ЛАБОРАТОРНА РОБОТА № 5

СТВОРЕННЯ ТА НАЛАШТУВАННЯ ДОМЕНУ НА БАЗІ СЕРВЕРНОЇ ПЛАТФОРМИ СІМЕЙСТВА ОПЕРАЦІЙНИХ СИСТЕМ WINDOWS.

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. Завантажити клієнтську та серверну ОС на віртуальних машинах.
2. На серверній платформі встановити домен. При налаштуванні встановити DNS-сервер. (*Назва домену повинна включати номер студента по списку).*
3. Під’єднати клієнта до створеного домену.
4. Перевірити функціонування домену на гостьовому ПК. (*Створити доменного користувача та перевірити можливість клієнта працювати з даним обліковим записом*).

ТЕОРЕТИЧНИЙ МАТЕРІАЛ

Частина 1
Засоби Manage Your Server

Після установки Windows Server 2003 сторінка Manage Your Server (Керування вашим сервером) автоматично з'являється при кожному завантаженні вашого комп'ютера (Рис.2.1). Це вікно представляє безліч утиліт для конфігурування ролей серверів і керування службами, які ви надаєте користувачам за допомогою цих ролей.

Примітка. Ви можете також відкрити цю сторінку, вибравши Manage Your Server у меню Start.

Рис.2.1

Ви можете використовувати можливості майстрів, які викликаються з вікна Manage Your Server, щоб конфігурувати сервер Windows Server 2003 для певної ролі або декількох ролей (для кожної ролі є окремий майстер). Відповідний майстер проводить вас через процес установки компонентів, що вимагаються для служб, які ви хочете надавати своїм користувачам за допомогою цього сервера.

Щоб запустити майстер, натисніть на посилання Add Or Remove Role (Додавання або видалення ролі). На першій сторінці майстра з'являється контрольний список попередніх завдань, більшість із яких ви імовірно, виконали автоматично під час установки операційної системи. (Рис.2.2)

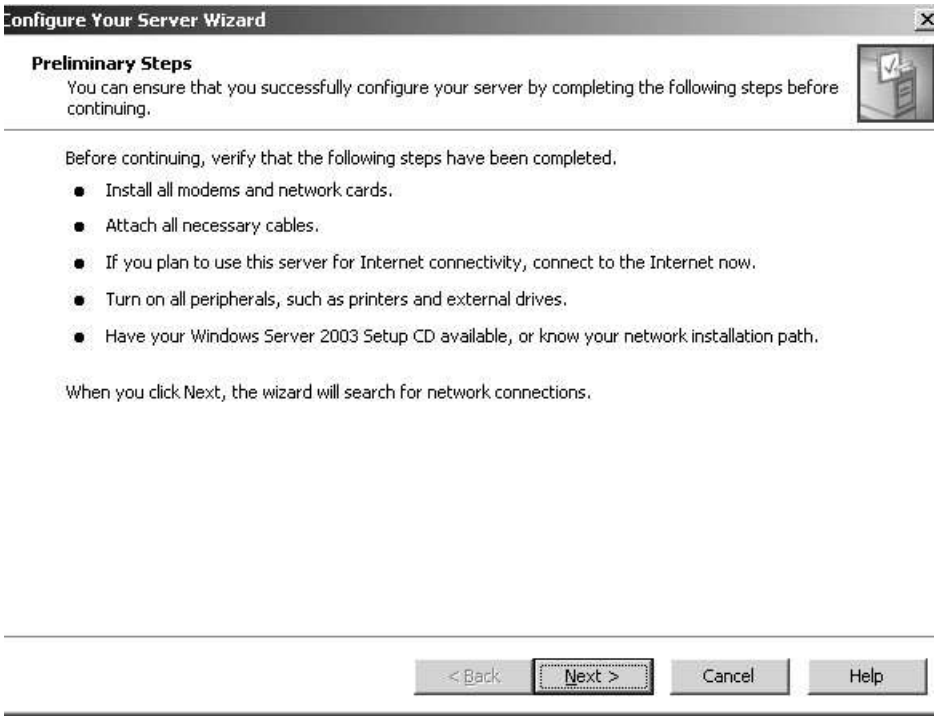


Рис.2.2

При натисканні на кнопку Next майстер перевіряє мережевий адаптер (NIC), щоб переконатися, що даний комп'ютер може взаємодіяти з мережею, і потім виводить список ролей, які ви можете призначити серверу. (Рис.2.3)

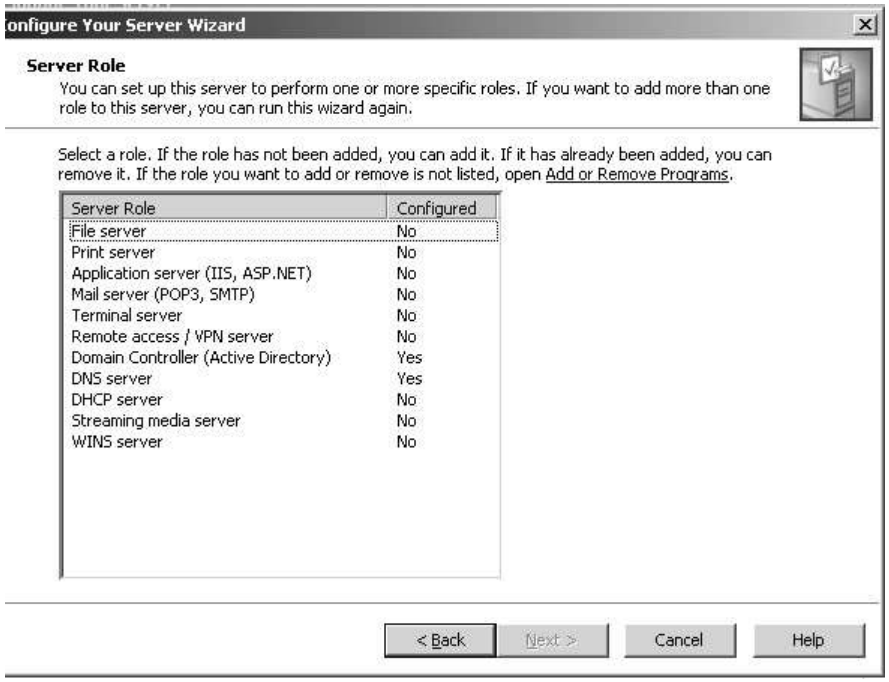


Рис.2.3

Далі приводиться базова інформація по кожній ролі сервера.

File Server (Файловий сервер)

Більшість адміністраторів створюють файлові сервери для зберігання файлів даних користувача, оскільки цей підхід дає багато переваг як користувачам, так і адміністраторам. Найважливішою перевагою є те, що резервне копіювання файлового сервера є також резервним копіюванням усіх даних користувача.

