfigurációnak megfelelően azonnal elkészíti a mentést.

A program segítségével akár más tartományi számítógépek mentése is elvégezhető (*„Connect to Other Systems”*), ami óriási könnyebbséget jelent a rendszergazda számára.

14.5 Image fájlok

A mentés eredménye egy összetett könyvtárszerkezet egy **.vhd** fájllal és több **.xml** állománnyal.



29. ábra. A mentés eredménye

A **.vhd** kiterjesztésű fájl tartalmazza mindazokat a könyvtárakat és fájlokat, amiket a mentéshez beállítottunk. Ez olyan, mint egy speciális tömö-

rített állomány. A VHD egy virtuális merevlemez (*Virtual Hard Disc*), amit virtuális gépekben is fel lehet használni.

14.6 Ghost

A rendszergazdák körében a **Ghost** ma már egy külön fogalom. Segítségével egy számítógép merevlemezének teljes tartalmát vagy csak egyetlen partícióját lehet egyetlen fájlban eltárolni, majd akár egyszerre, több másik gépre visszaírni. Gyakran alkalmazzák akkor, ha ugyanazt a rendszerkörnyezetet kell gyorsan előállítani egyszerre sok – célszerűen azonos hardverű – számítógépen. Ezt a műveletet hívják klónozásnak.

Mivel a klónozás során a merevlemez tartalma kerül másolásra, ezért operációs rendszertől függetlenül lehet alkalmazni, vagyis bármilyen rendszert lehet klónozni.

Maga a Ghost egy program, teljes neve a **Norton Ghost**. Jelenleg a 15.0 verziónál tart; fizetős program, használata viszont egyszerű. A hálózat bármely számítógépére fel lehet telepíteni, de akár CD-ről, floppyról, pendrive-ról is lehet futtatni.

A klónozás menete kétlépéses folyamat. Első lépésben elmentjük a forrásszámítógép merevlemezének adatait, majd a második lépésben klónozzuk akár több számítógépre is.

14.6.1 A mentés lépései

- Készítünk Ghost programmal egy boot lemezt (lehet floppy, CD vagy USB eszköz is), amivel el lehet indítani a számítógépeket.
- Kiválasztunk egy számítógépet, melyre feltelepítünk minden szükséges szoftvert (operációs rendszer, alkalmazások), és ki is próbáljuk azokat.
- Elindítjuk a Ghost programot azon a számítógépen, amelyikre feltelepítettük. Beállítjuk, hogy fogadjon adatokat, vagyis menteni fogunk.
- Elindítjuk a forrásszámítógépet a külön elkészített boot lemezről, majd elindítjuk róla magát a Ghost programot.

- Beállítjuk, hogy mit mentsünk (teljes merevelemez vagy csak egy partíció), majd kiválasztjuk a mentési számítógépet, mint célállomást.
- Végül elindítjuk a mentést. A menteni kívánt tartalomtól függően akár 30 perc is lehet a mentés.
- A mentés eredménye egyetlen fájl lesz azon a gépen, melyre fel lett telepítve a Ghost program.

14.6.2 A klónozás lépései

- Elindítjuk a feltelepített Ghost programot, majd beállítjuk, hogy küldjön adatokat, és kiválasztjuk, hogy melyik fájl tartalmát szeretnénk küldeni, illetve az is meghatározható, hogy hány gépre szeretnénk egyszerre küldeni, majd elindítjuk. A tényleges munkához a beállított számítógépnek be is kell csatlakoznia, addig nem indul el az adattovábbítás.
- A boot eszközről elindítjuk mindegyik gépet, amire másolni szeretnénk, majd egyenként be is csatlakozunk a küldő számítógépre (megadjuk az IP-címét).
- Ha minden gép elindult és be is csatlakozott, akkor elindulhat a másolási folyamat. Ez kicsit lassabb lehet, mint a mentés, de előnye, hogy nem kell külön gépenként elvégezni a telepítési folyamatokat.

Több ingyenes program is létezik ugyanezen feladatok ellátására, de a legkönnyebben használható program a **DriveImage XML**, ami jelenleg a 2.22-es verziónál tart. Az ingyenes változat a következő oldalról tölthető le:

http://www.runtime.org/driveimage-xml.htm

14.7 Mentés Linux alatt

Linux alatt a legegyszerűbb mentési eszköz a tar parancs. Segítségével akár a teljes fájlrendszer tartalmát egyetlen fájlba lehet elmenteni, akár rögtön tömörítve is. Például a **tar** következő formája készít egy másolatot

a */etc* könyvtár teljes tartalmáról *etc.tar.gz* névvel a parancs kiadásának helyén:

tar –cvpzf etc.tar.gz /etc

A **tar** parancsnak sok kapcsolója van. Ezek közül hasznos lehetőség a kizárás (--*exclude*). Segítségével ki lehet hagyni akár komplett könyvtárakat is a visszaállításból. A következő példában az *etc.tar.gz* mentésből nem kerül visszaállításra a */etc/apt* könyvtár tartalma:

tar –cvpzf etc.tar.gz /etc --exclude ”/etc/apt”

A Ghosthoz hasonló, Linuxon használható ingyenes megoldásból több is van, de kiemelkedik közülük a **partimage** program. Segítségével könnyedén lehet bármilyen partíciót vagy akár a teljes merevlemezt is egyetlen fájlba menteni helyi vagy hálózati tárhelyre. Ugyancsak a Ghost funkcióit kívánja megvalósítani a **G4L** (**Ghost for Linux** – http://sourceforge.net/projects/g4l/) program, ami szintén ingyenes, ráadásul hálózaton keresztül képes több gép klónozására is.

Éles, vagyis éppen működő rendszer mentésére használható a **Mondo**, ami két programot tartalmaz, a *mondoarhive*-t és a *mondorestore*-t. Segítségükkel hasonló funkciókat lehet megvalósítani, mint a „*Windows Server Backup*” programmal.

Ezen felül sok ingyenes program áll rendelkezésre Linuxon különböző mentési feladatokra. A következő oldalon még rövid leírást is lehet találni róluk:

http://www.thefreecountry.com/utilities/backupandimage.shtml

15. 12. lecke: Dokumentálás

15.1 Részcélkitűzések

A tanuló értse a dokumentálás szükségességét. Ismerje az Informatikai szabályzat szerepét, szükségességét, legyen tisztában a hálózati dokumentációk fajtáival. Legyen képes önállóan készíteni egy adott környezetben hálózati dokumentációkat. Legyen tisztában a szoftverek nyilvántartásának szükségességével. Legyen képes licence nyilvántartás készítésére.

