ЛАБОРАТОРНА РОБОТА № 6
РОЗМЕЖУВАННЯ ДОСТУПУ В ДОМЕННІЙ СТРУКТУРІ НА БАЗІ ACTIVE DIRECTORY

Тема: створення та налаштування домену користувацької системи. Розмежування доступу в доменній структурі на базі Active Directory сімейства операційних систем Windows.

Мета: дослідити та налаштувати домен за допомогою елементів служби каталогів ActiveDirectory ОС Windows Server.

ЗАВДАННЯ

1. Створити організаційний підрозділ.
2. Створити два доменні облікові записи користувачів. задати їм час входу в систему. *(понеділок, середа та п`ятниця для user1, вівторок, четвер та субота для user2. Робочий час – з 8:00 до 20:00)*
3. Створити ще два доменні облікові записи. дозволити доступ до різних комп'ютерів домену. *(Створити один список доступу до одного користувача та другий список для іншого.)*
4. Створити ще один доменний обліковий запис. підключити для доменного користувача папку як мережевий диск. *(На диску сервера (не системному) створити папку загального доступу. Надати повний доступ до цієї папки даному користувачу. Встановити квоту, яку використовує цей користувач.)*
5. Створити ще один доменний обліковий запис. Підключити декілька мережевих дисків для доменного користувача. *(Для реалізації написати скрипт. Встановити квоти даному користувачу на використання дискового простору.)*

ТЕОРЕТИЧНИЙ МАТЕРІАЛ

Работа з обліковими записами користувачів в Active Directory

Облікові записи (accounts) користувачів, комп'ютерів і груп - один з головних елементів керування доступом до мережних ресурсів, а виходить, і всієї системи безпеки мережі в цілому.

У середовищі Windows 2003 Active Directory існує 3 головних типа користувацьких облікових записів:

- Локальні облікові записи користувачів. Ці облікові записи існують у локальній базі даних SAM (Security Accounts Manager) на кожній системі, що працює під керуванням Windows 2003. Ці облікові записи створюються з використанням інструмента Local Users and Groups (Локальні користувачі й групи) консолі Computer Management (Керування комп'ютером). Помітимо, що для входу в систему по локальному обліковому запису, цей обліковий запис обов'язково повинен бути присутнім у базі даних SAM на системі, у яку ви намагаєтеся ввійти. Це робить локальні облікові записи непрактичними для більших мереж, внаслідок більших накладних витрат по їхньому адмініструванню.
- Облікові записи користувачів домена. Ці облікові записи зберігаються в Active Directory і можуть використовуватися для входу в систему й доступу до ресурсів по всьому лісу AD. Облікові записи цього типу створюються централізовано за допомогою консолі "Active Directory Users and Computers" ("Active Directory - користувачі й комп'ютери").
- Вбудовані облікові записи. Ці облікові записи створюються самою системою й не можуть бути вилучені. За замовчуванням будь-яка система, ізольована (окремо встановлена) або та що в домені, створює два облікові записи - Administrator (Адміністратор) і Guest (Гість). За замовчуванням обліковий запис Гість відключена.

Зосередимо свою увагу на облікових записах користувачів домена. Ці облікові записи зберігаються на контролерах домена, що зберігають копію бази даних Active Directory.

Додавання нового доменного облікового запису користувача

Розглянемо приклад створення облікового запису користувача домена. Щоб створити обліковий запис користувача клацніть правою кнопкою контейнер, у який ви прагнете помістити обліковий запис користувача, виберіть у контекстному меню New (Створити), а потім - User (Користувач). Відкриється вікно майстра New Object - User (Новий об'єкт - Користувач) (Рис.2.18)

1. Уведіть ім'я, ініціали і прізвище користувача у відповідних полях. Ці дані будуть потрібні для створення відображуваного імені користувача.
2. Відредагуйте повне ім'я. Воно повинне бути унікальним у домені й мати довжину не більш 64 символів.

3. Уведіть ім'я для входу. За допомогою списку, що розкривається, виберіть домен, з яким буде зв'язаний обліковий запис.

4. При необхідності змініть ім'я користувача для входу в системи з ОС Windows NT 4.0 або більш ранніми версіями. За замовчуванням у якості імені для входу в системи з попередніми версіями Windows використовуються перші 20 символів повного імені користувача. Це ім'я також повинне бути унікальним у домені.