Використовуйте для файлових серверів комп'ютери з жорсткими дисками великої ємності. Для цього має сенс використовувати кілька дисків. Оскільки введення-виведення інформації є найбільш істотним фактором для файлових серверів, намагайтеся придбати якомога більш швидкісні жорсткі диски.

При настроюванні файлових серверів ви повинні простежити, щоб параметри конфігурації користувацьких додатків вказували на цей сервер як місце за замовчуванням для файлів даних.

В залежності від додатка це можна зробити шляхом завдання відповідних параметрів під час розгортання або за допомогою групових політик. (Для деяких додатків вам може знадобитися відображення диска в місця роздільного доступу для користувачів.)

У випадку файлового сервера майстер Configure Your Server пропонує наступні опції конфігурування.

- Дискові квоти (в припущенні, що даний комп’ютер форматується в системі NTFS);
- Служби індексування.

Цей майстер також запускає майстер Share A Folder Wizard, який дозволяє вам надавати для роздільного доступу існуючі папки або створювати нові роздільні папки.

Print Server (Сервер друку)

Якщо Ви налаштовуюте сервер як сервер друку, то відповідний майстер проводить вас через процес надання драйверів принтерів клієнтським комп'ютерам. Ви можете навіть завантажувати драйвери для старих версій Windows (до Windows 2000), щоб користувачам цих версій було простіше виконувати установку принтерів. У вас повинен бути доступ до драйверів принтерів, і в багатьох випадках ви можете витягати ці драйвери з CD відповідної операційної системи. Або ви можете

копіювати драйвери колишніх версій Windows на сервер або гнучкий диск до запуску цього майстра.

Якщо ви встановлюєте драйвери для Windows Server 2003, Windows 2000 або Windows XP, то при натисканні на кнопку Next відбувається запуск майстра додавання принтерів Add Printer Wizard. Якщо ви також встановлюєте драйвери для клієнтів старих версій, то на додаток до майстра Add Printer Wizard запускається майстер Add Printer Drivers Wizard (Майстер додавання драйверів принтерів).

Application Server (Сервер додатків)

Роль "сервер додатків" фактично означає "сервер веб-додатків". Якщо вам потрібно надати мережним користувачам доступ тільки до таких додатків, як Word або Excel, то ви можете встановити Terminal Server. Більшість адміністраторів, які створюють сервери додатків, прагнуть надавати своїм користувачам доступ до цього сервера через Інтернет або прагнуть, щоб користувачі могли мати доступ до веб-технологій (наприклад, до засобів ftp- пересилання або до Html- документів). Якщо ви використовуєте майстер Configure Your Server Wizard для створення сервера додатків, то відбувається автоматична установка наступних компонентів.

- Internet Information Services (IIS). Забезпечує інфраструктуру для вебдодатків і веб-служб.
- Консоль Application Server. Надає право адміністрування для керування веб-додатками.
- COM+. Розширені моделі COM (Component Object Model), які добавляють право розробника до вбудованих інгерованих фунцій COM.
- Distributed Transaction Coordinator (DTC). Координує транзакції COM+.

Крім того, ви можете додатково вибрати наступні засоби.

- Install FrontPage Server Extensions. Дозволяє користувачам дистанційно адмініструвати и публікувати веб-сайт.
- Enable ASP.NET. Платформа веб-додатків для розгортання веб-додатків класу підприємства.

Mail Server (Поштовий сервер)

Поштовий сервер виконує збір електронної пошти з поштового сервера ISP (провайдера послуг Інтернет) і поширює цю пошту користувачам. Це спосіб централізації поштових послуг замість обігу кожного користувача до ISP. Крім того, у випадку конфігурування сервер Windows Server 2003 для цієї ролі він діє як сервер SMTP.

Перш ніж конфігурувати поштовий сервер, ви повинні звернутися до свого ISP, щоб одержати статистичний IP-адрес для даного комп'ютера, і повинні також переконатися, що у вашого ISP є запис Mail eXchanger (Mx-запис), яка відповідає імені поштового сервера для вашого доменного імені електронної пошти.

Майстер проводить вас через кроки конфігурування (включаючи настроювання аутентифікації), і після закінчення ви можете використовувати оснащення POP3 Service для керування вашим поштовим сервером.

Terminal Server (Термінальний сервер) Термінальний сервер надає користувачам доступ до Windows-додатків.

Використовуючи термінальний сервер, ви встановлюєте одну копію додатка й надаєте користувачам доступ до цього додатка на сервері. Користувачі можуть зберігати файли, підтримувати свої власні настроювання й працювати із цим ПО, начебто воно встановлене на їхньому власному комп'ютері.

Remote Access/VPN Server (Сервер дистанційного доступу/віртуальних приватних мереж)

Ця роль сервера використовується для того, щоб віддаленні користувачі одержували доступ до локальної мережі, до якої приєднаний даний сервер. Користувачі можуть використовувати, комутовані (dial-up) з'єднання або приєднуватися зі своїх браузерів. Діючи як точка доступу (шлюз), сервер дистанційного доступу/VPN забезпечує також трансляцію мережних адрес (NAT - Network Address Translation). ЗА допомогою VPN і NAT ваші користувачі- клієнти можуть визначати Ip-адреси комп'ютерів у вашій приватній мережі, а інші Інтернет-користувачі не можуть.

Хоча традиційні комутовані з'єднання продовжують використовуватися (їх часто застосовують співробітники, що приєднуються із будинку), VPN-з'єднання набувають усе більшого поширення. Використання широкосмугових з'єднань зробило VPN корисним засобом доступу до мережних ресурсів для мобільних користувачів і користувачів віддалених підрозділів.

Якщо ви прагнете використовувати свій комп'ютер Windows Server 2003 для цієї ролі, то він повинен мати кілька мережних адаптерів (multihomed), щоб з'єднання локальної мережі й широкосмугове з'єднання існували окремо (і незалежно).

Майстер проводить вас через усі кроки, пропонуючи опції конфігурування, які залежать від того, як ваші віддалені користувачі приєднані до мережі. Звичайно вам потрібно прийняти наступні рішення по конфігурації:

- Призначення мережних адаптерів. Укажіть майстрові, який мережний адаптер (NIC) виділений для широкосмугового з'єднання і який адаптер приєднаний до локальної мережі.
- Призначення IP-адреси вхідним клієнтам. Якщо ваша локальна мережа має сервер DHCP, то сервер дистанційного доступу VPN може одночасно орендувати десять адрес і призначати ці адреси віддаленим клієнтам. Якщо у вас немає сервера DHCP, то ви можете зконфігурувати сервер дистанційного доступу VPN для

генерації й призначення IP-адреси віддаленим клієнтам. Ви повинні задати діапазон IP-адресів, які використовуєте для цієї мети.

