ВСТУП

Незважаючи на те, що корпоративні мережі зазвичай використовують безліч операційних систем, особливо на серверах, на більшості робочих станцій, призначених для користувача, зазвичай установлена одна із версій Windows. Інтерфейс Windows є інтуїтивним і дружнім, немає жодних сумнівів у тому, що адміністрування серверів та сотень тисяч робочих станцій Windows являє собою вкрай масштабну задачу. Операційні системи Windows містять різні інструменти, які адміністратори мереж можуть застосовувати для полегшення процесів установлення, керування й обслуговування операційних систем великої кількості серверів і робочих станцій, але найбільшої уваги заслуговує служба Active Directory.

Active Directory — LDAP-сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft для операційних систем родини Windows NT. Active Directory дозволяє адміністраторам використовувати групові політики (GPO) для забезпечення подібного налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів (через групові політики або за допомогою Microsoft Systems Management Server (або System Center Configuration Manager)), встановлювати оновлення ОС, прикладного та серверного ПЗ на всіх комп'ютерах в мережі (із використанням Windows Server Update Services (WSUS); Software Update Services (SUS) раніше). Active Directory зберігає дані і налаштування середовища в централізованій базі даних. Мережі Active Directory можуть бути різного розміру: від кількох сотень до кількох мільйонів об'єктів.

Завдяки своїм можливостям AD здобув велику кількість користувачів, мільйони мереж працюють завдяки цій службі. Також в AD присутня групова політика, яка дозволяє налаштовувати широкий спектр налаштувань одночасно на робочих станціях всіх користувачів, або окремо взятої групи, тому дуже полегшує роботу системному адміністратору.

На даний момент Active Directory вважаться найкращим компонентом в своїй сфері для адміністрування.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ТЕХНОЛОГІЇ

1.1 Організація корпоративних мереж. Служба каталогу

Корпоративна мережа — це мультисервісна мережа передачі даних, що працює під єдиним керуванням і призначена для задоволення власних виробничих потреб компанії та організації.

Залежно від розмірів організації, що розгортає корпоративну мережу, робоче середовище корпорації може містити в собі як невелику кількість комп'ютерів, що розміщені в межах одного будинку, так і величезну кількість комп'ютерних робочих місць, що знаходяться на географічно розподіленій території. В тому та в іншому випадку виникає необхідність такої організації мережі, при якій буде забезпечена найбільш ефективна можливість взаємодії користувачів в майже реальному часі із наданням можливості спільного використання ресурсів, зручність керування обліковими даними користувачів та іншими характеристиками мережі, а також масштабованість, тобто незалежність принципів роботи мережі від кількості її вузлів.

1.1.1 Поняття служби каталогу

В комп'ютерній мережі корпорації взаємодіє величезна кількість об'єктів, зокрема, файлові сервери, принтери, факс-сервери, додатки, бази даних, користувачі. Для забезпечення їхнього надійного зберігання необхідні спеціальні структури у вигляді каталогів.

Каталогом (directory) називається сукупність інформації про об'єкти, які тим або іншим способом зв'язані один з одним. Приміром, в адресній книзі клієнта електронної пошти зберігаються імена користувачів і відповідні їм адреси

електронної пошти. Крім того, в неї можуть бути включені фізичні адреси та інші додаткові відомості про користувачів.

Оскільки в каталогах зберігаються самі різні об'єкти - завдання полягає в тому, щоб надати користувачам можливість знайти та застосувати ці об'єкти, керовані адміністраторами.

Служба каталогу (directory service) забезпечує зберігання всієї необхідної для застосування об'єктів і керування ними інформації в єдиному місці розташування, таким чином, процес виявлення та керування ресурсами значно спрощується. Крім того, служба каталогу надає зручний доступ до відомостей про різні об'єкти мережі, допомагаючи користувачам і додаткам знайти ці об'єкти. Таким чином, на відміну від каталогу, служба каталогу одночасно виконує дві ролі: джерела інформації та механізму, за допомогою якого ця інформація готується для доступу з боку користувачів.

Служба каталогу – є основною панеллю управління мережевої операційної системи. Це остання інстанція, що управляє ідентифікаторами, виступає посередником у взаємодії між розподіленими ресурсами та змушує їх працювати спільно. Оскільки служба каталогу забезпечує виконання операційною системою її основних функцій, то лише завдяки тісній інтеграції служби каталогу з механізмами управління і захисту операційної системи реалізуються такі характеристики мережі, як цілісність і конфіденційність. Саме від служби каталогу багато в чому залежить здатність компанії до проектування, впровадження і обслуговування мережевої інфраструктури, адміністрування системи та координації дій користувачів при взаємодії з корпоративними інформаційними системами.

1.2 Активний каталог Active Directory

Active Directory (AD) – це ієрархічно організоване сховище, що надає зручний доступ до відомостей про різні об'єкти мережі, допомагаючи користувачам і додаткам знайти ці об'єкти. До того ж тут відбувається перевірка, чи є у користувача, що запросив інформацію, право на її одержання. Список

користувацьких прав також розміщується в базі даних Active Directory.Службі каталогу Active Directory характерні наступні ознаки:

– Централізоване зберігання даних. Всі дані, що відносяться до Active Directory, зберігаються в єдиному розподіленому репозитарії, що надає можливість доступу до них із будь-якого місця розташування. Наявність єдиного розподіленого сховища даних скорочує витрати, пов'язані з адмініструванням і дублюванням, і підвищує доступність та організацію даних.

– Масштабованість. Active Directory дозволяє масштабувати каталог відповідно до комерційних і мережевих вимог шляхом конфігурування доменів і дерев, а також введення нових або переміщення контролерів доменів. Об'єкти в складі одного домена Active Directory можуть налічувати мільйони; продуктивність при цьому підвищується за рахунок застосування технології індексування та прогресивних методик реплікації.

– Розширюваність. Структура бази даних (схема) Active Directory припускає можливість розширення забезпечуючи можливість роботи із спеціальними типами інформації.

– Керованість. На відміну від простої доменної моделі Windows NT, Active Directory ґрунтується на ієрархічних структурах. Ці структури спрощують, поперше, керування адміністративними привілеями та іншими настроюваннями безпеки, а по-друге, виявлення користувачами таких мережевих ресурсів, як файли та принтери.

– Інтеграція із системою доменних імен (DNS). Active Directory звертається до DNS - стандартної служби Інтернет, призначеної для трансляції зручних у читанні імен вузлів у числові адреси протоколу Інтернет (Internet Protocol, IP).

– Управління конфігураціями клієнта. Active Directory передбачає нові технології управління елементами конфігурації клієнта – зокрема, мобільністю користувача та збоями жорстких дисків; адміністрування і втрати часу користувачем при цьому зводяться до мінімуму.

– Адміністрування на основі політик Політики в Active Directory визначають дозволені операції та настроювання, задані для користувачів і комп'ютерів у рамках даного сайту, домена або підрозділу. Керування на основі політик значно спрощує такі завдання, як відновлення операційної системи, установка додатків, створення користувальницьких профілів і блокування настільних систем.

– Реплікація даних. Реалізована в Active Directory технологія реплікації з декількома хазяїнами забезпечує готовність інформації, відмовостійкість, вирівнювання навантаження, і крім того значно підвищує продуктивність. Реплікація з декількома хазяїнами дозволяє оновляти каталог на будь-якому окремо взятому контролері домена й реплікувати ці зміни на всі інші контролери. Оскільки в процесі бере участь кілька контролерів домена, реплікація триває навіть у випадку виходу з ладу одного з них.

– Гнучкість і безпека процесів автентифікації та авторизації. Служби автентифікації та авторизації Active Directory гарантують надійний захист даних і зводять до мінімуму обмеження на комерційну діяльність у мережі Інтернет.

1.3 Поняття об'єкту Active Directory. Схема Active Directory

Дані, що зберігаються в Active Directory, - зокрема, інформація про користувачів, принтери, сервери, бази даних, групи, комп'ютери і політики - систематизуються в рамках об'єктів.

Об'єкт (object) - це окремий іменований набір атрибутів, які представляють мережевий ресурс, наприклад, одним з об'єктів є користувацький обліковий запис, що присвоюється конкретному користувачеві, також обліковий запис комп'ютера, що відповідає окремому комп'ютеру і т.д.. Атрибутами об'єктів називаються їхні характеристики в рамках каталогу. Приміром, серед характеристик об'єкта користувацького облікового запису можна виділити ім'я та прізвище користувача, його ім'я входу; атрибутами облікового запису комп'ютера можуть бути ім'я цього

комп'ютера і його опис. Існує категорія об'єктів, до складу яких можуть входити інші об'єкти. Вони називаються контейнерами (containers). Приміром, існує такий контейнер як домен, він містить об'єкти облікових записів користувачів і комп'ютерів, що входять у цей домен. Папка Users являє собою контейнер, що включає в себе об'єкти користувальницьких облікових записів. Контейнер Computers містить облікові записи комп'юрів даного домена.

Об'єкти, які можна зберігати в каталогах Active Directory встановлює схема Active Directory.

Схемою (schema) називається список, що визначає види об'єктів і типи інформації про них, що зберігаються в Active Directory. Самі визначення схеми також зберігаються у вигляді об'єктів, тому адмініструвати їх можна так само, як і всі інші об'єкти Active Directory.

Схема визначається двома типами об'єктів: об'єктами класів схеми (які також називаються класами схеми) і об'єктами атрибутів схеми (атрибутами схеми). Об'єкти класів і об'єкти атрибутів знаходяться в різних списках схеми. У об'єктів класів схеми та об'єктів її атрибутів є дві збірних назви: об'єкти схеми (schema objects) і метадані (metadata).

Об'єкти класів схеми (schema class objects) описують об'єкти, які можна створювати в Active Directory. Клас схеми виконує роль шаблона для створення нових об'єктів Active Directory. Наприклад, існує такий клас схеми як Користувач (User), на основі якої створюються облікові записи для всіх користувачів мережі.

Кожний клас схеми являє собою сукупність об'єктів атрибутів схеми. При створенні класу схеми інформація, що характеризує об'єкт, зберігається саме в складі атрибутів, наприклад клас User складається з великої кількості атрибутів схеми, — у тому числі, Network Address і Home Directory.

Кожний об'єкт, що управляється Active Directory, фактично є екземпляром того або іншого об'єкта класу схеми.