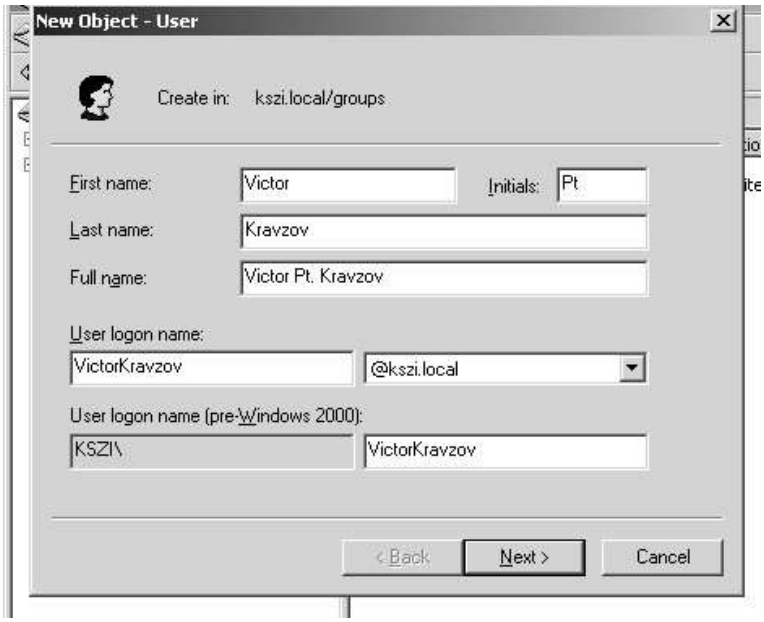


Рис.2.18

5. Клацніть Next (Далі). Укажіть пароль для користувача. Його параметри повинні відповідати вашій політиці паролів;

Confirm Password (Підтвердження) - поле, використовуване для підтвердження правильності введеного пароля;

User must change password at next logon (Вимагати зміну пароля при наступному вході в систему) - якщо цей прапорець установлений, користувачеві потрібно змінити пароль при наступному вході в систему;

User cannot change password (Заборонити зміну пароля користувачем) - якщо цей прапорець установлений, користувач не може змінити пароль;

Password never expires (Термін дії пароля не обмежений) - якщо цей прапорець установлений, час дії пароля для цього облікового запису не обмежений (цей параметр перекриває доменну політику облікових записів);

Account is disabled (Відключити обліковий запис) - якщо цей прапорець установлений, обліковий запис не діє (параметр зручний для тимчасової заборони використання ким-небудь цього облікового запису).

Облікові записи дозволяють зберігати контактну інформацію користувачів, а так само інформацію про участь у різних доменних групах, шлях до профілю,

сценарій входу, шлях домашньої папки, список комп'ютерів, з яких користувачеві дозволений вхід у домен і т.д.

Сценарії входу визначають команди, виконувані при кожному вході в систему. Вони дозволяють настроїти системний час, мережні принтери, шляхи до мережних дисків і т.д. Сценарії застосовуються для разового запуску команд, при цьому параметри середовища, що задаються сценаріями, не зберігаються для наступного використання. Сценаріями входу можуть бути файли сервера сценаріїв Windows з розширеннями .VBS, .JS і інші, пакетні файли з розширенням BAT, командні файли з розширенням .CMD, програми з розширенням .EXE.

Можна призначити кожному обліковому запису свою домашню папку для зберігання й відновлення файлів користувача. Більшість додатків за замовчуванням відкривають домашню папку для операцій відкриття й збереження файлів, що спрощує користувачам пошук своїх даних. У командному рядку домашня папка є початковим поточним каталогом. Домашня папка може розташовуватися як на локальному жорсткому диску користувача, так і на загальнодоступному мережному диску.

До доменних облікових записів комп'ютерів і користувачів можуть застосовуватися групові політики. Групова політика спрощує адміністрування, надаючи адміністраторам централізований контроль над привілеями, дозволами й можливостями користувачів і комп'ютерів. Групова політика дозволяє:

- створювати централізовано керовані спеціальні папки, наприклад My Documents (Мої документи);
- управляти доступом до компонентів Windows, системних і мережних ресурсів, інструментів панелі керування, робочого столу й меню Start (Пуск);
- настроїти сценарії користувачів і комп'ютерів на виконання завдання в заданий час;
- настроювати політики паролів і блокування облікових записів, аудита, присвоєння користувацьких прав і безпеки.

Політики доменних паролів

- Ви можете для своїх користувачів використовувати додаткові правила у формі політик паролів Windows Server 2003.
- Вам слід ретельно перевірити й обміркувати наявні політики паролів в Windows Server 2003, оскільки ваші користувачі будуть постійно підкорятися цим правилам.
- Політики паролів доступні тільки для домена, а не для OU.
- Конфігуруйте політики паролів для домена в Domain Security Policy -Security Settings\Account Policies\Password Policy. (Рис.2.19)

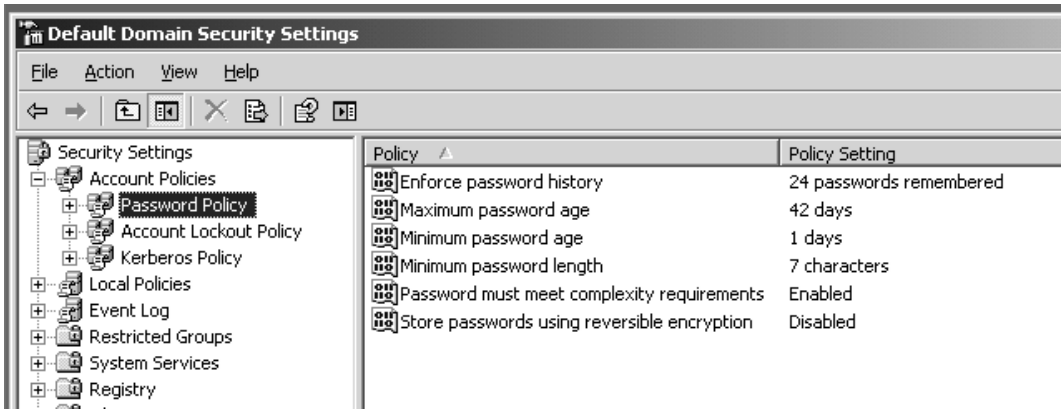


Рис.2.19

Всі паролі за завмовчуванням повинні відповідать наступним вимогам.