▪ Конфігурування служб RAS/RRAS, якщо ви дозволяєте, комутовані (dialup) з'єднання. Відзначимо, що служба RAS вбудована в Windows Server 2003, і її не треба встановлювати як компонент Windows.

Domain Controller (Контроллер домена)

- Контролер домена (DC) містить Active Directory і управляє входами в систему (logon). Ви можете використовувати цей майстер для установки першого контролера домена або якщо у вас уже встановлений який-небудь контролер домена, цей майстер проводить вас через кроки установки інших контролерів доменов наступних видів:
  - інший контролер домена для існуючого домена;
  - контролер домена для нового лісу;
  - контролер домена для нового дочірнього домена;
  - контролер домена для нового дерева доменів.

DNS Server (Сервер DNS)

Сервер DNS забезпечує роботу служби дозволу імен, яка потрібно для Active Directory.

DHCP Server (Сервер DHCP) Сервер DHCP надає IP-адреси для комп'ютерів вашої мережі.

Streaming Media Server (Сервер потокової медіа/інформації)

Якщо вам потрібно доставляти вміст Windows Media (потокове аудио й відео), то ви можете конфігурувати комп'ютер Windows Server 2003 як сервер потокової медіа-інформації. Цей майстер установлює службу Windows Media Services, яка дозволяє вам доставляти цифрову медіа-інформацію (у реальному масштабі часу) клієнтам локальної мережі, клієнтам комутуючого доступу і клієнтам VPN.

WINS Server (Сервер WINS)

Навіть після розгортання домена Windows Server 2003 вам очевидно, ще буде потрібно WINS протягом деякого часу. Це стосується не тільки до клієнтів старих версій Windows, яким потрібен дозвіл імен Netbios, але також пов'язане з тим, що у вас, очевидно, використовуються додатки у яких здійснюються виклики WINS. (Відразу спадає на думку Microsoft Office.)

Установка сервера WINS і підтримка служб WINS не представляє складностей, оскільки Windows Server 2003 виконує такі завдання ефективно й автоматично.

Видалення ролей сервера

У міру настроювання, коректування й оптимізації вашого підприємства звичайно доводиться переглядати ролі серверів у наданні мережних послуг користувачам. У вас можуть бути сервери, що виконують кілька ролей і в міру придбання нового обладнання ви можете передавати ролі новим комп'ютерам. Або може виявитися, що деякі сервери з декількома ролями відчувають занадто більше навантаження, обслуговуючи користувачів, що приводить до зниження продуктивності.

Manage Your Server дозволяє видаляти ролі так само легко й швидко, як і додавати їх. Для цього клацніть на посилання Add Or Remove Role, щоб запустити майстер Configure Your Server Wizard(Рис.2.4), який ви вже використовували для створення ролей. Клацніть на кнопку Next у першому вікні (попередня інформація) і після того, як Windows перевірить ваші мережні з'єднання, ви побачите список ролей серверів. Ролі, які ви призначили даному комп'ютеру, будуть представлені значенням Yes у колонку Configured. Якщо ви задали роль вручну, установивши певний компонент Windows замість використання майстра Configure Your Server Wizard, то ця роль теж буде представлена значенням Yes.

Виділіть роль, яку прагнете вилучити, і клацніть на кнопку Next, щоб викликати вікно майстра Role Removal Confirmation (Підтвердження видалення ролі).

Рис.2.4

Встановіть прапорець, що підтверджує видалення, і потім клацніть на кнопку Next. Майстер видалить відповідні файли й при необхідності внесе зміни в конфігурацію.

Клацніть на кнопку Finish в останньому вікні майстра, щоб завершити цей процес.

Задання ролей серверів вручну

Якщо ви віддаєте перевагу зробити це вручну й взагалі уникаєте працювати з майстрами, то можете налаштувати будь-який сервер Windows Server 2003 для будь-якої ролі. Для більшості доступних ролей серверів потрібно встановлення одного або декількох компонентів Windows. Виключення становлять ролі файлового сервера (для цього потрібні тільки спільні папки) і сервера друку (для цього потрібно задати спільний доступ до приєднаних принтерів).

Відкрийте вкладку Add Or Remove Programs в Control Panel і клацніть на кнопку Add. Потім виконаєте прокручування, щоб знайти компонент, що вимагається для ролі, яку повинен виконувати даний комп'ютер у вашій мережі.

Для багатьох компонентів ви можете вибрати певні засоби й функції або вибрати всі засоби, доступні для даного компонента.

Якщо встановити компонент у такий спосіб, то роль цього компонента з'явиться в списку ролей, які представлені значенням Yes у колонці Configured майстра Configure Your Server Wizard. Ви можете видалити цей компонент (і відповідну роль) вручну у вкладці Add Or Remove Programs або за допомогою майстра.

Частина 2
Служба каталогів Active Directory

Мережі, служби каталогів і контролери доменів

Мережі були створено одного чудового дня, коли користувачеві набридло бігати по коридору, щоб обмінюватися даними з іншим користувачем. Зрештою, ціль будь-якої мережі - забезпечити дистанційний доступ до ресурсів. Колись це були файли, папки й принтери. Згодом до них додалися інші ресурси, найбільш важливими з яких є електронна пошта, бази даних і додатки. Потрібен був механізм, що дозволяє відслідковувати ресурси, і надає як мінімум каталог користувачів і груп, щоб запобігти небажаному доступу до ресурсів.

Мережі Microsoft Windows підтримують дві моделі служб каталогів: робочу групу (workgroup) і домен (domain). Для огранізацій, що впроваджують Windows Server 2003, модель домена є найбільш кращою. Модель домена характеризується єдиним каталогом ресурсів підприємства - Active Directory, - якому довіряють усі системи безпеки, що належать домену. Тому такі системи здатні працювати із суб'єктами безпеки (обліковими записами користувачів, груп і комп'ютерів) у каталозі, щоб забезпечити захист ресурсів. Служба Active Directory, таким чином, відіграє роль ідентифікаційного сховища й повідомляє "хто є хто" у цьому домені. Втім, Active Directory - не просто база даних. Це колекція файлів, включаючи журнали транзакцій і системний том (Sysvol), що містить сценарії входу в систему й відомості про групову політику. Це служби, що підтримують, і використовують БД, включаючи протокол LDAP (Lightweight Directory Access Protocol), протокол безпеки Kerberos, процеси реплікації й службу FRS (File Replication Service). БД і її служби встановлюються на один або кілька контролерів домена. Контролер домена призначається майстром встановленя Active Directory, який можна запустити за допомогою майстра налаштування сервера або командою DCPROMO з командного рядка. Після того як сервер стає контролером домена, на ньому зберігається копія (репліка) Active Directory, і зміни БД на будь-якому контролері реплікуються на всі інші контролери домена.