Об'єкти атрибутів схеми (schema attribute objects) визначають об'єкти класів схеми, з якими вони асоційовані. Атрибути схеми можна задіяти в будь-якій кількості класів. Взяти хоча б атрибут Description, цей атрибут застосовується в

самих різних класах, разом з тим він визначений тільки в одній схемі, за рахунок чого забезпечується відсутність суперечності.

На основі вище сказаного можна надати наступне визначення схеми. Схема - це набір класів об'єктів і атрибутів, з яких створюються екземпляри об'єктів Active Directory.

В поставці Active Directory є в наявності ряд базових класів і атрибутів схеми. Досвідченим розробникам і мережевим адміністраторам цілком під силу динамічно розширювати схему, вводячи в неї нові класи та визначення вже існуючих атрибутів. Приміром, для того щоб ввести дотепер не визначену в схемі інформацію про користувачів, потрібно розширити клас схеми User. Треба, втім, мати на увазі, що розширення схеми - операція складна, і наслідки її проведення можуть бути досить серйозними.

Крім того, Active Directory не дозволяє видаляти що-небудь зі схеми, є можливість тільки деактивізувати класи об'єктів або атрибутів. Деактивізація якого-небудь класу не призводить до видалення екземплярів об'єктів, що використовують деактивізований клас. Вони як і раніше будуть присутні в Active Directory. Правда, не можна буде створювати нові екземпляри цих об'єктів. Для видалення таких об'єктів потрібно організувати їхній пошук по всьому каталогу.

Оскільки видалити схему не можна (можна тільки деактивізувати), а, крім того, вона підлягає автоматичній реплікації, її розширення потрібно ретельно планувати та готувати.

1.4 Структура Active Directory

В Active Directory передбачений ряд компонентів, що допомагають побудувати структуру каталогів відповідно до потреб компанії. Існують логічні та фізичні структури.

Логічні організаційні структури представлені наступними компонентами Active Directory: доменами, підрозділами (organizational units, OUs), деревами та лісами.

Фізичні організаційні структури представлені сайтами (фізичними підмережами) і контролерами домена. Логічна і фізична структури в Active Directory, таким чином, повністю розведені.

1.4.1. Логічна структура Active Directory

Систематизації ресурсів Active Directory в рамках логічної структури служать домени, підрозділи, дерева та ліси. Логічне угруповування дозволяє шукати ресурси по іменах, не запам'ятовуючи їхнє фізичне місце розташування. Оскільки ресурси групуються по логічному принципу, фізична структура мережі в Active Directory залишається прихованою від користувача. Відносини між доменами, підрозділами, деревами і лісами Active Directory представлені на рисунку 1.1

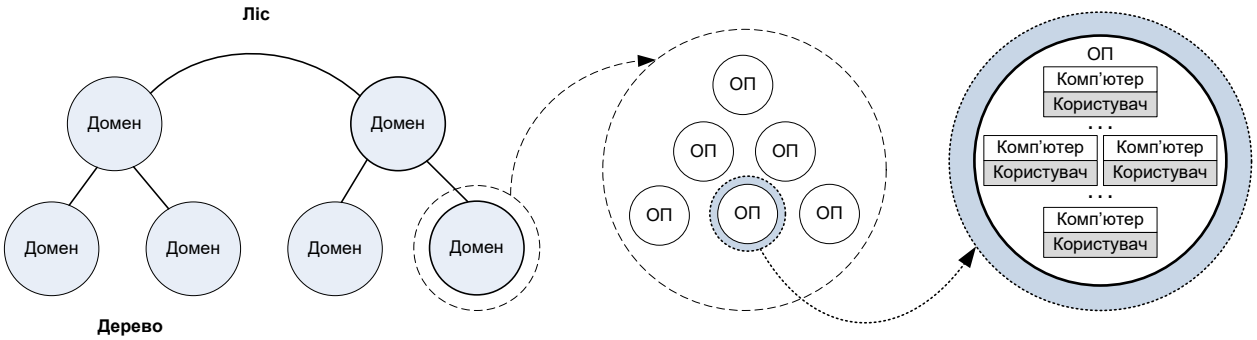

Рис. 1.1 – Відносини між доменами, підрозділами, деревами і лісами Active Directory

Домени

Базовою одиницею логічної структури в Active Directory є домен (domain). Об'єкти, що зберігаються в рамках домена, можуть нараховуватися мільйонами. До них відносяться принтери, документи, адреси електронної пошти, користувачі, розподілені компоненти та інші ресурси. В Active Directory може бути один або більше доменів.

Іноді домен поширюється на кілька фізичних місць розташування. Характеристики, загальні для всіх доменов, такі:

– Домен - це елемент каталогу, що має свій власний простір імен.

– Всі мережеві об'єкти існують у рамках певного домену, при цьому в кожному домені зберігається інформація тільки про ті об'єкти, які містяться в ньому.

– Границями домена визначаються границі системи безпеки, тобто всередині домена діють правила безпеки, що не розповсюджуються за його межі. Доступ до об'єктів домена регламентується списками керування доступом (access control lists, ACLs), в яких містяться пов'язані з об'єктами дозволи. Ці дозволи визначають, які користувачі можуть звертатися до об'єктів і який тип доступу для них відкритий. Об'єктами при цьому вважаються файли, папки, загальні ресурси, принтери та деякі об'єкти Active Directory. Всі політики і настроювання безпеки, будь то адміністративні права, права політики безпеки або списки ACL, поширюються строго в масштабах одного домена. У адміністратора домена є необмежені повноваження по настроюванню політик в рамках цього домена.

Підрозділи

Домен Active Directory має ієрархічну структуру. Ієрархічна будова домена значно полегшує роботу адміністратора, одночасно збільшуючи гнучкість настроювання різних параметрів у мережі.

Ієрархію домена утворять контейнери типу «організаційна одиниця» (OU, organisation unit), ще їх називають підрозділами.

Підрозділом називається контейнер, метою створення якого є систематизація об'єктів домена в рамках логічної адміністративної групи. Підрозділи дозволяють вирішувати різного роду адміністративні завдання - зокрема, пов'язані з адмініструванням користувачів і ресурсів. До складу підрозділу можуть входити такі об'єкти, як користувацькі облікові записи, групи, комп'ютери, принтери, додатки, загальні файли, а також інші підрозділи, що належать до цього домену.

Ієрархія підрозділів в рамках домена незалежна від ієрархічної структури підрозділів в інших доменах - таким чином, у кожному домені можна реалізувати індивідуальну ієрархію. За рахунок входження одних підрозділів в інші (інакше кажучи, за рахунок їхнього вкладення) адміністративне керування набуває ієрархічного характеру.

Існують деякі стандартні підрозділи Active Directory: Users, Computers, Domain Controllers та ін.

Дерева

Деревом (tree) називається угруповування або ієрархічна система одного або декількох доменів. Формується дерево шляхом введення одного або декількох дочірніх доменів до складу існуючого батьківського домена.

Всі вхідні в дерево домени характеризуються суміжними просторами імен та ієрархічною структурою імен. Відповідно до стандартів DNS, доменне ім'я дочірнього домена формується як його відносне ім'я у відповідності з іменем батьківського домена. Наприклад на рисунку 1.2 представлено дерево доменів, в якому домен microsoft.com виступає в ролі батьківського домена, а us.microsoft.com і uk.microsoft.com — в ролі дочірніх доменів. В свою чергу, стосовно uk.microsoft.com дочірнім є домен sls.uk.microsoft.com. На кількість доменів, що утворять дерево, обмежень немає.

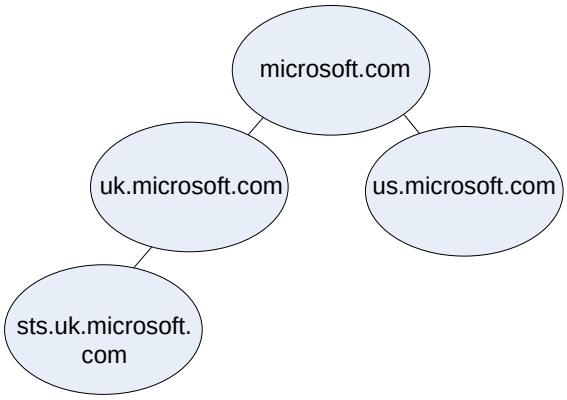

Рис. 1.2 – Дерево доменів

Створення в рамках дерева ієрархічної системи доменів дозволяє підтримувати на належному рівні безпеку та здійснювати адміністративні функції в масштабах підрозділу або окремого домена, що входить до складу дерева. Деревоподібна структура легко піддається модифікації, яка відображає зміни в організаційній структурі.

Задіяти в мережевому середовищі можливості Active Directory, що розповсюджуються на конкретний домен дозволяє режим роботи домена (domain functional level) або режим домена (domain mode).

Ліс

Лісом (forest) називається угруповування або ієрархічна система, що складається з одного або декількох повністю незалежних один від одного дерев доменів.

Нижче перераховані загальні характеристики лісів.

– Всі домени в складі лісу побудовані на основі загальної схеми.

– Всі домени лісу зв'язані неявними двосторонніми транзитивними довірчими відносинами.

– Структури імен дерев лісу різняться е відповідності з доменами.

– Домени в складі лісу функціонують незалежно один від одного, але в той же час ліс забезпечує шляхи інформаційного обміну в масштабі всієї організації.

Зображені на рисунку 1.3 дерева microsoft.com і msn.com утворюють ліс. Суміжність просторів імен спостерігається винятково в рамках окремих дерев.

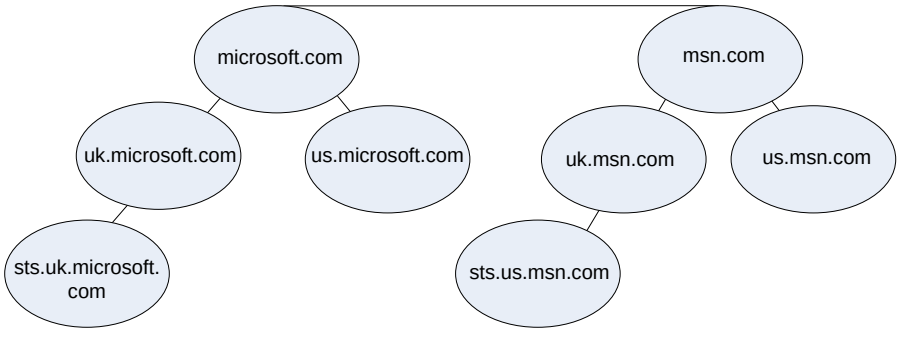

Рис. 1.3 – Ліс дерев

Активізувати в мережевому середовищі можливості Active Directory, пов'язані з конкретним лісом дозволяє режим роботи лісу (forest functional level).