- Він не може містити частково (або повністю) ім'я з облікового запису користувача.
- Він повинен містити не менше шести символів.
- Він повинен містити символи, принаймні, з трьох категорій серед наступних чотирьох категорій:
  - англійські прописні букви (від A до Z);
  - англійські малі літери (від a до z);
  - цифри від 0 до 9;
  - неалфавітні символи (наприклад, !, $, #, %).

Профілі користувачів

Профіль користувача - це група настроювань, які визначають робоче оточення користувача. Windows Server 2003 використовує профіль для створення робочого оточення користувача при вході. Типові настроювання профілю користувача включають конфігурацію робочого стола, вміст меню, настроювання панелі керування (Control Panel), з'єднання з мережним принтером і т.д.

Є декілька типів профілів, і ви можете використовувати будь-яку комбінацію профілів на всьому підприємстві, що відповідає потребам ваших користувачів. У цьому розділі дається огляд наступних типів профілів:

- локальні (Local);
- переміщаючі або "блукаючі" (Roaming);
- обов’язкові (Mandatory).

Локальні профілі

Windows Server 2003 створює локальний профіль при першому вході кожного користувача на комп'ютер. Кожний користувацький профіль зберігається в папці \Documents and Settings\User(Рис.2.20) де User - це ім'я входу цього користувача

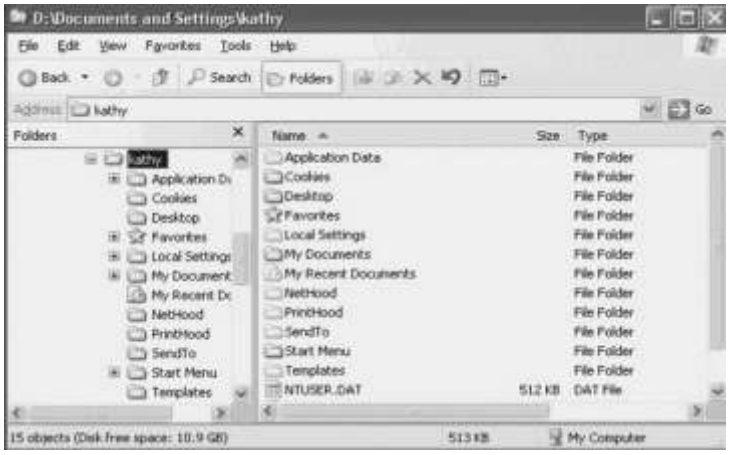


Рис.2.20

Переміщені профілі

Переміщуваний (блукаючий) профіль зберігається на сервері. Цей профіль завантажується на локальний комп'ютер із сервера, коли користувач входить у мережу, незалежно від комп'ютера, з якого виконує вхід цей користувач. Будь-які зміни, які вносить цей користувач у настроювання конфігурації, зберігаються в даному профілі на сервері.

Обов’язковий профіль

Обов'язковий профіль - це переміщуваний профіль, який не можна змінювати. Хоча користувачі можуть змінювати деякі настроювання під час сеансу, ці зміни не зберігаються в профілі на сервері й недоступні при наступному вході цього користувача в мережу. Однак адміністратори можуть вносити зміни в обов'язкові профілі користувачів. Оскільки обов'язкові профілі не можна змінювати відповідно до особистих настроювань користувача, їх можна застосовувати до груп користувачів.

Домашні папки

Домашня папка - це директорія, яку ви призначаєте як контейнер для документів користувача. У випадку домена це звичайно папка на сервері, яка сприяє резервному копіюванню даних користувача. Резервне копіювання серверів відбувається регулярно, у той час як резервне копіювання локальних робочих станцій не відбувається майже ніколи. Ви можете також створювати домашні папки для користувачів на їхніх локальних робочих станціях, але звичайно цю роль виконує папка My Documents. Домашні папки на сервері створюються для окремих користувачів усередині заздалегідь створеного розшареного ресурсу.

Перенаправлення документів у домашню папку

Якщо в користувача без переміщуваного профілю є домашня папка на сервері, то у вікні My Computer з'являється відображувана буква накопичувача, і запрошення в командному рядку теж містить цю букву накопичувача. Однак програми продовжують зберігати документи в папці My Documents, що є домашньою папкою. Вам потрібно перенаправляти папку My Documents у домашню папку, і це можна робити різноманітними способами.