15.2 Mit és miért kell dokumentálni?

A „Mit” kérdésre a rövid válasz: MINDENT!

Gondoljunk bele abba a helyzetbe, hogy új munkahelyre kerülünk, ahol van egy működő, több szerverrel üzemelő, akár 100 számítógépet is tartalmazó hálózat. Éppen ma kezdtünk, és nem megy a levelezés. Nincs dokumentáció, senki nem tud semmit, az előző rendszergazda egyik napról a másikra távozott, és nem hagyott maga után semmilyen információt. Nem tudunk semmit a hálózatról, a gépeken lévő operációs rendszerekről, programokról, nem tudjuk, hogy a dolgozók milyen programokat futtatnak, milyen hálózati erőforrásokat használnak, nem ismerjük a hálózat szerkezetét, nem ismerjük a szerverekhez tartozó hozzáféréseket, jelszavakat.

Ilyen esetben a hiba elhárítása akár napokba is kerülhet. Ha a vállalatnál addig nincs levelezés, akkor az komoly pénzkiesést is jelenthet, hiszen a cég akár megrendelésektől is eleshet.

Nemcsak azért van szükség dokumentációra, mert esetleg majd az utódnak szüksége van rá, hanem saját magunknak is fontos. Előfordulhat az is, hogy elfelejtünk valamit, például egy rendszergazdai jelszót, és így nem tudunk hozzáférni valamelyik szerverhez.

Ugyancsak előfordulhat az is, hogy egy külső vállalkozás készítette a hálózat kábelezését, és nem dokumentálta, egyszerűen fogalma sincs senkinek, hogy egy bizonyos kábel pontosan merre is van.

A „Miért” kérdésre a válasz, hogy megkönnyítse a saját és a többi informatikus életét, valamint meggyorsítsa a hibakeresést, csökkentse az állásidőt, vagyis pénzt takarítson meg.

15.3 Informatikai szabályzat

Az előző problémák elkerülése érdekében a vállalatok – saját érdekükben – Informatikai szabályzatban rögzítik mindazt, ami az informatikai rendszerük működésével kapcsolatos. Rögzítik, hogy ki mit tehet, illetve kinek mit kell tennie a napi tevékenysége során. Ki kell térni a dokumentációk készítésére, hozzáférhetőségére is.

Az Informatikai szabályzatnak tartalmaznia kell mentési és katasztrófa-helyreállítási tervet is. Egy ilyen szabályzatban sok minden lehet, de mindenhol egyedileg készítik.

15.4 Hálózatdokumentálás

A számítógépes hálózat szempontjából kétféle dokumentációt érdemes készíteni: fizikai és logikai dokumentációt.

A fizikai dokumentáció az épületek, szintek alaprajzán mutatja, a kábelek, fali aljzatok, huzalozási központok elhelyezkedését, hasonlóan a villamos hálózatok rajzához. A fali kábelek végpontjait minden esetben azonosítani kell, ez rendszerint egy számmal történik. A fizikai dokumentáción ezeket a végponti azonosító számokat is fel kell tüntetni.

A hálózat működése szempontjából érdekes a logikai dokumentáció. Ezen a rajzon a felhasználói számítógépek, szerverek, aktív eszközök (HUB, switch, router), egymáshoz való viszonyát, kapcsolódását kell feltüntetni, jelölve az IP-címtartományokat, egyedi IP-címeket, elnevezéseket (DNS, NETBIOS), és szolgáltatásokat.

15.5 Hozzáférések dokumentálása

A rendszerek legfontosabb felhasználóinak (rendszergazda, administrator, root stb.) neveit és jelszavait is ajánlott dokumentálni. Ennek tárolására azonban különösen oda kell figyelni, ugyanis ennek birtokában bármit

meg lehet tenni a hálózaton. Ha viszont nincs dokumentálva, akkor különleges helyzetekben komoly fennakadásokat okozhat.

15.6 Szerverszolgáltatások dokumentálása

Érdemes szerverenként külön rögzíteni, hogy az adott szerver milyen szolgáltatásokat lát el, és azt is, hogy milyen céllal, milyen kapcsolatai vannak más szerverekkel.

Az egyes szolgáltatások legfontosabb beállításait is érdemes dokumentálni, azzal együtt, hogy miért is így lettek beállítva. Sok esetben konfig fájlrészleteket is tartalmazhat a dokumentáció.

15.7 Szoftverdokumentálás

Ajánlatos összeírni, hogy az egyes számítógépeken milyen operációs rendszerek futnak, illetve milyen alkalmazásokat használnak. Néhány esetben szükség lehet arra is, hogy az egyes alkalmazások követelményeit is rögzítsük. Például mennyi memória kell a futtatáshoz, vagy szükség van-e a helyes futtatáshoz egy webszerverre a helyi hálózaton stb.

Külön nyilvántartást kell vezetni az operációs rendszerek és alkalmazások licence-eiről.

15.8 Tevékenységek dokumentálása

Kritikus helyeken a rendszergazda minden tevékenységéről dokumentációnak kell készülnie. Mikor, honnan, melyik gépre jelentkezett be és miért, valamint milyen feladatokat végzett el és milyen céllal.

15.9 A dokumentációt megkönnyítő eszközök

A fizikai és logikai rajzok készítéséhez használhatók egyszerű rajzprogramok is, de sokkal hatékonyabb, ha legalább folyamatábra-készítő programokat használunk, mint a Visio vagy a Dia. A Diához ráadásul van hálózati ikon gyűjtemény is.

Léteznek programok, amelyek képesek összegyűjteni a hálózaton lévő számítógépek IP-címeit, neveit, megosztásait, valamint olyan is, ami a routereket is feltérképezi, és képes azonnal egy logikai hálózati rajzot ké-

szíteni. Az utóbbi kategóriában professzionális programok is léteznek, de a szolgáltatásaikat meg kell fizetni.

16. 13. lecke: Windows rendszerek távoli elérése

16.1 Részcélkitűzések

A tanuló ismerje a távoli elérés fogalmát, szükségességét. Ismerje a fontosabb alapfogalmakat és rövidítéseket. Legyen képes beállítani Windows Server 2008 estén a távoli asztal kapcsolatot. Legyen képes másik gépről csatlakozni is a szerverhez. Legyen képes beállítani a webes távoli asztal kapcsolatot. Böngészővel is tudja kezelni távolról a szervert, ismerje az ingyenes és fizetős távoli elérési szolgáltatások néhány lehetőségét.

16.2 Fogalmak

Egy szerver rendszerint egy jól elkülönített helyen van, amihez nem lehet egyszerűen csak úgy leülni. Ezért kiemelkedő fontosságú lehetőség az, hogy hálózaton keresztül is el lehessen érni úgy, mintha ott ülnénk előtte.