1.4.2 Фізична структура Active Directory

Фізичними компонентами Active Directory є сайти та контролери домена.

Сайти

Сайтом або вузлом (site) називається IP-підмережа або сукупність таких підмереж, з'єднаних одна з одною надійним каналом з високою швидкістю передачі даних, що має на меті локалізувати як можна більший обсяг мережевого трафіка. Як правило, границі сайту збігаються із границями локальної мережі (local area network, LAN).

Підмережею називається підрозділ IP-мережі. Швидкими вважаються мережі із пропускною здатністю від 512 Кбіт/с. Для сайту потрібно, щоб корисна пропускна здатність становила не менше 128 Кбіт/с. Корисною пропускною здатністю (available bandwidth) називається пропускна здатність у період пікового навантаження за винятком стандартного мережевого трафіка.

Структура сайтів, що відповідає фізичному середовищу, обслуговується окремо від середовища логічного. Оскільки сайти не залежать від структури доменів, в домені може бути один або більше сайтів, і навпаки - в сайті може бути один або більше доменів.

Будь-який сайт служить цілям фізичної організації комп'ютерів і оптимізації мережевого трафіка. Сайти дозволяють обмежити область перевірки справжньості і трафік реплікації локальними пристроями. Оскільки мережевий трафік при цьому не пропускається через повільні канали глобальної мережі (WAN), навантаження на неї також знижується.

Існує дві основні ролі для сайта:

– спрощення перевірки справжньості користувачів робочих станцій шляхом пошуку найближчого контролера;

– спрощення міжсайтової реплікації даних.

Оскільки імена сайтів вносяться службою виявлення доменів в систему доменних імен (Domain Name System, DNS), вони повинні бути коректними іменами DNS.

Контролери домена

Комп'ютер, на якому працює служба каталогу, називається контролером домена (DC, Domain Controller). Всі запити до активного каталогу й взагалі всі запити, що стосуються доступу до інформації, яка зберігається в домені, обробляє саме цей комп'ютер. Будь-який контролер може обслуговувати лише один домен. Контролер домена проводить автентифікацію при спробах реєстрації користувачів і забезпечує виконання політики безпеки домена.

Роль управління доменом - настільки важлива в мережі функція, що від неї прямо залежить робота мережі. Тому і доступ до контролерів домена надається з більшою обережністю, ніж до інших серверів, а самі ці комп'ютери мають найвищий ступінь безпеки (як з погляду мережевого доступу, так і чисто фізично) і оснащуються самим надійним обладнанням. У великих мережах вони ніколи не виконують додаткових серверних функцій (не бувають серверами друку, серверами додатків, файловими серверами і т.д.).

Реалізація доменної моделі мережі починається з встановлення контролера домена.

Для забезпечення стабільної роботи домена у випадку виходу з ладу бази даних Active Directory, в домені створюється кілька контролерів домена на яких містяться копії (репліки) баз даних Active Directory. В процесі роботи зміни внесені в БД на одному контролері домена копіюються на інші, тобто виконується процес реплікації бази даних Active Directory на інші контролери домена. Більш детально поняття реплікації буде розглянуто нижче.

При реалізації служби Active Directory можна додавати стільки контролерів доменов, скільки необхідно для підтримки служби каталогу в даній організації.

Нижче наведений узагальнений список, що характеризує функції контролерів домена.

– На кожному контролері домена зберігається повна копія інформації Active Directory, що відноситься до даного домену. Контролер управляє змінами цієї інформації та реплікує на всі інші контролери свого домена.

– Контролери домена автоматично проводять реплікацію інформації каталогу, що відноситься до всіх об'єктів домена. Будь-яка операція, що має своїм результатом оновлення Active Directory, фактично призводить до внесення змін в інформацію, що зберігається на одному з контролерів домена. Потім цей контролер реплікує зміни на всі інші контролери даного домена. Трафік реплікації між контролерами домена можна обчислити як добуток частоти реплікації та максимального обсягу даних, що реплікуються за один раз.

– Окремі види інформації - наприклад, відомості про відключення користувацьких облікових записів - контролери домена реплікують негайно.

– В Active Directory використовується реплікація з декількома хазяїнами. В цих умовах жоден контролер домена не є головним. Навпроти, всі контролери рівноправні - на кожному з них міститься копія бази даних каталогу з можливістю запису в неї нових даних. В певні моменти, протягом нетривалого часу, інформація на різних контролерах домена може відрізнятися; втім, після синхронізації змін в Active Directory все встає на свої місця.

– Незважаючи на реалізовану в Active Directory підтримку реплікації з декількома хазяїнами, деякі зміни непрактично проводити в цьому режимі. Час від часу (для виконання операцій, які не можна проводити відразу в декількох місцях мережі) засобами одного або декількох контролерів домена здійснюється реплікація з одним хазяїном. При проведенні реплікації з одним хазяїном один або кілька контролерів домена відіграють роль хазяїна операцій (operations master role).

– Контролери домена є відповідальними за виявлення конфліктів, які, зокрема, відбуваються, коли, до повного поширення змін атрибута з одного контролера домена цей атрибут змінюється на іншому контролері. Конфлікти виявляються шляхом порівняння номерів версій властивостей атрибутів -

унікальних для кожного атрибута чисельних значень, які ініціюються в момент його створення. Для вирішення конфліктів Active Directory поширює змінений атрибут з більшим номером версії властивості.

– Наявність в домені декількох контролерів підвищує відмовостійкість. У випадку, якщо один з них стає недоступним, всі необхідні функції на зразок запису змін в Active Directory бере на себе інший контролер.

Глобальний каталог

Active Directory дозволяє користувачам і адміністраторам шукати в своїх доменах різного роду об'єкти - наприклад, файли, принтери та користувачів. Для того щоб шукати і знаходити об'єкти, розташовані поза межами конкретного домена, але в рамках підприємства, потрібен механізм, здатний консолідувати домени в єдиний логічний об'єкт. Таким механізмом в Active Directory є глобальний каталог.

Глобальним каталогом (global catalog) називається центральний репозитарій інформації про об'єкти дерева або лісу. За замовчуванням глобальний каталог автоматично створюється на вихідному контролері першого домена лісу. Контролер домена, на якому зберігається копія глобального каталогу, називається сервером глобального каталогу (global catalog server). Сервером глобального каталогу можна призначити будь-який контролер домена в рамках даного лісу.

Інформація із глобального каталогу в Active Directory поширюється між серверами глобального каталогу в інших доменах шляхом реплікації з декількома хазяїнами. На сервері зберігається повна репліка всіх атрибутів об'єктів каталогу, що належать домену-власнику, і часткова репліка атрибутів об'єктів каталогу, що відносяться до всіх інших доменів лісу. Часткова репліка містить в собі найбільш часто використовувані при операціях пошуку атрибути (наприклад, імена та прізвища користувачів, їхні реєстраційні імена й т.д.). Помітка і скасування помітки атрибутів, обраних для реплікації, здійснюється в глобальному каталозі одночасно з їх визначенням в схемі Active Directory. Атрибути об'єктів, що реплікуються в

глобальний каталог, успадковують дозволи від своїх екземплярів у вихідних доменах, таким чином, забезпечується безпека даних у глобальному каталозі.

Функції глобального каталогу

У глобального каталогу є дві основних функції:

– за його допомогою реєстрація користувача в мережі зводиться до надання контролеру домена, на якому ініціюється процес реєстрації, інформації про членство в універсальних групах;

– він дозволяє проводити пошук інформації в каталозі не залежно від того, який саме домен у складі лісу містить дані, що шукаються.

Якщо в домені є в наявності єдиний контролер, саме на ньому розміщений сервер глобального каталогу. Якщо в мережі кілька контролерів домена, глобальний каталог розміщається на одному з них.

Глобальний каталог покликаний відповідати на програмні запити та запити користувачів щодо будь-яких об'єктів, в якому б місці дерева доменів вони не розміщувалися, з максимальною швидкістю і мінімальним споживанням мережевого трафіка. Оскільки кожний глобальний каталог містить інформацію про всі об'єкти у всіх доменах лісу, запити про відсутніх у локальному домені об'єктах обробляються на сервері глобального каталогу в домені, у якому ці запити ініціюються. Таким чином, пошук інформації в каталозі не пов'язаний з генерацією додаткового трафіка поза границями даного домена.

Процес подачі запиту

Запит (query) подається користувачем у глобальний каталог з метою отримати, змінити або видалити потрібні дані Active Directory.

Процес подачі запиту складається з наступних етапів:

– Клієнт запитує DNS-сервер про місце розміщення сервера глобального каталогу.

– DNS-сервер проводить пошук місця розміщення сервера глобального каталогу, і повертає IP-адресу призначеного таким контролера домена.

– Клієнт відсилає запит на IP-адресу контролера домена, призначеного сервером глобального каталогу. На відміну від стандартних запитів Active Directory, які проходять через порт 389 на контролері домена, запити цього типу відправляються на порт 3268.

– Сервер глобального каталогу обробляє запит. Якщо атрибут потрібного об'єкта присутній у глобальному каталозі, сервер відправляє клієнтові відповідь. Якщо ж цього атрибута в ньому не виявляється, запит перенаправляється в Active Directory.

Настроїти в ролі сервера глобального каталогу можна будь-який контролер домена, на цю ж роль можливо призначити ще кілька допоміжних контролерів. При прийнятті рішення про те, які контролери домена найкраще зробити серверами глобального каталогу, необхідно враховувати можливості мережевої структури в плані обробки трафіка реплікації та трафіка запитів.

Крім описаних вище компонентів, що представляють фізичну структуру Active Directory необхідно відзначити що, фізичне представлення служби Active Directory відображається в наявності окремого файлу даних Ntds.dit, розташованого на кожному контролері домена в домені. Цей файл даних за замовчуванням перебуває в папці %SystemRoot%\NTDS. В ньому зберігається вся інформація каталогу, призначена для даного домена, а також дані, що є загальними для всіх контролерів домена в даній організації.