Інструкції дуже прості: потрібно клацнути правою кнопкою миші на папку My Documents, вибрати пункт Properties і потім змінити місце розташування в поле Target (Місце призначення) на домашню папку (відповідна буква накопичувача). Windows запитає вас, чи потрібно перемістити існуючі документи в це нове місце. Клацніть на кнопку Yes.

Крім завдань керування користувацькими обліковими записами й групами існує маса інших завдань керування доменом. Для цього служать інші вкладки й додатки.

Вкладка Active Directory Domains and Trusts служить для роботи з доменами, деревами доменів і лісами доменів.

Вкладка Active Directory Sites and Services (Рис.2.21) дозволяє управляти сайтами й підмережами, а так само міжсайтовой реплікацією.

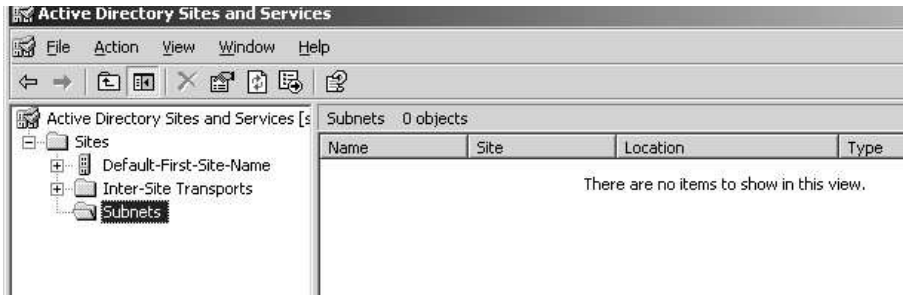


Рис.2.21

Для керування об'єктами AD існують засоби командного рядка, які дозволяють здійснювати широкий спектр адміністративних завдань:

Dsadd - додає в Active Directory комп'ютери, контакти, групи, організаційні підрозділи й користувачів. Для одержання довідкової інформації введіть dsadd /?, наприклад dsadd computer/?

Dsmod - змінює властивості комп'ютерів, контактів, груп, організаційних підрозділів, користувачів і серверів, зареєстрованих в Active Directory. Для одержання довідкової інформації введіть dsmod /?, наприклад dsmod server /?

Dsmove - переміщає одиночний об'єкт у нове розташування в межах домена або перейменовує об'єкт без переміщення.

Dsget - відображає властивості комп'ютерів, контактів, груп, організаційних підрозділів, користувачів, сайтів, підмереж і серверів, зареєстрованих в Active

Directory. Для одержання довідкової інформації введіть dsget /?, наприклад dsget subnet /?

Dsquery - здійснює пошук комп'ютерів, контактів, груп, організаційних підрозділів, користувачів, сайтів, підмереж і серверів в Active Directory за заданими критеріями.

Dsrm - видаляє об'єкт із Active Directory.

Ntdsutil - дозволяє переглядати інформацію про сайт, домен або сервер, управляти хозяїнами операцій (operations masters) і обслуговувати базу даних Active Directory.

Так само існують засоби підтримки Active Directory:

Ldp - Здійснює в Active Directory Administration операції по протоколу LDAP.

Replmon - Управляє реплікацією й відображає її результати в графічному інтерфейсі.

Dsacls - Управляє списками ACL (списками керування доступом) для об'єктів Active Directory.

Dfsutil - Управляє розподіленою файловою системою (Distributed File System, DFS) і відображає відомості про її роботу.

Dnscmd - Управляє властивостями серверів, зон і записів ресурсів DNS.

Movetree - Переміщає об'єкти з одного домена в інший.

Repadmin - Управляє реплікацією й відображає її результати у вікні командного рядка.

Sdcbeck - Аналізує поширення, реплікацію й спадкування списків керування доступом.

Sidwalker - Задає списки керування доступом для об'єктів, у минулому, що належали переміщеним, вилученим або загубленим обліковим записам.

Netdom - Дозволяє управляти доменами й довірчими відносинами з командного рядка.

Отже, об'єднання груп комп'ютерів у домени на базі Active Directory дозволяє суттєво знизити витрати адміністративних завдань за рахунок централізації керування доменними обліковими записами комп'ютерів і користувачів, а так само дозволяє гнучко управляти правами користувачів, безпекою й масою інших параметрів.