Windows környezetben azonban a távelérési szolgáltatás alatt mást értenek. Ott a távelérési szolgáltatás azt jelenti, hogy a távoli gép úgy csatlakozik az interneten keresztül a szerverhez és hálózatához, mintha ő is a tagja lenne. Ezt nevezik még **VPN**-nek, vagyis „**Virtual Private Network”**-nek, virtuális magánhálózatnak is.

Windowsban a távoli elérést **Távoli asztal kapcsolat**nak (**Remote Desktop Service - RDS**) nevezik, mivel a távoli gépen is elérhetővé válik a Windows asztala. Lehetőség van azonban grafikus felület nélküli elérésre Windows alatt is, ilyenkor távolról kapunk egy parancssort, amellyel bármilyen parancsot kiadhatunk. A Windows Core szerverek esetén nincs is más lehetőség.

Linux szerver környezetben többnyire nem jellemző a grafikus felület, így ott egyszerűen távoli bejelentkezésről beszélünk, aminek eredményeképpen kapunk egy shellt, ahol ugyanúgy dolgozhatunk, mintha ott ülnénk a szerver konzolja előtt. Persze itt is van lehetőség a grafikus felület távoli

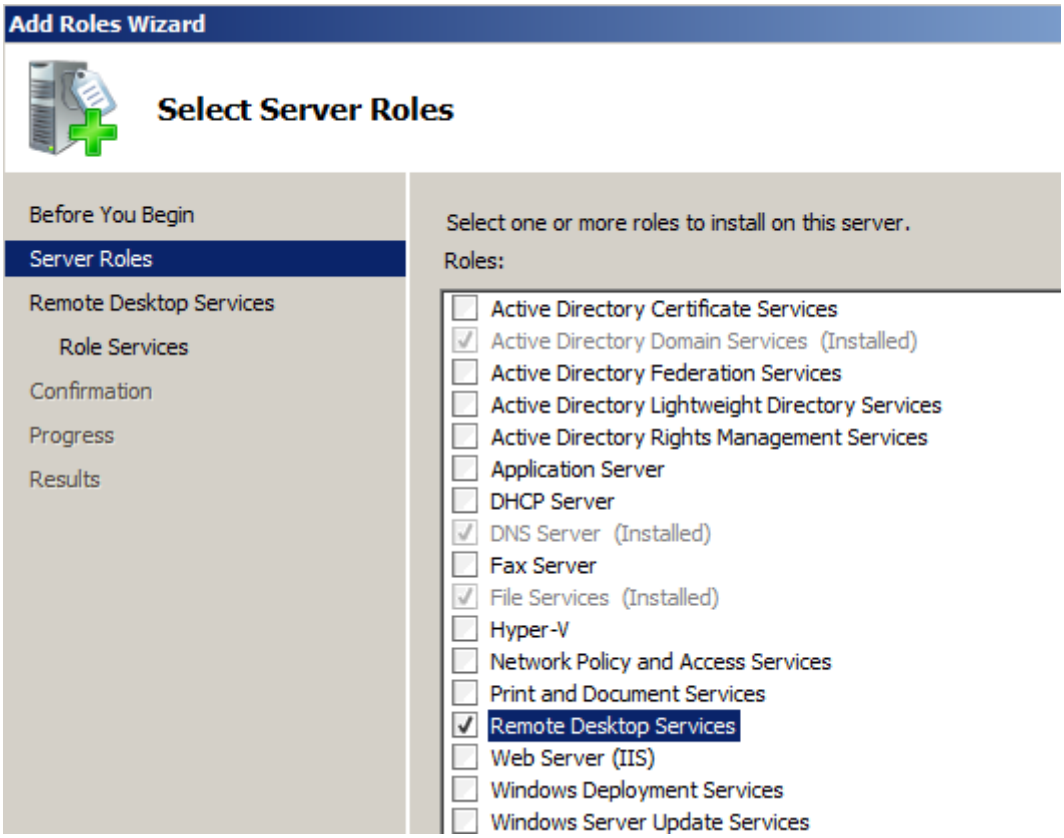
elérésére, amit Távoli asztal megjelenítésnek („**Remote Desktop Viewer**”) neveznek.

A távoli eléréshez ismerni kell a távoli gép IP-címét, és annak a portnak a címét, ahol a távoli elérési szolgáltatás elérhető. A port címe függ a programtól is, de van olyan, ahol nem módosítható az alapértelmezett port, és van olyan, ahol igen. Ezenkívül szükség van arra is, hogy megbízhatóan azonosítsuk magunkat a távoli elérés során. Ehhez persze ismerni kell egy feljogosított felhasználói nevet és jelszót is.

A távoli elérés akkor jelenthet problémát, ha az elérni kívánt számítógép egy routerrel leválasztott helyi hálózaton van, és az elérés kívülről, az interneten keresztül történne. Ekkor ugyanis nem lehet megadni az elérni kívánt gép címét, mivel az helyi cím, és kívülről közvetlenül nem lehet elérni. A problémára a megoldás a portátirányítás (**Port Forward**). Ilyenkor a routeren be kell állítani, hogy ha egy adott portra kapcsolódnak kívülről, akkor azt a forgalmat továbbítsa a belső hálózat adott gépe és portja felé. A külső port lehet ugyanaz is, mint a belső, de lehet különböző is. Ilyenkor persze a távoli kapcsolódásnál a router IP-címét és a külső portot kell megadni a kliensen, feltéve, ha van rá lehetőség, hogy más portot is meghatározzunk.

16.3 Beépített távoli asztal kapcsolat telepítése

Ez a szolgáltatás minden Windows operációs rendszernél adott. Windows 2008 Server esetén telepíteni kell a szolgáltatást a „*Server Manager*” program *Roles* fülén, az „*Add Roles*” elemmel. A listából először ki kell választani a „*Remote Desktop Service*”-t.



30. ábra. Távoli asztal kapcsolat telepítése 1

A következő lépésben csak *Next*. Ezután a „*Role Services*”-nél ki kell választani a „*Remote Desktop Session Host*”-ot. Erre megjelenik egy ablak, ahol nem ajánlja a telepítését az Active Directory-val. Mi most telepítjük („*Install Remote…*”).

Ismét *Next*, majd megint választani kell, hogy a biztonságosabb, de nem minden klienssel működő azonosítást („*Require Network Level Authentication*”), vagy a kevéssé biztonságos, de minden klienssel működő („*Do not require Network …*”) módot választjuk. Válasszuk az utóbbit.