Домени, дерева і ліса

Active Directory не може існувати без домена й навпаки. Домен - це основна адміністративна одиниця служби каталогів. Однак підприємство може включити у свій каталог Active Directory більш одного домена. Коли кілька моделів доменів спільно використовують безперервний простір імен DNS, то вони утворюють логічні структури, що називаються деревами (tree). Наприклад, домены contoso.com , us.contoso.com і europe.contoso.com спільно використовують безперервний простір імен DNS, отже, вони становлять дерево.

Контролери домена - спеціальні сервери, які зберігають відповідну даному домену частину бази даних Active Directory.

Основні функції контролерів домена:

- зберігання БД Active Directory (організація доступу до інформації, що міститься в каталозі, включаючи керування цією інформацією і її модифікацію);
- синхронізація змін в AD (зміни в базі даних AD можуть бути внесені на кожному з контролерів домена, будь-які зміни, здійснювані на одному з контролерів будуть синхронізовані с копіями, що зберігаються на інших контролерах);
- аутентификация користувачів (кожний з контролерів домена здійснює перевірку повноважень користувачів, що реєструються на клієнтських системах).

Настійно рекомендується в кожному домені встановлювати не менш двох контролерів домена - по-перше, для захисту від втрати БД Active Directory у випадку виходу з ладу якого-небудь контролера, по-друге, для розподілу навантаження між контролерами.

Домены Active Directory з різними кореневими доменами утворюють кілька дерев. Вони поєднуються в саму більшу структуру Active Directory - ліс (forest). Ліс Active Directory містить усі домены в рамках служби каталогів. Ліс може складатися з декількох доменів у декількох деревах або тільки з одного домена. Коли доменів декілька, набуває важливість компонент Active Directory, називаний глобальним каталогом (global catalog): він надає інформацію про об'єкти, розташовані в інших доменах лісу.

Об’єкти і організаційні підрозділи

Ресурси підприємства представлені в Active Directory у вигляді об'єктів або записів у БД. Кожний об'єкт характеризується рядом атрибутів або властивостей. Наприклад, у користувача є атрибути ім'я користувача й пароль, у групи - ім'я групи й список користувачів, які в неї входять.

Для створення об'єкта в Active Directory відкрийте консоль Active Directory - користувачі й комп'ютери (Active Directory Users And Computers) у групі програм Адміністрування (Administrative Tools). Розкрийте домен, щоб побачити його контейнери й організаційні підрозділи. Клацніть контейнер або ОП правою кнопкою й у контекстному меню виберіть Створити (New) тип_об'єкта.

Служба Active Directory здатна зберігати мільйони об'єктів, включаючи користувачів, групи, комп'ютери, принтери, загальні папки, сайти, зв'язки сайтів, об'єкти групової політики (ОГП) і навіть зони DNS і записи вузлів. Можна представити, у який жах перетворився б доступ до каталогу і його адміністрування без певної структури.

Структура - мета введення характерного типу об'єкта, названого організаційним підрозділом (organization unit, OU). ОП являють собою контейнери усередині домена, що дозволяють групувати об'єкти, керовані або настроюються однаковим образом. Однак завдання ОП - не тільки організувати об'єкти Active Directory, вони забезпечують важливі можливості керування, оскільки утворюють

місце, куди можуть делегуватися функції керування і з якого можна зв'язати групові політики.

Делегування управління

Делегування прав керування засноване на простій ідеї, що адміністратори на місцях повинні мати можливість змінити пароль для певної підмножини користувачів. У кожного об'єкта в Active Directory (у нашому випадку - в об'єктів користувачів) є таблиця керування доступом (access control list , ACL), яка визначає дозволи доступу до цього об'єкта, аналогічно тому, як файли на томі жорсткого диска мають таблицю ACL, що визначає доступ до цих файлів. Наприклад, ACL об'єкта користувача буде визначати, яким групам дозволено скидати свій пароль. Було б неправильно змушувати адміністратора змінювати пароль кожного користувача: простіше помістити всіх потрібних користувачів в одне ОП і дозволити адміністраторові міняти в ньому паролі. Цей дозвіл буде успадковуватися всіма об'єктами користувачів в ОП, так що адміністратор зможе змінити дозвіл для всіх користувачів.

Скидання паролів користувачів - один із прикладів делегування адміністративних повноважень. Існують тисячі комбінацій дозволів, які можна було б призначити групам, відповідальним за адміністрування й підтримку Active Directory. ОП дозволяють підприємству створювати активне представлення адміністративної моделі й вказувати, хто й що може робити з об'єктами в домені.

Групова політика

ОП також використовуються для об'єднання однаково настроєних об'єктів - комп'ютерів і користувачів. Групова політика Active Directory дозволяє централізовано управляти практично будь-якими конфігураційними змінами системи. З її допомогою можна вказати настроювання безпеки, розгорнути ПО й настроїти поведінку ОС і додатків, навіть не доторкаючись до комп'ютерів користувачів. Ви просто реалізуєте свою конфігурацію в рамках одного ОГП.

ОГП складаються із сотень можливих конфігураційних параметрів: від прав і привілеїв користувача до ПО, яке дозволено запускати на системі. ОГП підключається до контейнера усередині Active Directory (звичайно до ОП, але може й до доменів або навіть сайтів), і після цього його настроювання поширюються на всіх користувачів і комп'ютери усередині цього контейнера.

Важливо запам'ятати, що групова політика - засіб централізованої реалізації конфігурації, що одні настроювання застосовуються тільки до комп'ютерів, а інші - тільки до користувачів, і що політика поширюється тільки на комп'ютери й користувачів з ОП, з яким вона зв'язана.

Інсталяція контролера домена (DC) на базі Windows Server 2003 за допомогою майстра встановлення Active Directory

1. Щоб запустити майстер підвищення статусу сервера необхідно в меню Start (Пуск) вибрати Run… увести dcpromo і нажати OK.

2. Після запуску майстра установки Active Directory натисніть Next (Далі).

3. На сторінці Domain Controller Type (Тип контролера домена) виберіть варіант Domain controller for a new domain (Контролер домена в новому домені). (Рис.2.5) Натисніть Next.