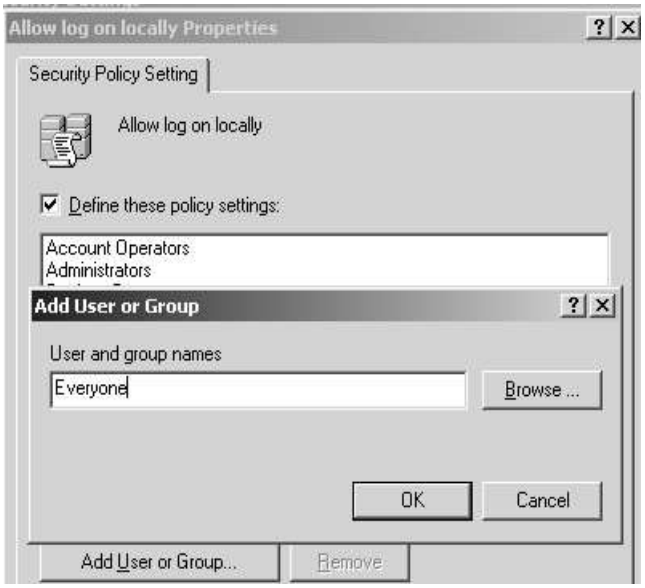
ПРАКТИЧНЕ ЗАВДАННЯ

1. Установка Політик паролів для домену.

- Відкриваємо вікно Start-administrative Tools--- Domain Security Policy
- З Security Settings вибираємо Account Policies - Password Policy
- Установлюємо Minimum Password Length в 0 символів
- Установлюємо Password Must Meet Complexity Requirements в Disabled
- Закриваємо вікно Domain Security Policy
- Відкриваємо вікно Start-administrative Tools--- Domain Controller Security

Policy

- З Security Settings вибираємо Local Policies - User Right Assignment ▪ Для Allow Log On Locally відкриваємо Properties. Натискаємо Add User Or Group. І задаємо ім'я Everyone..



- Закриваємо вікно Domain Controller Security Policy
- Для застосування зроблених настроювань відкриваємо cmd (командний рядок) і застосовуємо команду Gpupdate.

2. Створити сім нових облікових записів в Active Directory об'єкта Users з наступними параметрами:

4.1. First Name: Ginnie; Initial: B.; Last Name: Donald;
User Logon Name: Ginnie; Password: girLYc@t;
відмітити Password Never Expires; зняти відмітку User
Must Change Password at Next Logon.

4.2. First Name: Robert; Last Name: Jones; User Logon Name: Robert; Password: b4tm4n; відмітити Password Never Expires; зняти відмітку User Must Change Password at Next Logon.

4.3. First Name: Terry; Last Name: Belle; User Logon Name: Terry; Password: b4tg1rl; відмітити Password Never Expires; зняти відмітку User Must Change Password at Next Logon.

4.4. First Name: Ron; Last Name: Klein; User Logon Name: Ron; Password: sup3rm4n; відмітити Password Never Expires; зняти відмітку User Must Change Password at Next Logon.

4.5. First Name: Wendy; Last Name: Smith; User Logon Name: Wendy; Password: sup3rg1rl; відмітити Password Never Expires; зняти відмітку User Must Change Password at Next Logon.

4.6. First Name: Emily; Last Name: Buras; User Logon Name: Emily; Password: p34ch; відмітити Password Never Expires;
зняти відмітку User Must Change Password at Next Logon.

4.7. First Name: Michael; Last Name: Phillips; User Logon Name: Michael; Password: 4ppl3; відмітити Password Never Expires; зняти відмітку User Must Change Password at Next Logon.

З Windows XP Professional намагаємося зайти під створеними обліковими записами Ginnie, Robert, Terry, Ron.

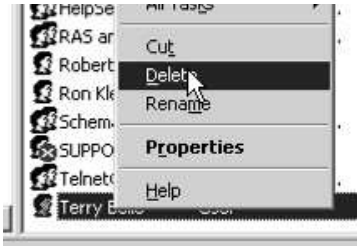
3. Відключення облікового запису користувача

- У вікні Active Directory Users and Computers серед списку користувачів нашого домена вибираємо для користувача Robert властивість Disable Account
-

З Windows XP Professional намагаємося зайти під користувачем Robert. Спроба повинна провалитися, тому що користувач Robert не активний.

4. Видалення облікового запису користувача

- У вікні Active Directory Users and Computers серед списку користувачів нашого домена вибираємо для користувача Terry властивість Delete



З Windows XP Professional намагаємося зайти під користувачем Terry.

5. Використання локального профілю користувача:

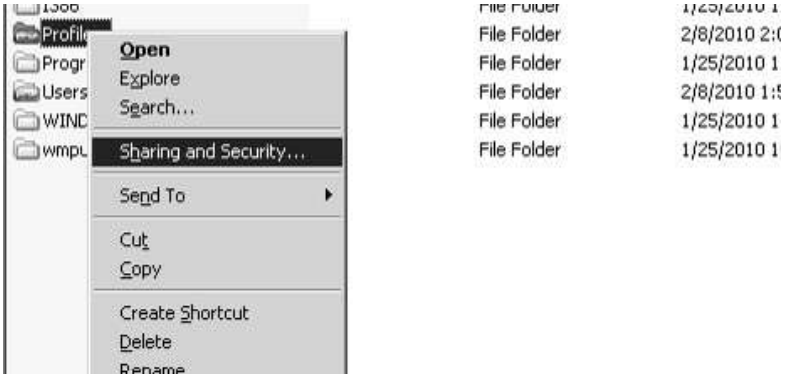
- З Windows XP Professional заходимо в домен під Administrator;
- Заходимо в папку C:\Documents and Settings. У папці перебувають підпапки для користувачів які залогінувалися у систему. Переконаєтеся що для користувачів Emily і Michael немає відповідних папок-профілів;
- Залогінуємося в домен під користувачем Emily (Password: p34ch) і створюємо профіль. Змінюємо настроювання Робочого Стола (міняємо фон й додаємо ярлик на calc.exe);
- Залогінуємося в домен під користувачем Michael (Password: 4ppl3);
- Залогінуємося в домен під Administrator. Заходимо в папку C:\Documents and Settings. Переконуємося що профілі для користувачів Emily і Michael з'явилися.