Друга копія файлу Ntds.dit знаходиться в папці %SystemRoot%\ System32. Ця версія файлу – копія (копія, задана за замовчуванням) бази даних каталогу, вона використовується для встановлення служби Active Directory. Цей файл копіюється на сервер під час встановлення Microsoft Windows Server 2003, щоб сервер можна було призначати контролером домена без необхідності звертатися до інсталяційного середовища. Під час виконання майстра інсталяції Active Directory (Dcpromo.exe) файл Ntds.dit копіюється з папки System32 у папку NTDS. Потім копія, збережена в папці NTDS, стає діючою копією сховища даних каталогу.

1.5 Планування структури корпоративної мережі

1.5.1 Етапи планування структури корпоративної мережі

Планування структури корпоративної мережі зводиться до побудови проекту структури доменів.

Для того щоб прийняти рішення щодо структури доменів необхідно, вивчивши фізичну структуру корпоративної мережі, вибрати кореневий домен лісу, визначитися з кількістю доменів і систематизувати їх у рамках ієрархічної системи на основі створення декількох доменів, дерев, лісів, тобто вибрати модель організації Active Directory, призначити імена доменам.

Фізична структура корпоративної мережі складається з наступних елементів:

– місце розташування пунктів мережі;

– кількість користувачів у кожному з пунктів;

– типи мережі, застосовувані в кожному з місць розташування;

– швидкість передачі даних по каналах і корисна пропускна здатність (у відсотковому відношенні) віддалених мережевих каналів.

– підмережі TCP/IP у кожному місці розташування;

– швидкість передачі даних по локальних мережевих каналах;

– місце розташування контролерів домена;

– розміщення серверів у кожному місці розташування та служби, що виконуються на них;

– розміщення брандмауерів у мережі.

1.5.2 Спеціалізований кореневий домен лісу

Оскільки домени Active Directory організовані в ієрархічному порядку, перший домен на підприємстві стає кореневим доменом лісу, він називається кореневим доменом або доменом лісу. Кореневий домен є відправною точкою для простору імен Active Directory.

Перший домен може бути призначеним (dedicated), його ще називають спеціалізованим або непризначеним (non-dedicated) кореневим доменом.

Спеціалізований кореневий домен є пустим доменом-замінником, призначеним для запуску Active Directory. Цей домен не буде містити ніяких реальних облікових записів користувачів (груп) і використовуватися для призначення доступу до ресурсів, тобто його функції обмежуються адмініструванням інфраструктури лісу. Єдині облікові записи, які присутні в спеціалізованому кореневому домені - це облікові записи користувачів і груп, заданих по замовчуванню, таких як обліковий запис Administrator (Адміністратор) і глобальна група Domain Admins (Адміністратори домена).

Непризначений кореневий домен - це домен, у якому створюються облікові записи фактичних користувачів і груп.

Інші домени на підприємстві існують або як рівні по положенню (peers) стосовно кореневого домену, або як дочірні домени. Рівні по положенню домени перебувають на том ж ієрархічному рівні, що й кореневий домен.

Процес розміщення структури доменів, як правило, починається із призначення спеціалізованого кореневого домена лісу.

Нижче перераховані аргументи «за» призначення спеціалізованого кореневого домена лісу.

– Він дозволяє контролювати чисельність адміністраторів, яким дозволено вносити зміни в масштабі всього лісу. Обмеження чисельності адміністраторів у кореневому домені лісу, в свою чергу, знижує ймовірність адміністративних помилок, що впливають на поведінку лісу в цілому.

– З'являється можливість реплікації даних з кореневого домена на будь-які сайти підприємства. Компактність спеціалізованого кореневого домена спрощує його реплікацію з метою захисту від непередбачених обставин.

– Спеціалізований кореневий домен лісу ніколи не застаріває, оскільки інших функцій він не виконує.

– Передавати володіння кореневим доменом досить зручно. Більше того передача повноважень володіння ним не тягне за собою перенесення виробничих даних і ресурсів.

Спеціалізований кореневий домен лісу служить для керування інфраструктурами, тому не рекомендується зв'язувати користувачів і ресурси, що не мають відношення до адміністрування лісу, з кореневим доменом. Необхідність виділення кореневого домена, призначеного винятково для адміністративних цілей, повинна бути передбачена вже на стадії планування домена.

1.5.3. Моделі побудови доменної структури

Вивчивши фізичну структуру компанії та передбачивши в плані спеціалізований кореневий домен лісу, можна починати планування структури доменів.

При цьому, насамперед, необхідно вирішити, скільки доменів доречно створити в поточних умовах. Іншими словами необхідно вибрати модель організації доменів. Розглядаючи поняття логічної структури Active Directory були представлені такі поняття як домен, дерево та ліс. На основі цих компонентів стає можливим організувати такі моделі побудови доменної структури як:

- однодоменна модель;
- модель із декількома доменами в складі одного дерева;
- модель із декількома деревами в складі одного лісу;
- модель із декількома лісами.

Далі розглянемо основні характеристики кожної моделі, а також основні причини та наслідки її створення.

Однодоменна модель організації корпоративної мережі.

Однодоменна модель організації припускає наявність одного домена в мережі. Схематично така модель представлена на рисунку 1.4

Рис. 1.4 – Однодоменна модель.

Нижче наведені деякі причини створення одного домена в компанії:

– розмір організації такий, що може керуватися одним доменом (рекомендується менш 1-2 мільйонів користувачів);

– використовується централізована структура керування мережею з добре деталізованою політикою;

– припустимо застосування єдиної політики безпеки (паролі, блокування облікових записів, Kerberos, файлова система із шифруванням, IPSecurity, інфраструктура відкритих ключів);

– географічна розподіленість така, при якій відсутні неякісні або перевантажені канали між окремими ділянками;

– підприємство стабільно та не планується його розділення на декілька нових або злиття з іншим підприємством;

– немає потреби у використанні більше одного доменного імені.

Таким чином, ліс підприємства буде складатися з одного дерева, у якому є тільки один домен. Він же є коренем всього лісу та носієм імені.

Переваги однодоменної моделі Active Directory наступні:

– Простота керування. Всі адміністратори зосереджені в одному місці, мають чітку спеціалізацію. Не потрібно делегувати (навіть тимчасово) надлишкові адміністративні повноваження додатковим адміністраторам.

– Таке рішення є дешевшим. Для підтримки працездатності одного домена потрібно менше контролерів домена.

– Простота розподілу повноважень. Повноваження адміністраторів розподіляються по ОП всередині одного домена, а не між декількома.

– Менше число адміністраторів. Для керування декількома доменами, особливо розкиданими географічно, потрібно більше адміністраторів, а звідси витікають додаткові витрати на їх навчання та утримання.

– Гранична ємність така ж, як у цілого лісу доменів. Глобальний каталог може зберігати не більше 4 мільярдів об'єктів. З іншого боку, він містить короткі відомості про всі об'єкти в лісі незалежно від кількості доменів у лісі. Виходить, і для одного домена, і для декількох ця межа незмінна.

Модель із декількома доменами в складі одного дерева

Чим більше організація, тим вище ймовірність того, що буде потрібним введення додаткових доменів. Найбільш часто при цьому реалізується така логічна структура служби каталогів як дерево. Приклад реалізації такої структури наведений на рисунку 1.5

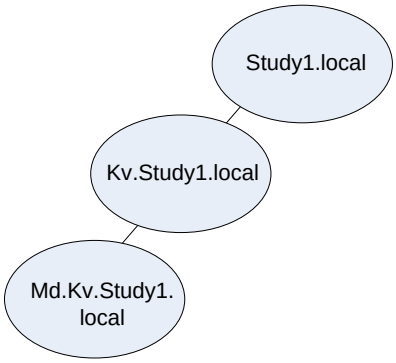

Рис. 1.5 – Модель із декількома доменами в складі одного дерева.

Перш ніж включати в структуру Active Directory нові домени, необхідно, по-перше, чітко визначитися з тим, навіщо це потрібно, а, по-друге, розрахувати пов'язані із цією операцією адміністративні витрати та вартість апаратних засобів.

Підстави для введення додаткових доменів наступні:

– дотримання вимог по безпеці;
– задоволення адміністративних вимог;
– оптимізація трафіка реплікації;
– збереження доменів Microsoft Windows NT.

Розглянемо більш докладно наведені вище причини.

Створення доменів для відповідності вимогам по безпеці

Настроювання в підкаталозі Account Policies (Політики облікових записів) вузла Security Settings (Параметри безпеки) об'єкта групової політики (Group Policy Object, GPO) задаються винятково на рівні домена. Якщо вимоги по безпеці, які встановлюються в підкаталозі Account Policies (Політики облікових записів), в масштабах компанії виявляються неоднорідними, їх потрібно рознести по окремим доменам. В підкаталозі Account Policies (Політики облікових записів) містяться наступні політики.

– Політика паролів. Містить настроювання паролів, пов'язані з їх історією, термінами дії, довжиною, складністю та зберіганням.

– Політика блокування облікових записів. Містить настроювання блокування облікових записів, що регламентують тривалість, поріг та звітність.

– Політика Kerberos. Містить настроювання протоколу Kerberos, пов’язані з обмеженнями на реєстрацію, термінами дії квитків користувачів і служб, а також обов'язковістю.

Докладніше про групові політики а також про політики безпеки в Active Directory буде розказано нижче.

Створення доменів для дотримання адміністративних вимог

У деяких компаніях до мережевої інфраструктури виставляються дуже серйозні адміністративні вимоги, які неможливо задовольнити шляхом введення в домен додаткових підрозділів. Ці вимоги, як правило, пов'язані із правовими нюансами та питаннями конфіденційності. Приміром, може статися, що зовнішні адміністратори отримають повноваження керування конфіденційними файлам якого-небудь проекту, що є небажаним. Ця вимога суперечить умовам, які виникають при наявності єдиного домена, коли всі члени глобальної групи Domain Admins (Адміністратори домена) одержують необмежені повноваження керування всіма об'єктами в межах домена — включаючи будь-які конфіденційні файли. Якщо ж розмістити файли (разом з розробниками) в окремому домені, вони виявляться за межами компетенції членів описаної вище групи Domain Admins (Адміністратори домена), і вимога буде задоволена.