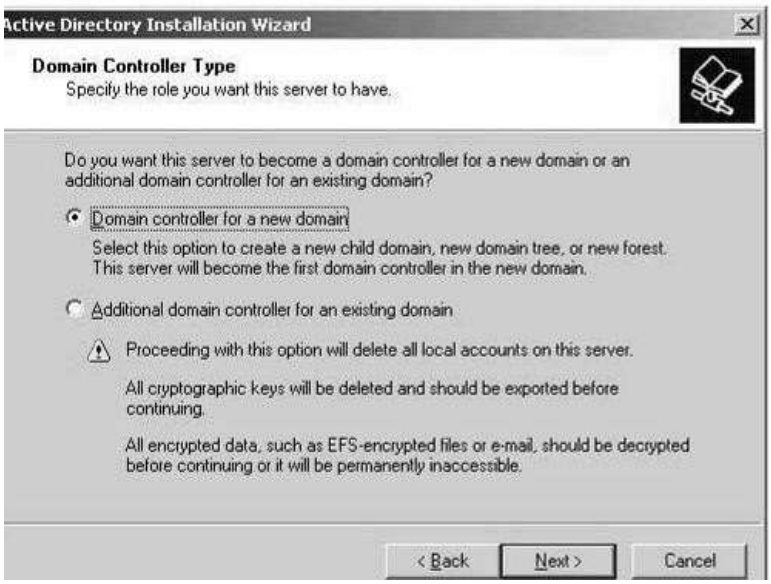


Рис.2.5

4. На сторінці Create New Domain (Створити новий домен) виберіть варіант Domain in a new forest (Новий домен у новому лісі). (Рис.2.6) Натисніть Next.

Рис.2.6

5. На сторінці New Domain Name (Нове ім'я домена)(Рис.2.7) уведіть повне (FQDN) Dns-ім'я для створюваного нового домена лісу Active Directory (наприклад, kszi.local). Не рекомендується використовувати одиночне (single label) ім'я домена (наприклад, kszi). Натисніть Next.

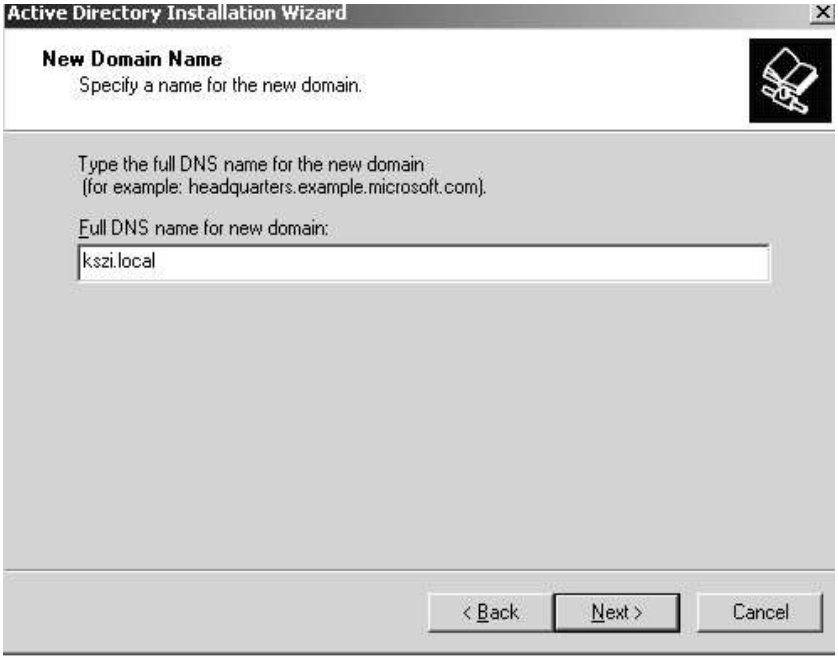


Рис.2.7

6. Перевірте Netbios- Ім'я на сторінці Netbios Domain Name (Netbios-Ім'я домена) (Рис.2.8). Хоча домени Active Directory позначаються у відповідності зі стандартами іменування DNS, необхідно так само задати Netbios-ім'я. Netbios-імена по можливості повинні збігатися з першої міткою DNS-імені домена. Якщо перша

мітка DNS-імені домена Active Directory відрізняється від його Netbios-імені, у якості повного доменного імені використовується DNS-ім'я, а не Netbios-ім'я. Натисніть Next.

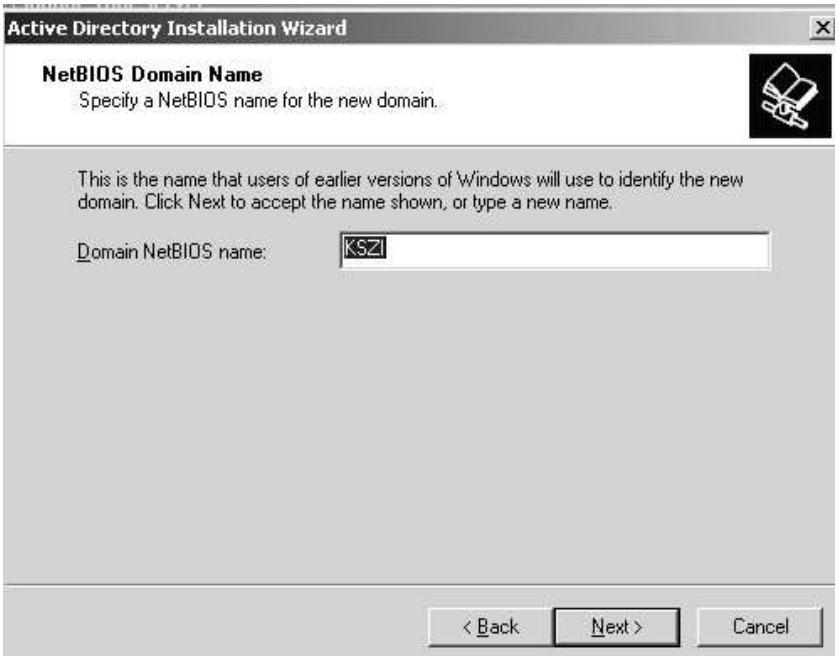


Рис.2.8

7. На сторінці Database and Log Folders (Папки бази даних і журналів) (Рис.2.9) уведіть шлях, по якому будуть розташовуватися папки бази даних і журналів, або натисніть кнопку Browse (Огляд), щоб указати інше розташування. Переконаєтеся, що на диску досить місця для розміщення бази даних каталогу й файлів журналів, щоб уникнути проблем при установці або видаленні Active Directory. Майстрові установки Active Directory необхідно 250 МБ дискового простору для установки бази даних Active Directory і 50 МБ для файлів журналів. Натисніть Next.