6. Використання переміщуваного профілю користувача:

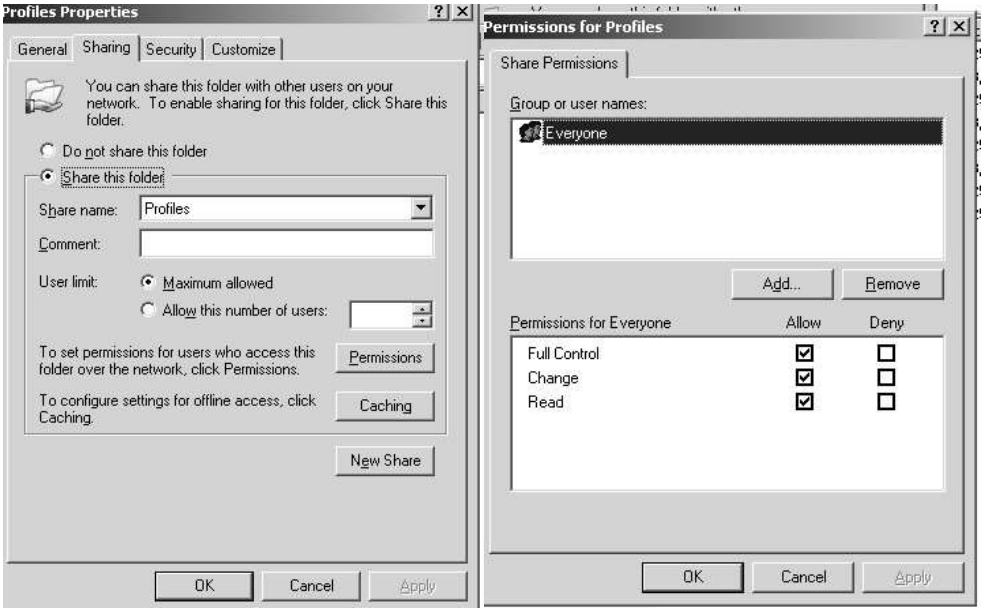
▪ У вікні Active Directory Users and Computers для об'єкта Users створюємо нового користувача

First Name: Test; Last Name: Accounts; User Logon Name: Test; Password:girlyc@t; відзначити Password Never Expires; зняти оцінку User Must Change Password at Next Logon.

▪ На диску (C:) створюємо папку Profiles. І заходимо у вікно Sharing and Security…



▪ Вибираємо вкладку Sharing і відзначаємо Share this Folder. Натискаємо кнопку Permissions і у вікні, що відкрилося, для групи Everyone відзначаємо Allow Full Control.



▪ У вікні Profiles Properties вибираємо вкладку Security і відзначаємо Allow Full Control для групи Users .

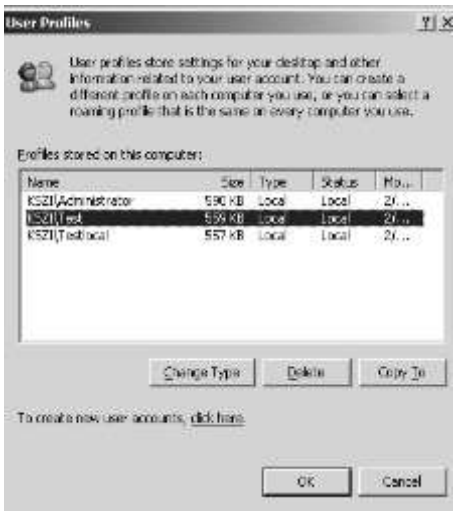
▪ Залогінюємось на сервер у домен під користувачем Test (Password: girlyc@t).

▪ На Робочому Столі створюємо два ярлики: Calc і Explorer.

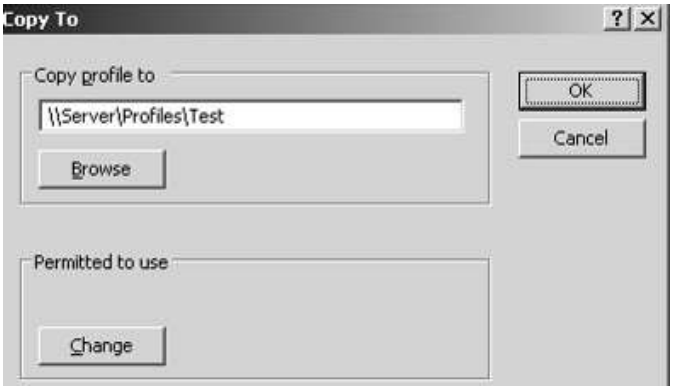
▪ Залогінюємось в домен під Administrator.