Створення доменів з метою оптимізації трафіка реплікації

В тих компаніях, де мережева інфраструктура складається з декількох сайтів, встає проблема передачі по міжсайтових каналах трафіка реплікації в межах одного домена. В лісі з одним доменом всі об'єкти реплікуються по всіх контролерах. Якщо об'єкти реплікуються серед систем, в яких їм не має застосування, значить має місце неефективне споживання пропускної здатності. За рахунок створення декількох компактних доменів і настроювання реплікації об'єктів тільки серед тих систем, де вони потрібні, можна скоротити трафік реплікації та оптимізувати цей процес. Але вигоди, які можна одержати від оптимізації, необхідно попередньо співставити з адміністративними витратами та вартістю апаратного забезпечений при введенні додаткових доменів.

Перед ухваленням рішення про створення додаткових доменів з метою оптимізації трафіка реплікації потрібно врахувати наступні фактори.

– Пропускна здатність і готовність каналу. Якщо пропускна здатність розглянутого каналу наближається до максимуму або в певні періоди він стає недоступним, то, цілком ймовірно, що цей канал не підготовлений до передачі трафіка реплікації, в результаті чого потрібно буде створити додатковий домен. З іншого боку, якщо із пропускною здатністю все в порядку і канал регулярно простоює, можна запланувати реплікацію на періоди простою, і необхідність у введенні нового домена відпаде.

– Конкуренція трафіка реплікації із трафіком інших видів. Якщо через розглянутий канал проходить трафік більшої значимості, чим трафік реплікації, щоб виключити конкуренцію різних видів трафіка потрібно створити новий домен.

– Оплата каналів відповідно до навантаження. Якщо трафік реплікації доводиться пускати по дорогих каналах, які оплачуються відповідно до навантаження, потрібно завести новий домен.

– Обмеженість каналів протоколом SMTP. Якщо система з'єднана з іншими системами за допомогою каналів, передача даних через які проходить тільки по протоколу SMTP, для цієї системи необхідно створити окремий домен, тому що реплікація по протоколу SMTP можлива тільки між доменами, але не між контролерами в межах одного домену.

Створення нових доменів з метою збереження успадкованих доменів Windows NT

Компанії, що володіють великими інфраструктурами Windows NT, прагнуть зберегти існуючі домени Windows NT. Домени Windows NT можна обновити до Windows Server 2003 (цю операцію іноді називають заміщаючим відновленням). Необхідно зпівставити витрати, пов'язані з модернізацією або об'єднанням доменів Windows NT, і вигоду від супроводу та адміністрування меншої кількості доменів. Перед оновленням до Windows Server 2003 рекомендується об'єднати домени Windows NT і в такий спосіб скоротити їх чисельність.

Наслідки створення декількох доменів

Введення кожного нового домена призводить до підвищення адміністративних витрат і вартості апаратного забезпечення. Перед ухваленням рішення про створення додаткових доменів необхідно врахувати наступні фактори.

– Адміністратори. Разом з кожним новим доменом з'являється нова визначена глобальна група Domain Admins (Адміністратори домена), тому потрібно потратити більше зусиль на відстеження дій членів цієї групи.

– Учасники безпеки. Із введенням нових доменів підвищується ймовірність переміщення між ними учасників безпеки. На відміну від операції переміщення учасників безпеки між підрозділами одного домена, що не являє особливої складності, переносити їх з одного домена в інший набагато складніше.

Примітка. Учасниками безпеки (security principals) називаються користувачі, групи, комп'ютери та служби, яким призначені унікальні ідентифікатори безпеки (security identifiers, SIDs). Докладніше про учасників безпеки буде викладено в підрозділі 2.2.

– Групові політики та керування доступом. Групові політики та повноваження керування доступом задаються на рівні домена. Таким чином, навіть єдина для всієї компанії групова політика і єдині принципи делегування адміністративних повноважень повинні індивідуально визначатися для кожного домена.

– Апаратне забезпечення та фізичні засоби захисту контролерів доменів. Для того, щоб реалізувати в рамках домена Windows Server 2003 відмовостійкість і задовольнити вимоги по реплікації з декількома хазяїнами, у ньому повинно бути не менше двох контролерів. Крім того, рекомендується розміщувати контролери домена в захищених приміщеннях з обмеженим доступом.

– Надійні канали. Для того, щоб користувач із одного домена міг зареєструватися в іншому домені, необхідно мати можливість організації з'єднання між їхніми контролерами. Відповідно, збій каналу між доменами призводить до припинення обслуговування. Вирішити цю проблему допомагає збільшення чисельності надійних каналів. Однак останнє пов’язано з підвищенням витрат на встановлення та супровід.

Модель із декількома деревами в складі одного лісу.

Обговорюючи причини створення декількох доменів, мається на увазі, що мова йде про дерево, в якому всі дочірні домени успадковують ім'я кореневого. Однак таке не завжди прийнятно. Часто організація складається з ряду асоційованих з нею підприємств. Кожне таке підприємство займається незалежним бізнесом, має своє керівництво і політику. Можливо також, що ім'я цього підприємства відомо широкому колу осіб і не пов’язано з головною організацією.

З іншого боку, вимога єдиної адресної книги, заснованої на Active Directory, говорить про те, що це повинен бути єдиний ліс. Саме в цьому випадку резонно створити окреме дерево для кожної з таких компаній. У цього дерева буде своє унікальне в рамках лісу ім'я, але конфігурація та схема будуть загальними. Крім того, вони зможуть звертатися до єдиного глобального каталогу і здійснювати доступ до всіх наданих їм ресурсів. Приклад організації такої моделі наведений на рисунку 1.6.

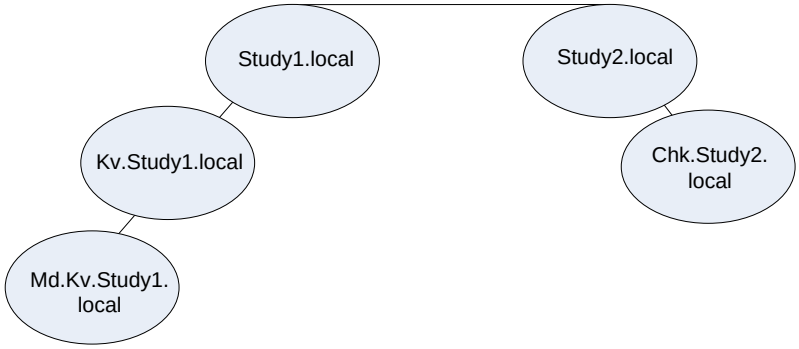

Рисунок 1.6 – Модель із декількома деревами в складі одного лісу

В ситуації, коли користувачам з одного дерева в лісі потрібно звернутися до ресурсів, розміщених у домені іншого дерева, автентифікація доступу буде виконуватися не прямо, а по ланцюжку, шляхом перебору всіх доменів від вихідного до кореневого, а потім від кореневого - до домену призначення. Якщо необхідність у такому доступі існує регулярно, то варто організувати скорочення - довірчі відносини, що зв'язують ці два домена прямо.

Переваги моделі Active Directory з декількома деревами наступні.

– Можливість використовувати різні простори імен. Ім'я кожного дерева унікально в рамках лісу.

– Децентралізоване керування. Асоційовані підприємства ряду компаній мають незалежність як юридичні особи і мають власні IT-служби.

– Простота включення нових асоційованих підприємств. Якщо компанія придбає фірму з технічним персоналом, своїми правилами безпеки та ін., то структура з декількома деревами дозволяє створити для неї дерево відповідно до її вимог.

– Використання єдиної схеми та глобального каталогу. Незважаючи на різницю, організації, що входять у різні дерева, використовують єдині додатки, інтегровані з Active Directory, і єдину адресну книгу (наприклад, в Microsoft Exchange 2000).

Переваги моделі з одним лісом

Розглянуті вище моделі побудови доменної структури відносяться до так званої моделі Active Directory з одним лісом доменів. В 99% випадків варто дотримуватися саме цієї моделі.

Нижче перераховані основні переваги цієї моделі.

– Ліс характеризується наявністю єдиного глобального каталогу. Це означає, що для створення єдиної адресної книги не треба застосовувати ніяких додаткових зусиль.

– Наявність єдиного глобального каталогу також може бути використано різними серверами додатків такими, наприклад, як IBM Web Sphere. Вони можуть звернутися до глобального каталогу для авторизації користувачів. Це може стати першим кроком на шляху до створення єдиної точки входу в гетерогенну систему (single sign-on).

– Одною з найважливіших переваг єдиного лісу є простота та ефективність впровадження єдиної політики безпеки. Пов'язано це як з організаційними, так і з технічними причинами. Керування всім лісом виконується єдиною командою IT, тому одна і та ж політика не може бути впроваджена по-різному тими самими людьми. Високий рівень кваліфікації співробітників забезпечує її правильне впровадження та підтримку. Технічна єдність політик забезпечується тим, що, незважаючи на різні домени, до них застосовується той самий об'єкт групової політики, збережений в Active Directory. Крім того, цей об’єкт можна захистити від несанкціонованого доступу засобами AD.

– В рамках єдиної політики безпеки легко реалізується концепція делегування повноважень. Делегування дозволяє, з одного боку, різко скоротити число співробітників, що володіють адміністративними повноваженнями, а з іншого боку - централізовано контролювати зону відповідальності кожного із сервісних адміністраторів. У такій ситуації особи, що не мають достатньої кваліфікації, не зможуть отримати доступ до функцій, що впливають на стабільність і безпеку всієї системи.

– Наявність єдиного лісу дозволяє централізовано впровадити систему моніторингу, що буде в реальному масштабі часу стежити за контролерами доменів

і іншим обладнанням. Причому, наприклад, така система, як Microsoft Operations Manager (MOM 2000), дозволить не тільки контролювати стан систем, що обслуговуються, і вчасно повідомляти оператора про всі збої, але й автоматично відпрацьовувати процедури по усуненню несправностей.

– Наявність єдиного лісу Active Directory значно спрощує процес впровадження корпоративних стандартів на робочі місця користувачів. Використання групових політик у рамках лісу дозволяє управляти додатками, встановленими на настільних і мобільних комп'ютерах, виконувати своєчасне їхнє відновлення, застосовувати певні настроювання окремих додатків, що регулюють доступ до ресурсів, централізовано управляти сценаріями реєстрації та ін. Так, наприклад, групова політика може для всіх користувачів визначити розташування сервера Software Update Service (SUS) у корпоративній мережі підприємства, що використовується для поширення виправлень для операційної системи та пов'язаних з нею додатків.