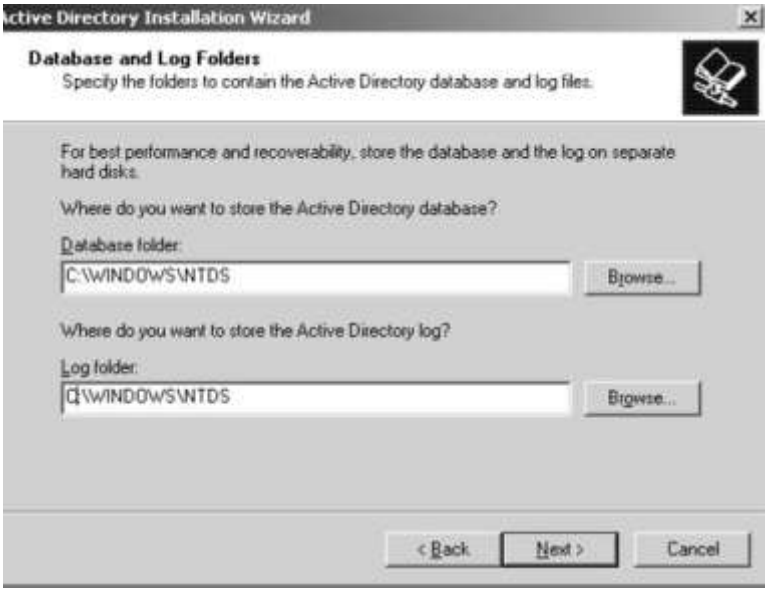


Рис.2.9

8. На сторінці Shared System Volume (Загальний доступ до системного тому) (Рис.2.10) укажіть розташування, у яке слід установити папку SYSVOL, або натисніть кнопку Browse (Огляд), щоб вибрати розташування. Папка SYSVOL повинна перебувати на томі NTFS, тому що в ній перебувають файли, репліковані між контролерами домена в домені або лісі. Ці файли містять сценарії, системні політики для Windows NT 4.0 і більш ранніх версій, загальні папки NETLOGON і SYSVOL і параметри групової політики. Натисніть Next.

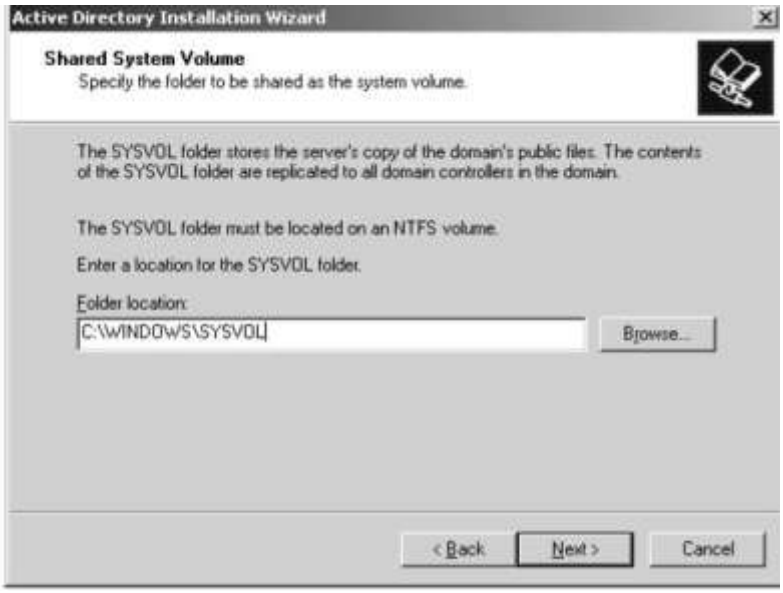


Рис.2.10

9. На сторінці DNS Registration Diagnostics (Діагностика реєстрації DNS) (Рис.2.11)перевірте правильність установки параметрів. Якщо у вікні Diagnostic Results (Результати діагностики) відображається повідомлення про помилку діагностики, натисніть кнопку Help (Довідка) для одержання додаткових інструкцій з усунення помилки. Натисніть Next.

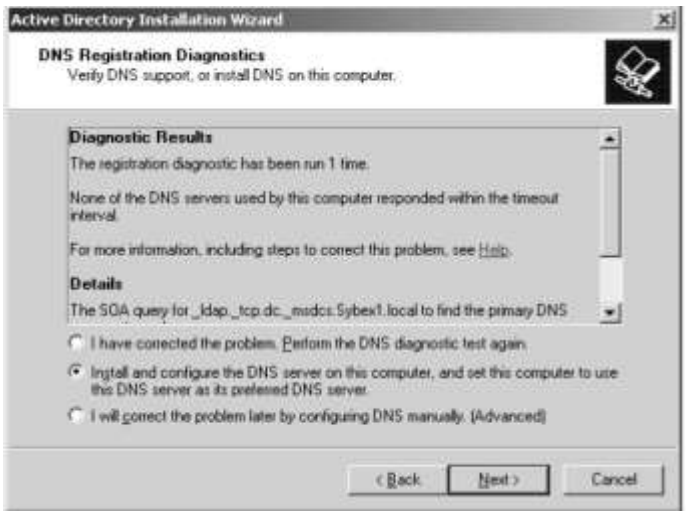


Рис.2.11

10. На сторінці Permissions (Дозволи) (Рис.2.12) виберіть необхідний рівень сумісності додатків з операційними системами pre-windows 2000, Windows 2000 або Windows Server 2003. Натисніть Next.

Рис.2.12

11. На сторінці Directory Services Restore Mode Administrator Password (Пароль адміністратора для режиму відновлення) (Рис.2.13) уведіть і підтвердіть пароль для

облікового запису адміністратора режиму відновлення Active Directory для даного сервера. Цей пароль необхідний для відновлення резервної копії стану системи даного контролера домена в режимі відновлення Active Directory. Натисніть Next.

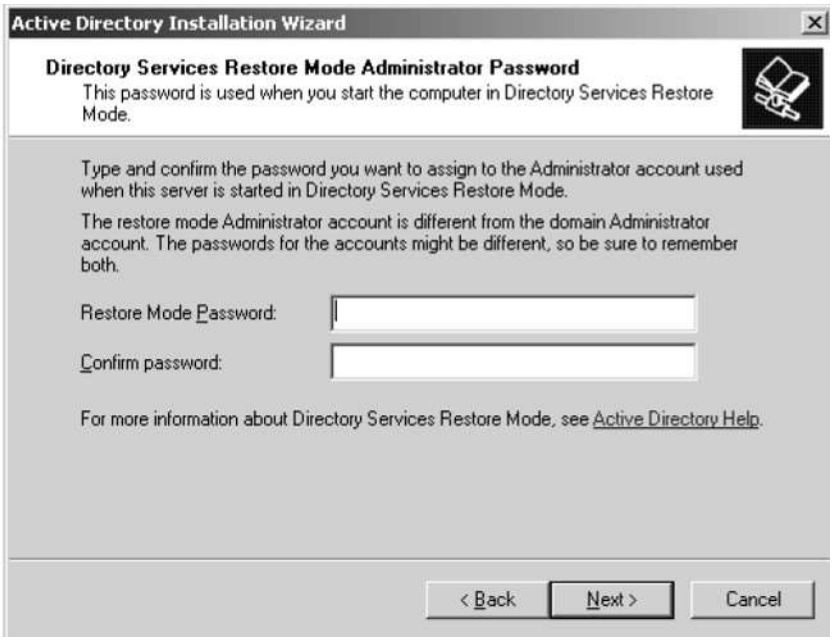


Рис.2.13

12. Перевірте відомості на сторінці Summary (Рис.2.14) і натисніть Next.