A licence-elés módját határozhatjuk meg a következő lépésben. Külön licence-ekre (hozzáférési engedélyekre) van szükség ahhoz, hogy a szervert távolról is el lehessen érni. Ez vagy a szerverhez kapcsolódik („*Per Device*”), vagy a kliensekhez („*Per User*”).

Ezután a hozzáférést szabályozhatjuk. Alapesetben csak az *Administrators* csoport tagjai fogják tudni használni a szolgáltatást. Nekünk most ez jó így.

Következő lépésben a klienshozzáférés specialitásait lehet beállítani, de itt sem kell semmit állítani.

Végül *Install*, aminek hatására települ a szolgáltatás.

A telepítés végén újra kell indítani a szervert.

Az újraindítás után még folytatja a beállításokat, és csak miután bejezte, lehet csatlakozni távolról.

16.4 Beépített távoli asztal kapcsolat használata

A távoli számítógépen el kell indítani a „*Távoli asztal kapcsolat*” programot, ami XP esetén a Kellékek között található. Itt meg kell adni az elérni kívánt számítógép IP-címét, valamint célszerű beállítani, hogy milyen névvel szeretnénk csatlakozni a géphez. Ehhez a „*Beállítások…*” gombra kell kattintani, ami után több beállítási lehetőség is elérhetővé válik. A hozzáférési névhez „*domain**név*” – jelen esetben a „*PELDA**Administrator*” vagy a „*pelda.local**Administrator*” – alakot kell használni akkor, ha tartományi felhasználóval szeretnénk csatlakozni.

Ha a bejelentkezési névnél nem adjuk meg a domain nevét, akkor helyi felhasználóval fogunk csatlakozni a szerverre.

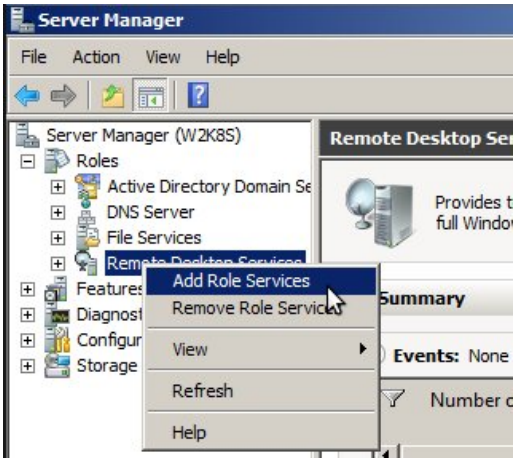
A Csatlakozás gomb hatására teljes képernyős módban kapunk egy bejelentkező ablakot – ami ugyanaz, mint a szerveren magán –, ahol még választhatunk felhasználót, vagy meg is adhatjuk azt, valamint a jelszavát. A sikeres bejelentkezés után a távoli gép asztalát látjuk, ahol ugyanúgy dolgozhatunk, mintha a távoli gép előtt ülnénk. Az ablak felső részén van a kezelőfelület, ahol elérhető a kilépés is.

31. ábra. Távoli asztal kapcsolat bejelentkezés

16.5 Webes felület

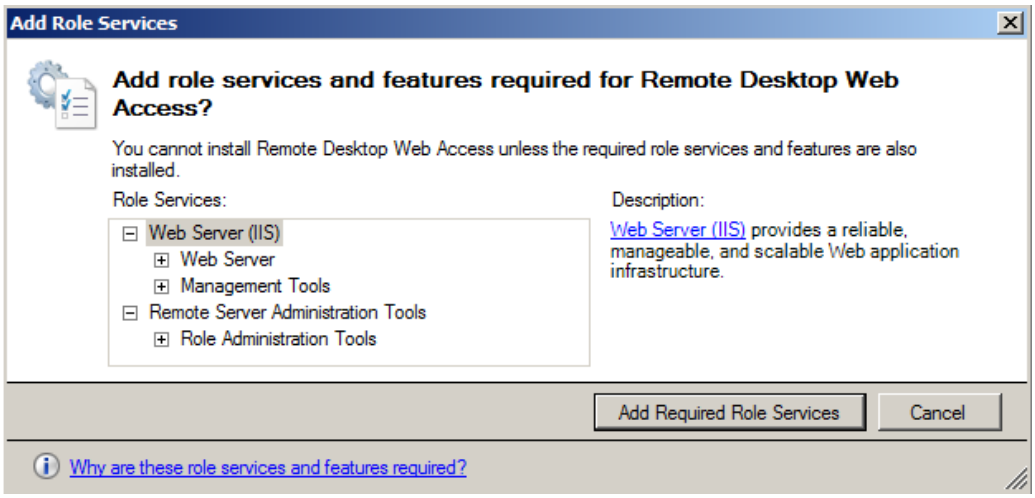
Ez a lehetőség akkor hasznos, ha a távoli gépen nincs olyan program, amivel távoli asztal kapcsolatot lehetne felépíteni. A szerveren ehhez telepíteni kell a „*Remote Desktop Services*” szolgáltatáson belül a „*Remote Desktop Web Access*” szolgáltatást.

Ha már telepítve van az RDS, akkor a nevén jobb egérgombbal előjövő menüben kell kiválasztani az „*Add Role Services*” menüpontot.



32. ábra. Távoli asztal webhozzáférés telepítés 1

A Web Access szolgáltatást kiválasztva a telepítő felajánlja a szükséges elemek telepítését („*Web Server (IIS)*”), mivel a szolgáltatáshoz szükség van webszolgáltatásra is.

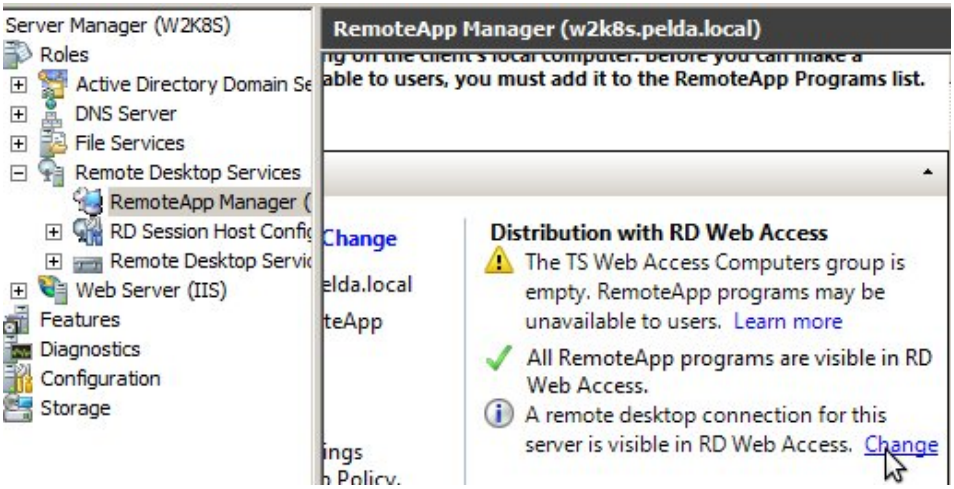


33. ábra. Távoli asztal webhozzáférés telepítés 2

A Web Server szolgáltatás jellemzőit is részletesen be lehet állítani. Csak akkor módosítsunk, ha tudjuk, mit csinálunk!