– Одним із завдань, що стоять перед організаціями, робота яких не повинна перериватися при будь-яких обставинах (катастрофи, дії терористів і т.п.), є організація резервного центра керування. Резерв може бути як «гарячим», так і «холодним». У випадку, коли є єдиний ліс Active Directory, інфраструктура каталогу може бути спроектована таким чином, що навіть у випадку повного знищення центральної частини організації та частина, що залишилася, буде продовжувати працювати без перерв і втрати функціональності. Більше того, співробітники центральної частини, що переїхали в будь-яке місце в структурі підприємства, зможуть негайно приступитися до роботи, зберігши при цьому доступ до всіх необхідних додатків.

Модель із декількома лісами

Оскільки для всіх доменів лісу є ряд загальних елементів, таких як схема, контейнер конфігурацій і глобальний каталог, і, крім того, домени всередині такого лісу пов'язані двосторонніми транзитивними довірчими відносинами, одного лісу в компанії цілком достатньо.

Вводити декілька лісів треба тільки при необхідності об'єднання інфраструктур двох або декількох організацій, інакше кажучи, при злитті, поглинанні або вибудовуванні партнерських відносин з іншою компанією. Введення додаткових лісів тягне за собою істотне підвищення адміністративних витрат і зниження зручності використання, тому у більшості випадків заводити в компанії більше одного лісу не рекомендується.

Завдання, що виступають підставами для створення додаткових лісів, перераховані нижче.

– Захист даних. Доступ до уразливих даних можна обмежити рамками лісу. Це актуально в умовах роздільного ведення даних підрозділів, а також при необхідності ізолювати схему, контейнер конфігурацій або глобальний каталог.

– Ізольована реплікація каталогу. Зміни схеми та конфігурації при наявності декількох лісів впливають тільки на один із цих лісів.

– Виділення середовища розробки моделювання лабораторних умов. Шляхом створення додаткових лісів можна відокремити від інших частин інфраструктури дослідні або тестові середовища. Так, якщо потрібно жорстко відокремити один від одного підрозділи компанії або обмежити повноваження доступу до ресурсів окремих користувачів, але шляхом реструктуризації доменів або підрозділів вирішити це завдання не можливо, можна створювати додаткові ліси – це досить ефективний метод забезпечення конфіденційності та захисту.

При створенні кожного нового лісу помітно підвищуються адміністративні витрати та вартість апаратних засобів. Ухвалюючи рішення щодо створення структури з декількох лісів, необхідно мати на увазі наступні фактори.

– Схема. У кожного лісу власна схема. Навіть якщо схеми схожі один на одну, супроводження її даних і членства в адміністративних групах здійснюється для кожної окремо.

– Контейнер конфігурацій. У кожного лісу власний контейнер конфігурацій. Супровід даних і членства в адміністративних групах для кожного з контейнерів проводиться окремо - навіть якщо контейнери схожі між собою.

– Довірчі відносини. Між кореневими доменами двох різних лісів можуть встановлюватися односторонні або двосторонні довірчі відносини. Настроюються та супроводжуються вони явно і вручну. В результаті всі домени одного лісу входять у транзитивні довірчі відносини з доменами іншого лісу. При цьому необхідно мати на увазі, що в ланцюжку із трьох і більше лісів транзитивність міжлісових відносин втрачається.

– Реплікація. Реплікація об'єктів між лісами проводиться вручну на основі індивідуальних адміністративних політик і процедур.

– Злиття лісів або переміщення доменів. Злиття лісів - це операція, що включає в себе клонування учасників безпеки, переміщення об'єктів і пониження контролерів домена до статусу рядових серверів з наступним перепризначенням у рамках нового лісу.

– Переміщення об'єктів. При переміщенні об'єктів з одного лісу в інший необхідно використовувати утиліту ClonePrincipal, що допомагає клонувати учасників безпеки та переносити копії в новий ліс, а також команду Ldifde.exe, призначену для переміщення всіх інших об'єктів.

– Реєстрація по смарт-картах. Для забезпечення можливості реєстрації в різних лісах по смарт-картах необхідно ведення стандартних основних імен користувачів (user principal names, UPNs).

– Додаткові домени. У кожному лісі повинен бути як мінімум один домен. Чим більше доменів, тим вище адміністративні витрати і вартість апаратного забезпечення.

– Реєстрація користувачів. При відсутності між двома лісами довірчих відносин в процесі реєстрації користувача з одного лісу на сервері, розміщеному в іншому лісі, йому доводиться вказувати складне стандартне ім'я UPN, що складається з повного шляху до домену облікового запису користувача. Необхідність введення стандартного UPN пов'язана з тим, що контролер домена в лісі призначення не зможе знайти у своєму глобальному каталозі просте ім'я UPN.

Просте ім'я UPN є присутнім тільки в тому глобальному каталозі, що відноситься до лісу, якому належить даний користувач.

– Запити користувачів. Під час відсутності довірчих відносин між лісами користувачів потрібно спеціально навчати складанню запитів, що діють у всіх лісах компанії. Велика кількість невірно складених або неповних запитів впливає на ефективність роботи користувачів.

Розглянувши можливі моделі побудови доменної структури корпоративної мережі можна зробити наступні висновки. Так, плануючи структуру доменів, при можливості, бажано обмежитися одним дочірнім доменом, а нові вводити тільки в умовах крайньої необхідності. В одному домені може бути кілька сайтів і мільйони об'єктів. Структури сайтів і доменів повинні бути, по-перше, автономні по відношенню один до одного, а, по-друге, гнучкі. З одного боку, один домен може поширюватися на кілька географічних місць розташування, а, з іншого, одному сайту можуть належати користувачі та комп'ютери із різних доменів.

Не варто прив'язувати структуру доменів до підрозділів і відділів компанії, оскільки ризик переформування функціональних структур, до яких відносяться підрозділи, відділи та проектні групи, досить великий. Для моделювання ієрархії управління в рамках кожного домена існують підрозділи (Organizational Units, OU) - вони допомагають вирішувати завдання, пов'язані з делегуванням і адмініструванням.

2 МЕТОДИ УДОСКОНАЛЕННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Механізм організації захисту служби каталогу Active Directory

Одною з основних причин розгортання служби каталогу Active Directory є забезпечення безпеки корпоративної мережі. Кожна компанія зберігає найважливішу для свого бізнесу інформацію на файлових серверах у мережі. Керування безпечним доступом до інформації повинно гарантувати, що доступ до даних одержать тільки належним чином уповноважені користувачі.

Система безпеки Active Directory складається з декількох елементів: групи безпеки, керування доступом, делегування адміністрування, групова політика.

Групи безпеки спрощують адміністрування, дозволяючи призначити права доступу для групи користувачів не залежно від того, які права має кожний обліковий запис користувача окремо. Керування доступом - це надання або відмова в правах доступу до ресурсів мережі. Делегування адміністрування - надання можливості іншим адміністраторам, групам або користувачам управляти функціями відповідно до їхніх власних потреб. Групова політика надає можливість настоювання аудиту, ведення журналу безпеки, параметрів аналізу та настроювання безпеки групової політики.

Далі розглянемо більш детально представлені складові системи безпеки служби каталогу. Але перед цим необхідно відзначити, що існують деякі основні концепції, які лежать в основі принципів захисту Active Directory в мережі Windows Server 2003.

Захист Active Directory будується на двох типах об'єктів та на взаємодії між ними. Перший об'єкт - учасник безпеки, який представляє користувача, групу, службу або комп'ютер, що має потребу в доступі до деякого ресурсу в мережі. Другий об'єкт - це сам ресурс, що є об'єктом, до якого потрібно одержати доступ учаснику безпеки. Щоб забезпечити належний рівень захисту, служба Active Directory повинна ідентифікувати учасників безпеки, а потім надавати правильний рівень доступу до ресурсів.

До кожного об'єкта Active Directory прив’язується дескриптор захисту, що регламентує коло осіб, які мають повноваження доступу до цього об'єкта, і визначає дозволені типи доступу, тобто забезпечує керування доступом до об'єктів.

Керування доступом до об'єктів Active Directory фактично зводиться до надання відповідних дозволів учасникам системи безпеки і їхнього відкликання.

2.2 Керування доступом

2.2.1 Поняття учасника безпеки

Учасниками системи безпеки, як було відзначено вище, є користувачі, групи, служби або комп'ютери, які мають потребу в доступі до деякого ресурсу в мережі.

Кожному учаснику системи безпеки присвоїно унікальний ідентифікатор захисту (security identifiers, SID), що ідентифікує користувача, групу, комп'ютер або службу в рамках підприємства та задіюється в процесі керування учасниками системи безпеки.

Всередині систем сімейства Windows NT ідентифікатор системи захисту представлений унікальним 48-розрядним числом. Такий підхід дозволяє системі розрізняти, наприклад, локальний обліковий запис Administrator комп'ютера A та одноіменний локальний обліковий запис Administrator комп'ютера B.

Ідентифікатор SID складається з декількох частин. Наприклад:

S-1-5-21-1507001333-1204550764-1011284298-500

– Перед ідентифікатором SID ставиться буква S, а його частини розділяються дефісами.

– Перше число (в цьому прикладі 1) – номер редакції.

– Друге – значення повноважень ідентифікатора (для Windows Server 2003 це завжди 5).

– Наступні чотири числа - значення повноважень (у розглянутому прикладі це 21 і три довгі послідовності цифр).

– Останнім вказується відносний ідентифікатор (RID - Relative Identifier) (в нашому прикладі його значення дорівнює 500).

Ідентифікатор SID має дві частини: одна його частина унікальна для домена або інсталяції в цілому, а інша - будується на підставі загальних правил і умов для всіх доменів і інсталяцій (відносний ідентифікатор RID) – і є унікальною для кожного учасника безпеки. Після установки Windows Server 2003 локальний комп'ютер випадково вибирає SID. Те ж саме відбувається і при створенні домена під Windows Server 2003 - він також одержує унікальний ідентифікатор SID. Таким чином, для будь-якого комп'ютера або домена під керуванням Windows Server 2003 значення повноважень завжди будуть унікальними

Правила, що встановлюють значення RID є постійним для всіх комп'ютерів і доменів. Наприклад, ідентифікатор SID, у якого значення RID дорівнює 500, завжди належить обліковому запису Administrator локальної машини.

RID 501 використовується для облікового запису Guest.