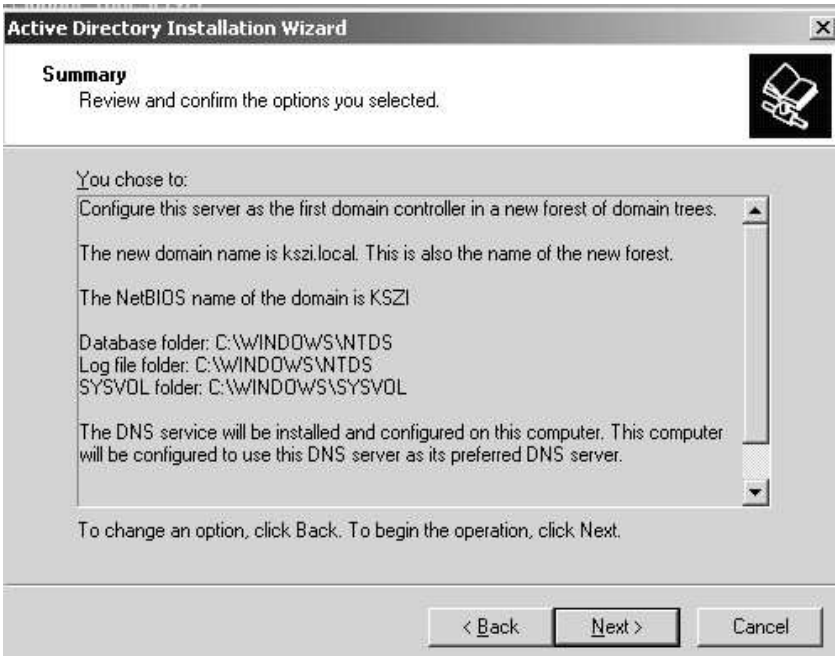


Рис.2.14

13. Після завершення установки натисніть кнопку Finish. Для перезавантаження комп'ютера натисніть кнопку Restart Now, щоб зміни набули чинності .

Основи управління доменом Active Directory

Ряд засобів у вкладках Microsoft Management Console (MMC) спрощує роботу з Active Directory.

Вкладка Active Directory Users and Computers (Active Directory - користувачі й комп'ютери) є консоллю керування MMC, яку можна використовувати для адміністрування й публікації відомостей у каталозі. Це головний засіб адміністрування Active Directory, який використовується для виконання всіх завдань, пов'язаних з користувачами, групами й комп'ютерами, а також для керування організаційними підрозділами.

Для запуску вкладки Active Directory Users and Computers (Active Directory - користувачі й комп'ютери) (Рис.2.15) виберіть однойменну команду в меню Administrative Tools (Адміністрування).

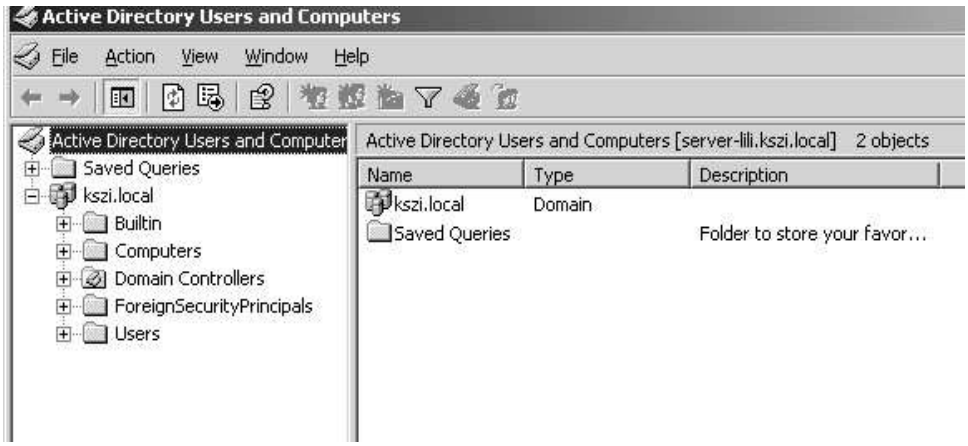


Рис.2.15

За замовчуванням консоль Active Directory Users and Computers (Рис.2.16) працює з доменом, до якого відноситься Ваш комп'ютер. Ви можете одержати доступ до об'єктів комп'ютерів і користувачів у цьому домені через дерево консолі або підключитися до іншого домену. Засоби цієї ж консолі дозволяють переглядати додаткові параметри об'єктів і здійснювати їхній пошук.

Одержавши доступ до домену ви побачите стандартний набір папок:

- Saved Queries (Збережені запити) - збережені критерії пошуку, що дозволяють оперативно повторити виконаний раніше пошук в Active Directory;
- Builtin - список вбудованих облікових записів користувачів;
- Computers - контейнер за замовчуванням для облікових записів комп'ютерів;

- Domain Controllers - контейнер за замовчуванням для контролерів домена;
- ForeignSecurityPrincipals - містить інформацію про об'єкти з довіреного зовнішнього домена.

Звичайно ці об'єкти створюються при додаванні в групу поточного домена об'єкта із зовнішнього домена;

- Users - контейнер за замовчуванням для користувачів.

Деякі папки консолі за замовчуванням не відображаються. Щоб вивести їх на екран, виберіть у меню View (Вид) команду Advanced Features (Додаткові функції). Ось ці додаткові папки:

- Lostandfound - об'єкти каталогу, що втратили власника;
- NTDS Quotas - дані про квотування служби каталогів;
- Program Data - збережені в службі каталогів дані для додатків Microsoft;
- System - вбудовані параметри системи.