▪ Заходимо Start->Control Panel-> System. Переходимо у вкладку Advanced і вибираємо User Profiles Settings.

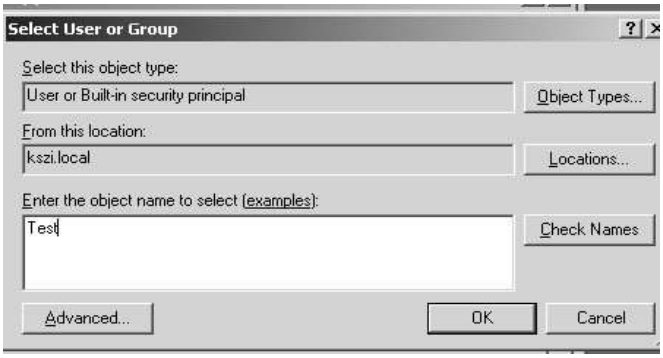
▪ Вибираємо користувача Test і натискаємо Copy To



▪ Визначаємо мережний шлях до переміщуваного профілю користувача \\yourservername\Profiles\Test.

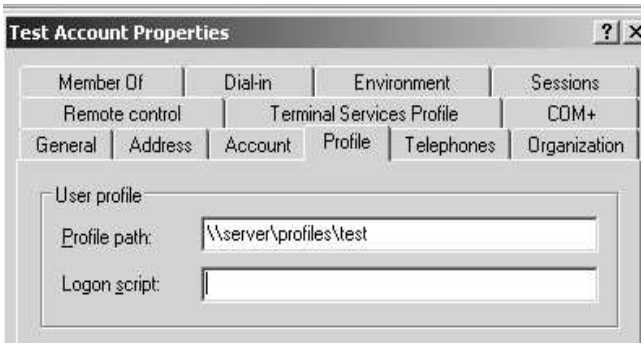


Нажимаємо кнопку Change в області Permitted to use. ▪ Задаємо ім'я користувача Test. І закриваємо всі вікна нажимаючи Ok.



▪ У вікні Active Directory Users and Computers серед списку користувачів нашого домена вибираємо для користувача Test властивість Properties.

▪ Переходимо у вкладку Profile і для поля Profile Path задаємо шлях \\yourservername\Profiles\Test.

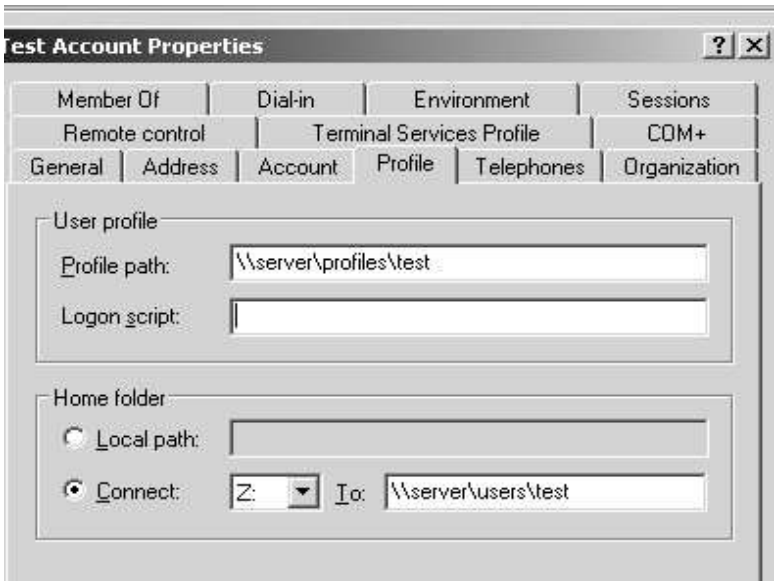


▪ З Windows XP Professional заходимо під користувачем Test. Ми повинні побачити ярлики додані на Робочий Стіл під час створення переміщуваного профілю.

7. Використання Додавання домашніх папок до профілів

▪ Створіть папку з іменем Users і з іменем розшареного ресурсу Users на диску (Z:), задайте для групи Everyone повноваження Full Control.

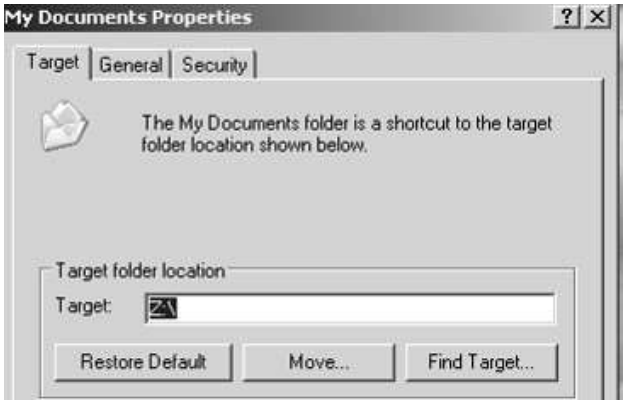
▪ Щоб створити домашню папку для користувача, відкрийте діалогове вікно Properties для цього користувача в оснащенні Active Directory Users and Computers. Перейдіть у вкладку Profiles, виберіть варіант Connect (Приєднати), що фактично є автоматичним відображенням букви накопичувача, укажіть букву накопичувача й потім уведіть Unc-шлях.