RID для домена починається зі значення 1001 і показує кількість облікових записів користувачів (наприклад, RID 1015 одержить п'ятнадцятий користувач домена).

Досить сказати, що перейменування облікового запису ніяк не впливає на відповідний їй SID, тому обліковий запис завжди буде ідентифікований. Перейменувавши обліковий запис Administrator, можна лише змінити його ім'я, система Windows Server 2003 (або зловмисник, що використовує спеціальні засоби) завжди визначить його за значенням RID 500. Однак, якщо об'єкт користувача вилучений, а потім створений заново з тим же самим ім'ям, користувач не зможе звертатися до ресурсів, тому що SID зміниться.

2.2.2 Дозволи

Дозволом називається право виконання стосовно об'єкта конкретної операції або набору операцій. Призначаються дозволи власниками об'єктів, а в коло обов'язків адміністратора входить керування дозволами на операції з учасниками системи безпеки. Призначення дозволів можливо тільки стосовно даних, розмішених на дисках NTFS.

Список дозволів на доступ користувачів до кожного об'єкта Active Directory в Windows Server 2003 зберігається в так званому списку керування доступом (access control list, ACL). Список керування доступом зберігається в атрибуті NT Security Descriptor, що складається з одного або більше записів керування доступом (ACI), вони визначають, які права на даний об'єкт має кожний ідентифікатор SID. Дескриптор захисту містить власника об'єкта, а також список керування розмежувальним доступом (DACL) і список керування системним доступом (SACL). Список DACL визначає дозволи на об'єкт, які мають всі учасники безпеки. Список SACL визначає параметри настроювання аудита об'єкта.

Отже, в ACL об'єкта перераховані всі особи, що володіють повноваженнями доступу до нього, і вказані операції, відкриті для кожного з них. Рівень контролю доступу до об'єктів різних типів в Windows Server 2003 досить високий. Для того, щоб наділити того або іншого учасника системи безпеки повноваженнями доступу до конкретного об'єкта, його потрібно ввести в ACL цього об'єкта. Тільки після цього задаються конкретні операції, які даний учасник системи безпеки може виконувати відносно розглянутого об'єкта.

Будь-які дозволи можуть бути виставлені в одному із двох значень: Allow – дозволити або Deny – заборонити. При забороні звертання до об'єкта тому або іншому користувачу не допоможе навіть членство в групі, для якої аналогічна операція дозволена. Конкретний перелік дозволів на доступ до об'єкта визначається його типом. Приміром, дозвіл Reset Password (Сброс пароля) - скидання пароля об'єкта користувача можна надати учасникові системи безпеки, але не можна – принтеру. Кожному типу об'єкта відповідає, по-перше, група стандартних дозволів, а, по-друге, група більш деталізованих спеціальних дозволів.

Стандартні дозволи призначаються найчастіше. Список стандартних дозволів, що відповідають тому або іншому об'єкту, можна переглянути на вкладці Security (Безпека) його діалогового вікна властивостей. У таблиці 2.1 представлені стандартні дозволи на доступ до об'єктів, а в таблиці 2.2 представлені дозволи на доступ до файлів і папок.

Таблиця 2.1 Стандартні дозволи на доступ до об'єктів.

Назва Дозволу	Можливості, що надаються
Read (Читання)	с цим дозволом користувач може: - бачити імена файлів і папок; - мати доступ до підпапок загального ресурсу; - читати дані та атрибути файлів; запускати на виконання програми.

Продовження таблиці 2.1 Стандартні дозволи на доступ до об'єктів.

Change (редагування)	користувачам дозволено читати дані з папки, а також: - створювати файли і підпапки; - змінювати файли; - змінювати атрибути файлів і підпапок; - видаляти файли й підпапки.
Full Control (Повний доступ)	користувачам дозволено читати дані з папки, а також: - створювати файли і підпапки; - змінювати файли; - змінювати атрибути файлів і підпапок; - видаляти файли й підпапки.

Таблиця 2.2 Дозволи файлів і папок

Назва Дозволу	Можливості, що надаються для файлів	Можливості, що надаються для папок
Read (Читання)	Перегляд списку файлів і підпапок	Перегляд і копіювання вмісту файлу

Write (Запис)	Добавлення файлів і підпапок	Запис у файл
Read & Execute (Читання і виконання)	Перегляд списку файлів і підпапок, а також виконання файлів (успадковується файлами і папками)	Перегляд і копіювання вмісту файлу, а також виконання файлу
List Folder Contents (Список вмісту папки)	Перегляд списку файлів і підпапок, а також виконання файлів (успадкову-ється тільки папками)	
Modify (Змінити)	Читання і запис файлів і підпапок, видалення папки	Читання, запис і видалення файлу
Full Control (Повний доступ)	Читання, запис, зміна і видалення файлів і підпапок	Читання, запис, зміна і видалення файлу

Стандартні дозволи розширюються за рахунок спеціальних дозволів, які надають підвищений рівень контролю над призначенням повноважень доступу.

В таблиці 2.3 приведені спеціальні дозволи, що використовуються при створенні базових дозволів для файлів, а в таблиці 2.4 приведені спеціальні дозволи, що використовуються при створенні базових дозволів для папок.

Таблиця 2.3 Спеціальні дозволи, що використовуються при створенні базових дозволів для файлів

	Основні дозволи

Спеціальні дозволи	Full Control (Повний доступ)	Modify (Змінити)	Read Execute (Читання и виконання)	Read (Читання)	Write (Запис)
Traverse Folder/Execute File (Огляд папок/Виконання файлів)	Так	Так	Так	Ні	Ні
List Folder/Read Data (Зміст папки/ Читання даних)	Так	Так	Так	Так	Ні
Read Attributes (Читання атрибутів)	Так	Так	Так	Так	Ні
Read Extended Attributes (Читання додаткових атрибутів)	Так	Так	Так	Так	Ні
Create Files/ Write Data (Створення файлів/Запис даних)	Так	Так	Ні	Ні	Так

Create Folders/ Append Data (Створення папок/Допис даних)	Так	Так	Ні	Ні	Так
Write Attributes (Запис атрибутів)	Так	Так	Ні	Ні	Так
Write Extended Attributes (Запис додаткових атрибутів)	Так	Так	Ні	Ні	Так

Продовження таблиці 2.3 Спеціальні дозволи, що використовуються при створенні базових дозволів для файлів

Delete Subfolders and Files (Видалення підпапок й файлів)	Так	Ні	Ні	Ні	Ні
Delete (Видалення)	Так	Так	Ні	Ні	Ні
Read Permissions (Читання дозволів)	Так	Так	Так	Так	Так
Change Permissions (Редагування дозволів)	Так	Ні	Ні	Ні	Ні
Take Ownership (Зміна власника)	Так	Ні	Ні	Ні	Ні

Таблиця 2.4 Спеціальні дозволи, що використовуються при створенні базових дозволів для папок

Спеціальні дозволи		Основні дозволи				
	Full Control (Повний доступ)	Modify (Змінити)	Read Execute (Читання и	List Folder Contents (Список	Read (Читання)	Write (Запис)

			виконанн я)	вмісту папки)		
Traverse Folder/Execute File (Огляд папок/Виконан ня файлів)	Так	Так	Так	Так	Ні	Ні
List Folder/Read Data (Зміст папки/ Читання даних)	Та к	Та к	Так	Та к	Ні	Н і
Read Attributes (Читання атрибутів)	Та к	Та к	Так	Та к	Та к	Н і

Продовження таблиці 2.4 Спеціальні дозволи, що використовуються при створенні базових дозволів для папок

Read Extended Attributes (Читання додаткових атрибутів)	Так	Так	Так	Так	Так	Ні
Create Files/ Write Data (Створення файлів/Запис даних)	Так	Так	Ні	Ні	Ні	Так
Create Folders/ Append Data (Створення папок/Допис даних)	Так	Так	Ні	Ні	Ні	Так
Write Attributes (Запис атрибутів)	Так	Так	Ні	Ні	Ні	Так
Write Extended Attributes (Запис	Так	Так	Ні	Ні	Ні	Так

додаткових атрибутів)						
Delete Subfolders and Files (Видалення підпапок й файлів)	Так	Ні	Ні	Ні	Ні	Ні
Delete (Видалення)	Так	Так	Ні	Ні	Ні	Ні
Read Permissions (Читання дозволів)	Так	Так	Так	Так	Так	Так
Change Permissions (Редагування дозволів)	Так	Ні	Ні	Ні	Ні	Ні
Take Ownership (Зміна власника)	Так	Ні	Ні	Ні	Ні	Ні

2.2.3 Володіння об'єктами

Користувач, що створив об'єкт, автоматично стає його власником. Право володіння більшістю об'єктів Active Directory і об'єктів мережевих серверів належить адміністраторам. Користувачі ж створюють і володіють всіма файлами даних у своїх домашніх каталогах і деякими файлами даних на мережевих серверах. Власник об'єкта контролює механізм призначення дозволів на звернення до цього

об'єкта та встановлює коло осіб, яким ці дозволи доступні. Об'єкти передаються у володіння:

– адміністраторам [за замовчуванням, членам групи Administrate (Администраторы) передається право користувачів Take Ownership Of Files Or Other Objects (Заволодіння файлами або іншими об’єктами)]. При цьому адміністратор може прийняти володіння будь-яким файлом, розміщеним на підвідомчому комп'ютері, але він не може передавати повноваження володіння третім особам;

– користувачам або групам, яким призначений дозвіл стати власником конкретних об'єктів - Take Ownership (Стати володарем). В результаті останній може в будь-який момент прийняти володіння на себе, і лише після цього операція передачі буде вважатися завершеною;

– користувачам, у яких є права відновлення файлів і каталогів - Restore Files And Directories (Відновлення файлів і каталогів). В результаті користувач, що володіє правом відновлення файлів і каталогів, може передавати володіння будь-яким стороннім користувачам і групам.

В Windows Server 2003 Active Directory є можливість встановлення квот на кількість об'єктів розділу каталогу, які можуть перебувати у володінні одного учасника системи безпеки (користувача, групи або комп'ютера). Квоти Active Directory запобігають відмові від обслуговування в результаті нестачі дискового простору на контролерах домена — ситуації, що, в свою чергу, зумовлена надмірним збільшенням кількості об'єктів, створених одним учасником системи безпеки. Квоти не поширюються на всіх, за виключенням членів груп, в які входять адміністратори домена - Domain Administrators (Адміністратори домена) та адміністратори підприємства - Enterprise Administrators (Адміністратори підприємства). У деяких випадках на одного учасника системи безпеки поширюється відразу кілька квот - наприклад, квота, встановлена для нього особисто, і квота, встановлена для групи, до якої він належить. В таких випадках діє найбільша квота.