A telepítés végén kapunk egy figyelmeztetést, ami emlékeztet minket arra, hogy a helyes működéshez még konfigurálni kell a *RemoteApp* szolgáltatást is, amivel meg lehet határozni, hogy távolról milyen programokat lehet majd elindítani, illetve milyen felhasználók tehetik azt meg. A „*RemoteApp Manager*” felületen középen lent hozzá kell adni az alkalmazásokat.

Ezenkívül engedélyezni is kell a „*Remote Desktop Web Access*”-t a *Change* linkkel.



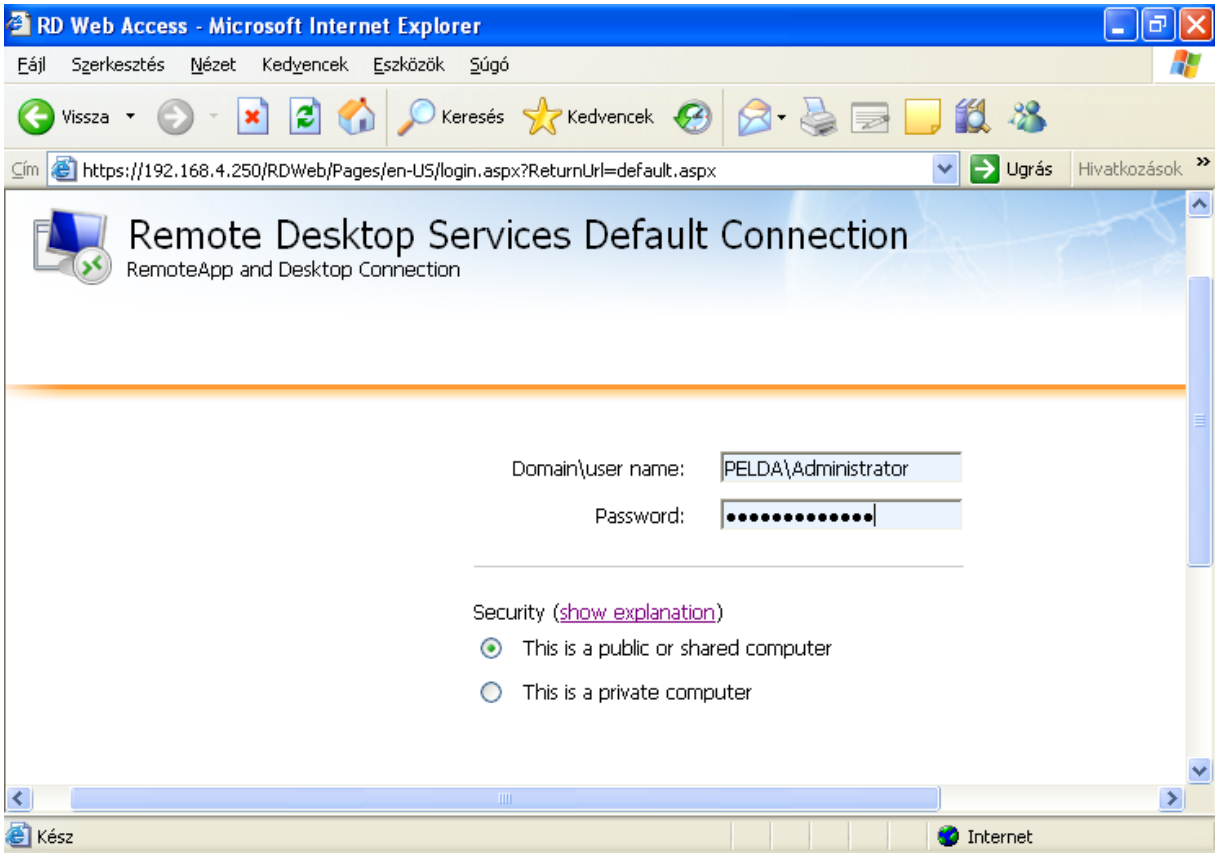
34. ábra. Távoli asztal webhozzáférés engedélyezése

Be kell még állítani, hogy kinek, kiknek vagy milyen számítógépről lehessen hozzáférni a rendszerhez a böngészőn keresztül. Ezt a Users szervezeti egységben megjelent „TS Web Access Computers” csoporthoz való hozzáadással lehet szabályozni.

Ezek után már lehet is csatlakozni böngésző segítségével egy távoli gépről. Címnek a következőt kell írni:

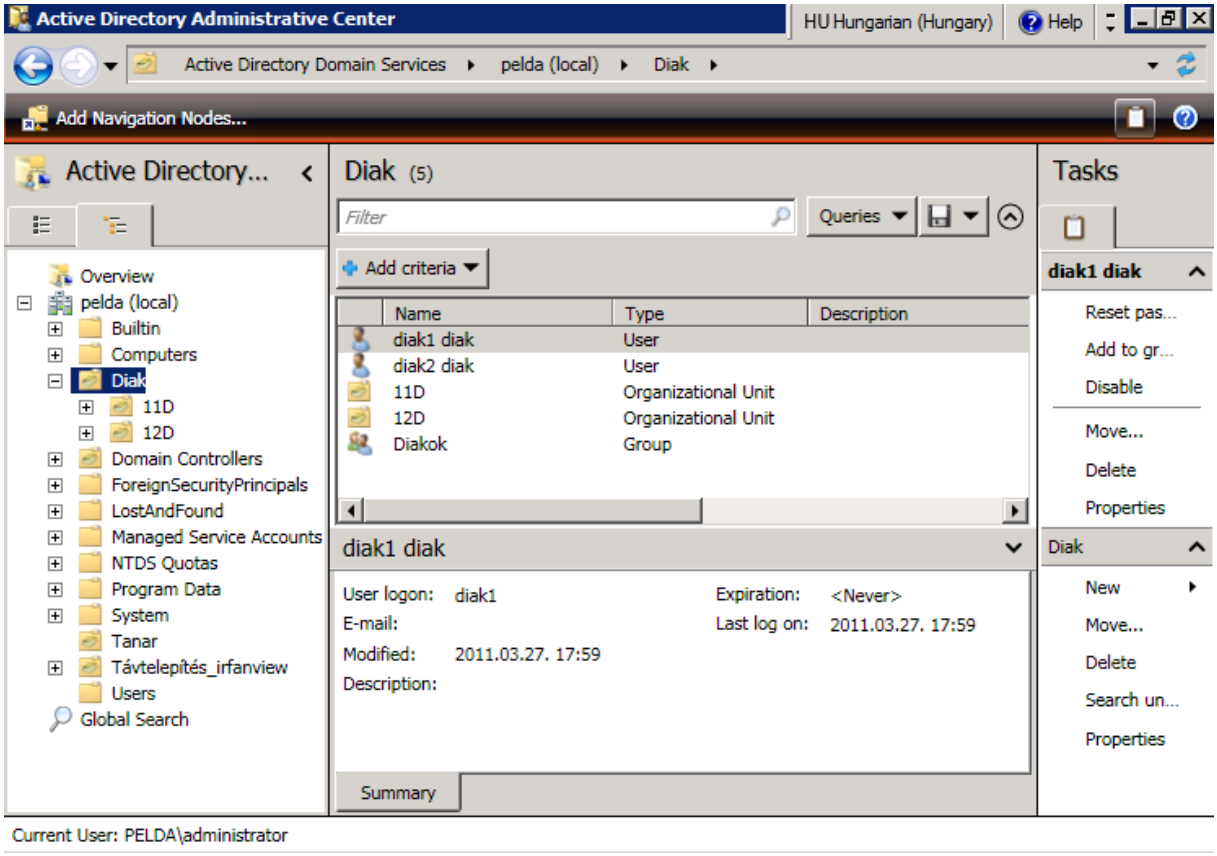
http://IPCím/RDWeb, aktuálisan http://192.168.0.250/RDWeb

Meg kell adni a hozzáférés adatait, domain\felhaszn formában.



35. ábra. Webes távoli asztal kapcsolat bejelentkezés

A bejelentkezés után megjelennek az engedélyezett programok ikonjai. Akármelyiket választjuk ki, egy figyelmeztetést kapunk, ahol a RemoteApp alkalmazás üzen, hogy egy webhely távoli kapcsolatot próbál indítani. A „Csatlakozás” gombot kiválasztva még egyszer azonosítani kell magunkat. Mivel a szerveren még nincs hitelesített tanúsítvány, ezért egy újabb figyelmeztetést kapunk. Az „Igen” hatására elindul a RemoteApp alkalmazás, ahol a „Részletek” gombra kattintva láthatóvá válik a távoli asztal. Kicsit később megjelenik a kiválasztott alkalmazás, és úgy dolgozhatunk, mintha a szerver előtt ülnénk.



36. ábra. Munkában a webes távoli asztal kapcsolat

Az egyetlen probléma a webes táveléréssel kapcsolatban, hogy csak windowsos gép alól működik.

16.6 VNC

A VNC egy ingyenesen elérhető szoftvercsomag, amelynek segítségével bárhonnan el lehet érni egy gép asztalát. A szoftver egyik része a szerveren fut, a másik része pedig a távoli gépen. Több VNC változat is van (UltraVNC, TightVNC, RealVNC, stb), amelyik csak Windowson használható (UltraVNC), és van, ami a legtöbb platformon (Win, Linux, Mac).

A szerveren telepíteni kell a szerverváltozatot, majd a kliensen el kell indítani a Viewert, amivel majd csatlakozni lehet a szerverhez. A csatlakozáshoz ismerni kell a távoli gép IP-címét, és annak a portnak a címét, ahol az szolgáltat. A port címe alapesetben 5000, de ez módosítható. Lehetőség van egyedi azonosítók használatára, de az is beállítható, hogy a szerver valamelyik létező felhasználójával azonosítsuk magunkat.

16.7 RAdmin

A Remote Admin (RAdmin) csak egy a sok, fizetős program közül, amivel a távoli elérést meg lehet valósítani. Ezt is telepíteni kell a szerverre. A kliensen pedig ugyanúgy meg kell adni a távoli gép IP-címét és a csatlakozáskor használni kívánt felhasználó nevét és jelszavát.

16.8 Logmein

Ez egy igen különleges szolgáltatás, azonban sokan félnek az alkalmazásától, a távoli elérés ugyanis egy külső szerveren keresztül történik.

Használatához be kell regisztrálni a következő oldalon:

http://logmein.com

Azokon a gépeken, amelyeket távolról is el szeretnénk érni, telepíteni kell a logmein megfelelő változatát. Van ugyanis ingyenes és fizetős programváltozat is, persze a fizetős program többet is tud.

A telepítés után a logmein webes felhasználó felületén megjelenik a számítógép, és különböző műveleteket lehet elvégezni ezen a felületen keresztül.

Gyakorlatilag minden olyan helyen, ahol van internetelérés és van böngésző, be lehet jelentkezni a logmein oldalán, és el lehet érni azokat a gépeket, amelyekre telepítettük a programot. Böngészőn keresztül lehetőség van az asztal teljes értékű elérésére, gyakorlatilag mindent ugyanúgy elérhetünk, mintha ott ülnénk a számítógép előtt, ráadásul egy egyszerű böngészőn keresztül.

A logmein előnye még, hogy nincs szükség portátirányításra, az elérni kívánt gép bárhol lehet, tűzfal és router mögött is.

17. 14. lecke: Linux rendszerek távoli elérése

17.1 Részcélkitűzések

A tanuló ismerje a távoli elérés fogalmát, szükségességét. Ismerje a fontosabb alapfogalmakat és rövidítéseket. Ismerje a Linux szerverekhez kapcsolódó távelérési lehetőségeket, legyen képes beállítani a Linux szerveren az SSH szolgáltatást. Legyen képes másik linuxos és windowsos gépről is csatlakozni a Linux szerverhez.

17.2 SSH

Linuxos rendszereket vagy SSH szolgáltatáson keresztül, vagy VNC-n keresztül szokták kezelni távolról. A grafikus felület használatához mindenképpen VNC-re van szükség.

Az SSH a Secure Shell rövidítése, ami biztonságos shell kapcsolatot jelöl. Lényegében a két gép közötti kommunikáció titkosított formában kerül továbbítása, így azt harmadik személy nem tudja értelmezni.