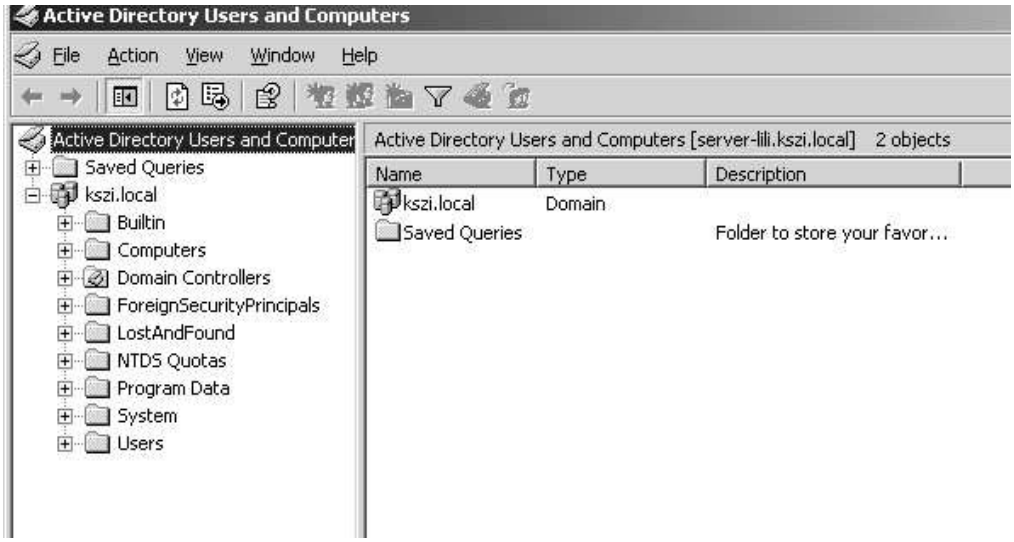


Рис.2.16

Ви можете самостійно додавати папки для організаційних підрозділів в дерево AD. (Рис.2.17)

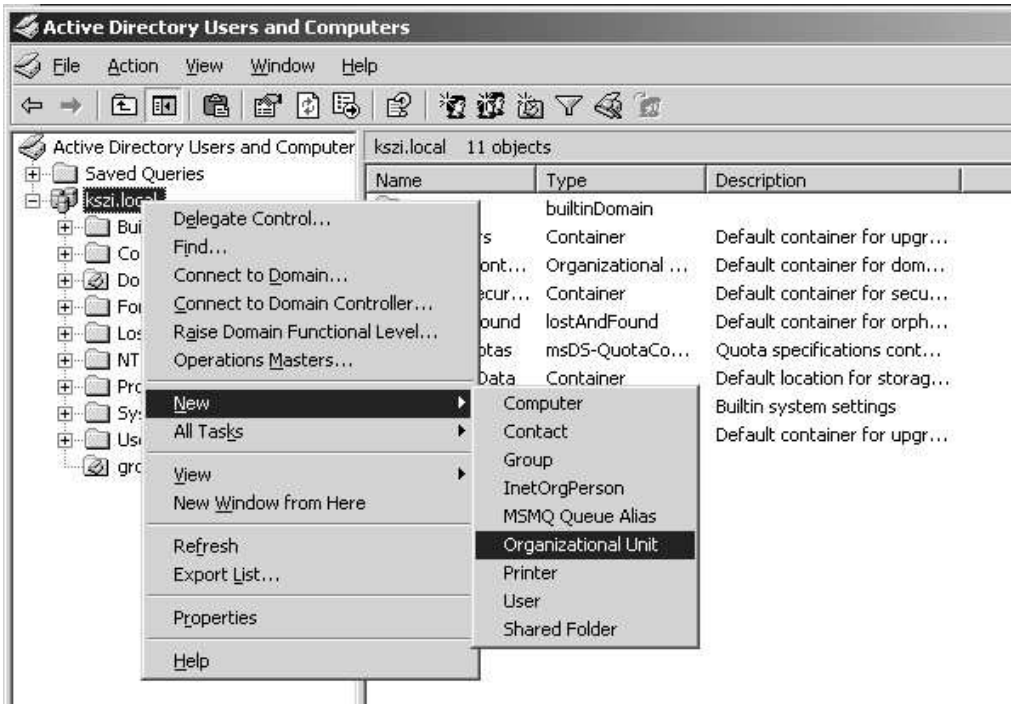


Рис.2.17

ПРАКТИЧНЕ ЗАВДАННЯ

1. Установити контролер домена на Windows Server 2003 з наступними параметрами:

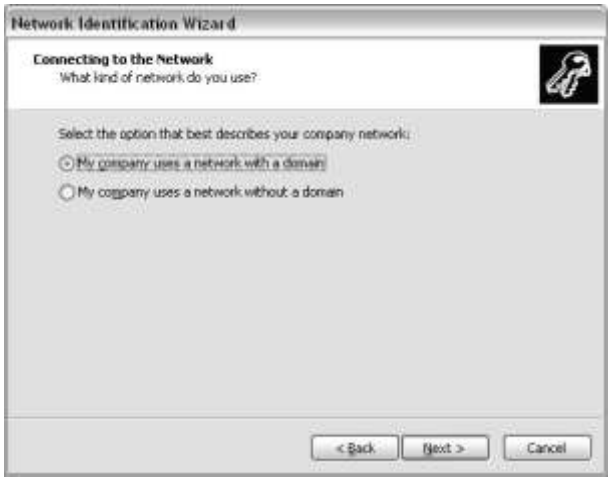
- Domain Name: kszi.local;
- Restore Mode Administration Password: leave as blank (залишити порожнім);

2. Приєднати комп'ютер з Windows XP Professional до домену Windows 2003 у такий спосіб:

- Вибрати вкладку властивостей для My Computer из Windows XP Professional;
- В вкладці Computer Name натиснути Network Id;
- Зробити кроки згідно малюнкам:


Network Identification Wizard
Welcome to the Network Identification Wizard
This wizard helps you connect your computer to a network.
To continue, click Next.
< Back
Next >
Cancel


Network Identification Wizard
Connecting to the Network
How do you use this computer?
Select the option that best describes your computer:
This computer is part of a business network, and I use it to connect to other computers at work.
This computer is for home use and is not part of a business network.
< Back
Next >
Cancel


Network Identification Wizard
Connecting to the Network
What kind of network do you use?
Select the option that best describes your company network:
My company uses a network with a domain
My company uses a network without a domain
< Back
Next >
Cancel


Network Identification Wizard
Network Information
Gather domain and account information before you proceed.
To connect your computer to a Windows network, you need the following information:
• User name
• Password
• User account domain
You might also need:
• Computer name
• Computer domain
If you do not have this information, contact your network administrator before proceeding.
< Back
Next >
Cancel


Network Identification Wizard
User Account and Domain Information
A user account gives you access to files and resources on a network.
Type your Windows user account and domain information. If you do not have this information, ask your network administrator.
User name:
Administrator
Password:
Domain:
KSZI.LOCAL
< Back
Next >
Cancel


Network Identification Wizard
User Account
You can add a user to this computer.
Adding a user to this computer grants the user access to all the resources on this computer and to all shared resources on the network.
Type your network user account information, or type the account information of another user on your network.
Add the following user:
Do not add a user at this time.
< Back
Next >
Close


Network Identification Wizard
Completing the Network Identification Wizard
You have successfully completed the Network Identification Wizard.
Your computer must be restarted in order for these changes to take effect.
To close this wizard and restart your computer, click Finish.
< Back
Finish
Close


Computer Name Changes
You must restart this computer for the changes to take effect.
OK