▪ Після натискання на Ok остання частина цього шляху (ім'я_користувача) негайно створюється. Цей процес відрізняється від створення даної частини шляху для переміщуваних профілів, яка не створюється на сервері, поки даний користувач не виконає вхід у домен.

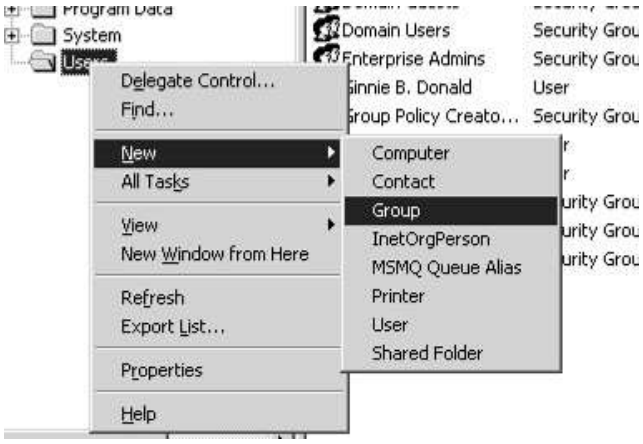
▪ З Windows XP Professional заходимо під користувачем Test. Заходимо в Мій Комп'ютер і бачимо новий мережний диск Test на сервері.

▪ Відкриваємо Properties для папки My Documents, у поле Target (Місце призначення) задаємо домашню папку (відповідна буква накопичувача). Windows запитає вас, чи потрібно перемістити існуючі документи в це нове місце. Клацніть на кнопку Yes.



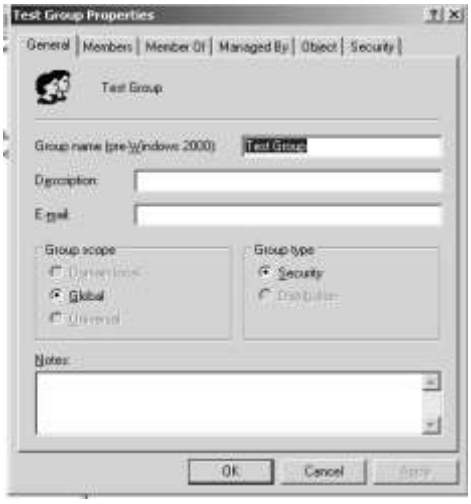
8. Створення групи в Active Directory

- у вікні Active Directory Users and Computers для об’єкта Users створюємо нову группу

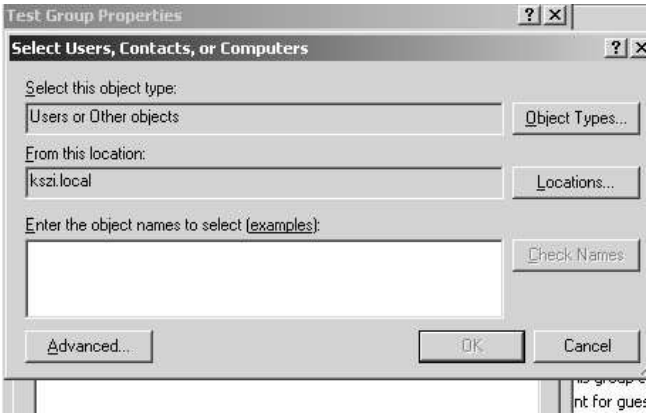


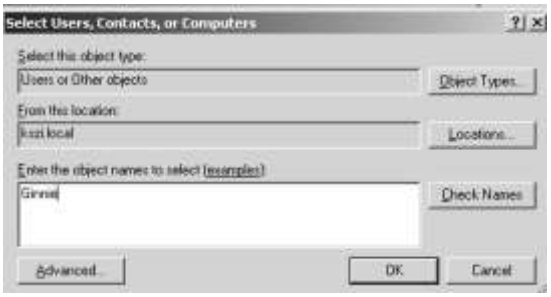
- у вікні New Object-Group прописуємо наступні параметри:

- відкриваємо вікно Properties для групи Test Group



- Переходимо до вкладки Members і натискаємо Add. Вводимо імя Ginnie і натискаємо Ok. Ще додаємо в групу користувачів Emily і Wendy.





Перевірте приналежність до груп у користувачів Wendy і Ron.


Ron Klein Properties
Account
Profile
Telephones
Organization
Member Of
Dial-in
Member of:
Name
Active Directory Folder
Domain Users
kszi.local/Users
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.