A szerveren az SSH szolgáltatást telepíteni kell. Miután frissítettük a rendszert, adjuk ki a következő parancsot:

```
apt-get install ssh
```

A telepítés után a szolgáltatás azonnal elérhető a 22-es tcp porton. Ha szükséges, módosítható a portcím a **/etc/ssh/sshd_config** fájlban, a Port sorban. Ajánlatos letiltani az ssh-n keresztüli root bejelentkezést. Ezt a „*PermitRootLogin no*” beállítással lehet elérni. Korlátozható az is, hogy milyen felhasználóval lehet bejelentkezni. Ehhez az „*AllowUsers felhnev1, felhnev2*” sort kell elhelyezni. Hatására csak a *felhnev1* és *felhnev2* felhasználók fognak tudni bejelentkezni.

A távoli gépen szükség van egy olyan programra, ami képes SSH kapcsolatok kezelésére.

Csatlakozás Linux alól

Ha távoli gép, ahonnan csatlakozni akarunk szerverhez, Linuxot futtat, akkor ez a program egyszerűen az *ssh*. Paraméteréül meg kell adnunk a

távoli gép IP-címét (pl. *„ssh 192.168.253”*). Ilyenkor automatikusan a 22-es porthoz próbál kapcsolódni. Ha más porthoz szeretnénk kapcsolódni, akkor a *–p* kapcsoló után kell meghatározni azt: *„ssh 192.168.4.253 –p 2200”*.

A sikeres kapcsolódást követően normál bejelentkezéshez hasonlóan meg kell adni egy felhasználónevet és a hozzá tartozó jelszót. Ha sikeres volt a bejelentkezés, akkor kapunk egy shell felületet, ahol ugyanúgy dolgozhatunk, mintha a távoli számítógép konzolja előtt ülnénk.

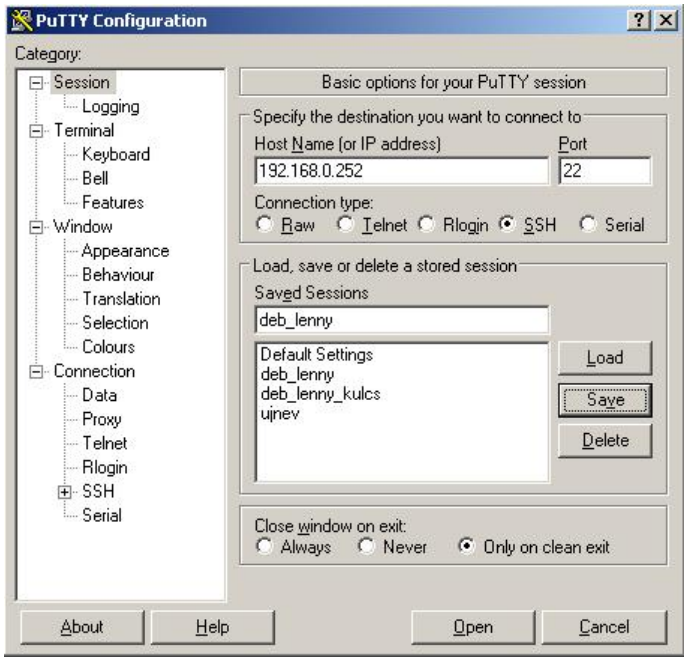
Csatlakozás Windows alól

Ehhez szükségünk lesz a **Putty** csomagra, amit a következő címről tölthetünk le:

http://the.earth.li/~sgtatham/putty/latest/x86/putty.zip

Hozzunk létre a puttynak egy külön könyvtárat, ahova csomagoljuk is ki a zip fájlt. Majd indítsuk el a **putty.exe** programot.

A puttyban több távoli kapcsolat beállításait is külön névvel ellátva lehet eltárolni, amit sessionnek nevez. Meg kell adni az IP-t (*„Host Name”*), a portot, valamint egy session nevet (*„Saved Session”*). Ezen kívül sok-sok minden állítható, de a lényeg az, hogy ha beállítottuk, amire szükségünk van, akkor mindig vissza kell térni a kezdőlapra (a bal oldalon a *Category* részben a *Session*-t kell választani), és menteni kell a *Save* gombbal.



37. ábra. Putty

Ha másra nem is, de a kódlap beállítására érdemes odafigyelni, mivel a Linux alapvetően UTF-8 kódolást használ, míg a magyar Windows jellemzően iso-8859-2 kódlapot. Ezt a *Window* elem *Translation* részben lehet állítani a „*Received data assumed …*” kezdetű listadobozban.

17.3 VNC

A szerveren telepíteni kell a távoli asztal szolgáltatást, a kliensen pedig, ahonnan el szeretnénk érni, egyszerűen el kell indítani a távoli asztal kapcsolatot, majd meg kell adni a szerver IP-címét és portját. A bejelentkezés után egyszerűen kezelhető távolról a rendszer.

18. 15. lecke: III. témazáró feladatsor

1. Egészítse ki a következő mondatot! (1 pont)

A _____ mentés esetében csak azok a fájlok kerülnek mentésre, amelyek az előző mentés óta változtak.

2. Melyik az a beépített szolgáltatás, amelyikkel Windows Server 2008 alatt menteni lehet? Válassza ki a helyes megoldást! (1 pont)

a) ntbackup.exe

b) Windows Server Backup

c) wsbackup.exe

d) Server Backup

e) Backup to

3. Jelölje be azokat az eszközöket, ahova menteni lehet a beépített mentési programmal! Több jó válasz is lehetséges! (2 pont)

a) CD

b) Egy könyvtár

c) Hálózati meghajtó

d) Szalagos egység

e) Külön csak mentésre szolgáló merevlemez

4. Mit jelent a klónozás? Válassza ki a helyes megoldást! (1 pont)

a) Másolatot készítünk egy adott könyvtár fájljairól.

b) A merevlemez tartalmát egy másik merevlemezre másoljuk.

c) Egy CD lemezről másik CD lemezt készítünk.

d) A szövegszerkesztő programban ugyanazt a formátumot állítjuk be egy másik bekezdésre is.

5. **Írja le azt a parancsot, amellyel egyetlen fájlba tömöríthető linux alatt a /var/www könyvtár, és a fájl neve www.tar.gz legyen! (2 pont)**

6. **A dokumentáció melyik része az, ahol a rajzon az aktív eszközök és számítógépek kapcsolatai is szerepelnek IP-címekkel együtt? Válassza ki a helyes megoldást! (1 pont)**

    a) Informatikai szabályzat

    b) Hálózat logikai dokumentációja

    c) Szoftverek dokumentációja

    d) Hálózat fizikai dokumentációja

    e) Hálózati terv

7. **Igaz-e a következő kijelentés? (1 pont)**

    A Windows 2008 Serverek esetén a távoli gépről történő kezelést biztosító programot VPN-nek, Virtual Private Network szolgáltatásnak nevezik.

8. **Melyik az a távoli elérést biztosító programrendszer, amelynek használatához nincs szükség Port Forwardra, ha az elérendő számítógép router mögött van? Válassza ki a helyes megoldást! (1 pont)**

    a) SSH

    b) VNC

    c) Logmein

    d) Távoli asztal kapcsolat

    e) Putty.exe

19. 16. lecke: Összegző felmérés

A feladatok végrehajtásához szükség van egy frissen telepített Windows 2008 Serverre és egy Windows XP-s számítógépre (a gépek lehetnek virtuálisak is!). Mindkettőn telepítve kell lennie a legutolsó Service Packeknek, valamint a szükséges drivereknek!

1. Állítsa be a szerver és kliens gépet úgy, hogy mindkettő a 10.1.xx.00/24 hálózat tagja legyen, a szerver 250-es IP-t kapjon, az XP pedig 10-est! Az alapátjáró címe és a DNS címe is legyen 254! Ellenőrizze is a hálózati kapcsolatot a két gép között, valamint a gépek és az átjáró között! (4 pont)
2. Nevezze át a szervert „Server”-re, az XP-s gépet pedig „Kliens”-re! (2 pont)
3. Telepítse fel a szerverre az Active Directory szolgáltatást! Új tartományt készítsen, aminek a teljes neve legyen „vizsga.local”, a NetBIOS neve pedig „VIZSGA”. A telepítés végén módosítsa a szerver hálózati beállításait úgy, hogy a saját DNS szerverét használja névfeloldásra! Ellenőrizze a DNS működését is! (5 pont)
4. Módosítsa a kliens gép hálózati beállításait úgy, hogy a szerver DNS-ét használja, majd léptesse be a tartományba! (2 pont)
5. Hozzon létre egy „Tanulo” és egy „Tanar” szervezeti egységet, valamint készítsen hozzájuk egy „TanarokGPO” és egy „TanulokGPO” nevű GPO-t! (2 pont)
6. Hozzon létre egy „diak1” és egy „diak2” felhasználót a „Tanulo” szervezeti egységen belül, valamint egy „tanar1” és „tanar2” felhasználót a „Tanar” szervezeti egységen belül! (2 pont)
7. Hozzon létre egy csoportot a tanulók részére „Tanulok” névvel, és egy „Tanarok” csoportot a tanárok részére, majd adja is hozzá a megfelelő csoportokhoz a megfelelő felhasználókat! (2 pont)

8. A tanuló GPO-n keresztül korlátozza le a vezérlőpult szolgáltatásait, valamint állítson be egyedi háttérképet! (2 pont)
9. Készítsen a szerveren a C: gyökerében egy Home nevű könyvtárat, amiben hozzon létre egy Tanulok és egy Tanarok nevű könyvtárat is! (2 pont)
10. Állítsa be a megfelelő helyeken, hogy a Tanulok csoport tagjainak home könyvtárai az előbb létrehozott Tanulok nevű könyvtárba kerüljenek, és S: meghajtóként automatikusan kerüljenek felcsatolásra a bejelentkezéskor! (2 pont)
11. Állítsa be a megfelelő helyeken, hogy a Tanarok csoport tagjainak home könyvtárai az előbb létrehozott Tanarok nevű könyvtárba kerüljenek, és S: meghajtóként automatikusan kerüljenek felcsatolásra a bejelentkezéskor! (2 pont)
12. Készítsen a szerveren egy Megosztasok nevű könyvtárat a C: gyökerében! A Megosztasok könyvtáron belül hozzon létre egy Közös nevű könyvtárat, amit Kozos névvel meg is oszt a hálózaton! Állítsa be a Közös könyvtár elérési jogait úgy, hogy a Tanulok csak olvasni tudjanak a könyvtárból, míg a Tanarok írni is tudjanak bele! (4 pont)
13. Állítson be egyedi Login scriptet a tanárok és a tanulók részére is úgy, hogy mindkettőben K: egységként kerül csatlakoztatásra a Kozos megosztás! A tanárok csoport tagjainak bejelentkezésekor jelenjen meg egy szövegablak is, amiben a következő szöveg legyen: „Üdvözlöm Tanár Úr!” (5 pont)
14. A szerveren biztosítsa, hogy távoli asztal kapcsolattal is lehessen csatlakozni hozzá, majd csatlakozzon is be a kliens rendszerről! 3 pont)
15. Állítson be automatikus biztonsági mentést a szerveren, ami minden nap 00:05-kor lementi a C:\Home, és C:\Megosztas könyvtárak tartalmát! (4 pont)

20. Értékelés, feladatmegoldások

I. témazáró feladatsor

1. b)
2. Organizational Unit, vagy OU vagy szervezeti egység
3. f), g), b), h), d), a), e), c)
4. b), d)
5. Nem igaz
6. c)
7. aktuális felhasználót

Összesen 10 pontot lehet szerezni. A pontozásnál a 2 pontos feladatoknál a részmegoldásért 1 pont jár. A témazáró akkor tekinthető eredményesnek, ha 80%-ot (8 pontot) sikerül elérni.

II. témazáró feladatsor

1. Group Policy Object
2. c)
3. Nem igaz
4. netlogon
5. d)
6. d)
7. El
8. b)
9. Nem igaz
10. d)

Összesen 10 pontot lehet szerezni. A pontozásnál a 2 pontos feladatoknál a részmegoldásért 1 pont jár. A témazáró akkor tekinthető eredményesnek, ha 80%-ot (8 pontot) sikerül elérni.

III. témazáró feladatsor

1. növekményes
2. b)
3. b), c), e)
4. b)
5. tar –cvpzf www.tar.gz /var/www
6. b)
7. Nem igaz
8. c)

Összesen 10 pontot lehet szerezni. A pontozásnál a 2 pontos feladatoknál a részmegoldásért 1 pont jár. A témazáró akkor tekinthető eredményesnek, ha 80%-ot (8 pontot) sikerül elérni.

Összegző felmérés

Összesen 43 pontot lehet szerezni. A pontozásnál a több pontos feladatoknál a részmegoldásért is jár pont. A modulzáró akkor tekinthető eredményesnek, ha 60%-ot (30 pontot) sikerül elérni.

21. Irodalomjegyzék

Kis Balázs, Szalay Márton: *Windows Server 2008 rendszergazdáknak.* 2008, Szak Kiadó Kft., 544 o.

Kis Balázs: *Windows 2000 Server rendszergazdáknak.* 2001, Szak Kiadó Kft., 424 o.