Якщо учасник системи безпеки виявляється поза областю дії прямої квоти, на нього поширюється стандартна квота, встановлена для його розділу. Якщо ж і така відсутня, то будь-які обмеження в межах даного розділу знімаються. Для того, щоб квоти в рамках розділу каталога домена діяли, всі контролери даного домена повинні працювати під керуванням операційної системи Windows Server 2003. Для активізації квот у межах розділу конфігурації всі домени в рамках лісу повинні працювати під керуванням Windows Server 2003. Квоти щодо розділів схеми не встановлюються.

2.2.4 Вплив членства в групах на керування доступом

Будь-який учасник системи безпеки може бути членом декількох груп, кожна з яких характеризується різними наборами дозволів і рівнями доступу до об'єктів. Конкретний набір дозволів учасника системи безпеки складається з дозволів на доступ до конкретних об'єктів і дозволів, що поширюються на нього за допомогою членства в групах. Приміром, якщо особисто користувачеві призначений дозвіл Read (Читання), а для групи, в якій він перебуває, встановлений дозвіл Write (Запис), в його розпорядженні перебуває обидва дозволи. При призначенні дозволів групам необхідно враховувати, на яких користувачів вони будуть поширені.

Групи та користувачі, що мають дозвіл Full Control (Повний доступ) щодо папки, мають право видаляти будь-які розміщені в ній файли і підпапки незалежно від дозволів, встановлених для їхнього захисту.

2.2.5 Вплив наслідування на керування доступом

Існує два способи встановлення дозволів на доступ до об'єкта: явне призначення та наслідування.

Явні дозволи встановлюються безпосередньо стосовно об'єкта його власником.

Дозволи, одержувані шляхом наслідування, передаються батьківськими об'єктами дочірнім. Можливість наслідування дозволів значно спрощує завдання керування і забезпечує несуперечність дозволів в рамках контейнера.

Наприклад, якщо, члени групи Management мають у своєму розпорядженні дозвіл Full Control щодо папки Library, він поширюється на дочірні об'єкти: підпапки Shop і Marketing, а також їх власні дочірні об'єкти, якими є папка Sport_shop. При цьому дозволи, призначені групі Management щодо папки Library, вважаються явними, а дозволи, отримані цією групою щодо інших підпапок — успадкованими.

Вся сукупність дозволів щодо розглянутого об'єкта, якими володіє учасник системи безпеки називається фактичними дозволами. Фактичні дозволи - це набір, в який входять, крім особистих, дозволи, отримані за рахунок членства в групах і успадковані від батьківських об'єктів.

2.3 Делегування адміністративних повноважень

Як було розглянуто вище служба Active Directory забезпечує ієрархічне представлення каталога, спочатку через ієрархію доменної системи імен (DNS) множини доменів, а потім через структуру організаційних підрозділів (OU) в межах доменів. Ця ієрархія створює важливу адміністративну можливість: делегування адміністративних повноважень.

Делегуванням повноважень адміністративного керування доменами, підрозділами, контейнерами називається процес передачі іншим адміністраторам, користувачам або групам можливості керування об'єктами, включеними в ці домени, підрозділи і контейнери.

Делегувати повноваження адміністративного керування потрібно для того, щоб інші адміністратори, групи і користувачі могли розпоряджатися функціями цих об'єктів у відповідності зі своїми завданнями. У невеликих компаніях за керування об'єктами Active Directory, як правило, відповідає невелика кількість адміністраторів. У великих організаціях з великою кількістю доменів, підрозділів і контейнерів адміністраторів набагато більше, іноді навіть спеціальні адміністратори призначаються для керування окремими об'єктами в рамках підрозділів і контейнерів.

Для делегування адміністративних дозволів можна прямо звертатися до списків ACL індивідуальних об'єктів. Оскільки всі об'єкти в Active Directory мають ACL-список, існує можливість управляти адміністративним доступом до будь-якої властивості будь-якого об'єкта. А це, в свою чергу, означає, що можна надавати іншим адміністраторам Active Directory досить точні дозволи, щоб вони могли виконувати тільки делеговані їм завдання.

Для автоматизації і спрощення процесу встановлення адміністративних повноважень відносно доменів і підрозділів існує майстер делегування керування (Delegation Of Control Wizard).

При делегуванні адміністративних прав можна досить глибоко їх деталізувати, але завжди треба підтримувати рівновагу між збереженням максимально можливої простоти речей і задоволенням вимог безпеки. У більшості випадків делегування адміністративних дозволів в Active Directory відбувається по наступним сценаріям:

– Призначення повного керування одним організаційним підрозділом. Досить типова ситуація, коли компанія має кілька офісів з локальним адміністратором у кожному офісі, який повинен управляти всіма об'єктами локального офісу. Цей варіант може також використовуватися компаніями, які злили домени ресурсів Windows NT в організаційний підрозділ одного домена Active Directory. Колишнім адміністраторам доменів ресурсів можна дати повне керування всіма об'єктами, розташованими в певному організаційному підрозділі. Використання цієї опції означає, що можна практично повністю децентралізувати адміністрування організації, маючи єдиний домен.

– Призначення повного керування певними об'єктами в організаційному підрозділі. Це різновид першого сценарію. У деяких випадках компанія може мати кілька офісів, але локальні адміністратори повинні управляти тільки певними об'єктами в організаційному підрозділі даного офісу. Наприклад, можна дозволити локальному адміністратору управляти всіма об'єктами користувачів і груп, але не комп'ютерними об'єктами. В ситуації, коли домени ресурсів стали організаційними підрозділами, можливо, буде потрібно, щоб адміністратори організаційних

підрозділів управляли всіма комп'ютерними обліковими записами і локальними групами в цьому підрозділі, але не об'єктами користувача.

– Призначення повного керування певними об'єктами всього домена. Деякі компанії мають високо централізоване адміністрування користувачами і групами, в цьому випадку тільки одна група має дозвіл добавляти і видаляти облікові записи груп і користувачів. При такому сценарії даній групі можна давати повне керування об'єктами користувачів і груп незалежно від того, де в межах домена розташовані об'єкти. Цей сценарій є типовим для компанії із централізованою групою адміністрування комп'ютерами і серверами. Комп'ютерній групі можна дати повне керування всіма комп'ютерними об'єктами в домені.

– Призначення прав на модифікацію тільки деяких властивостей об'єктів. У деяких випадках можна надати групі адміністративний дозвіл управляти піднабором властивостей об'єкта. Наприклад, встановлювати паролі для всіх облікових записів користувача, але не мати інших дозволів. Відділу кадрів можна дати дозвіл на модифікацію особистої і відкритої інформації, що стосується всіх облікових записів користувача в домені, але не давати дозвіл на створення або видалення облікових записів користувача.

2.4 Мережева автентифікація. Основні поняття

Щоб процеси захисту, що включають використання ідентифікаторів SID і записів ACL, працювали належним чином, повинен існувати якийсь спосіб, яким користувач одержує доступ до мережі. По суті, користувач повинен мати можливість довести, що він є тим, за кого себе представляє, тобто, що саме йому належить введений ним ідентифікатор. Цей процес називається автентифікацією. В основі надання користувачам можливості доступу до ресурсів мережі лежить базовий принцип «єдиного входу», який припускає те, що користувачеві досить один раз пройти процедуру автентифікації, щоб одержати доступ до мережевих ресурсів.

В процесі автентифікації беруть участь дві сторони: одна сторона доводить свою автентичність, подаючи деякі докази, а інша сторона - автентифікатор - перевіряє ці докази та приймає рішення. Для доказу автентичності застосовуються найрізноманітніші прийоми:

– той, що автентифікується може продемонструвати знання якогось загального для обох сторін секрету: слова (пароля) або факту (дати та місця події, прізвища людини і т.п.);

– той, що автентифікується може продемонструвати, що він володіє унікальним предметом (фізичним ключем), в якості якого може виступати, наприклад, електронна магнітна карта;

– той, що автентифікується може довести свою ідентичність, використовуючи власні біохарактеристики: малюнок райдужної оболонки ока або відбитки пальців, які попередньо були занесені в базу даних автентифікатора.

Мережеві служби автентифікації будуються на основі всіх цих прийомів, але найчастіше для доказу ідентичності користувача використовуються паролі. Простота та логічна ясність механізмів автентифікації на основі паролів у певній мірі компенсує відомі слабкості паролів. Це, по-перше, можливість розкриття та розгадування паролів, а по-друге, можливість «підслуховування» пароля шляхом аналізу мереженого трафіка. Для зниження рівня загрози від розкриття паролів адміністратори мережі, як правило, застосовують вбудовані програмні засоби для формування політики призначення і використання паролів, які дають можливість задати максимальний та мінімальний терміні дії пароля, зберігати список вже використаних паролів, керувати поведінкою системи після декількох невдалих спроб логічного входу і т.д. Перехоплення паролів по мережі можна попередити шляхом їхнього шифрування перед передачею в мережу.

Легальність користувача може встановлюватися стосовно різних систем. Так, працюючи в мережі, користувач може проходити процедуру автентифікації і як локальний користувач, що претендує на використання ресурсів тільки даного комп'ютера, і як користувач мережі, що хоче одержати доступ до всіх мережевих ресурсів. При локальній автентифікації користувач вводить свої ідентифікатор і

пароль, які автономно обробляються операційною системою, встановленою на даному комп'ютері. При логічному вході в мережу дані про користувача (ідентифікатор і пароль) передаються на сервер, що зберігає облікові записи про всіх користувачів мережі. Багато додатків мають свої засоби визначення, чи є користувач законним. В цьому випадку користувачеві доводиться проходити додаткові етапи перевірки.

Об'єктами, що вимагають автентифікації, можуть виступати не тільки користувачі, але й різні пристрої, додатки, текстова та інша інформація. Так, наприклад, користувач, що звертається із запитом до корпоративного сервера, повинен довести йому свою легальність, крім того він повинен переконатися сам, що веде діалог дійсно із сервером свого підприємства. Інакше кажучи, сервер і клієнт повинні пройти процедуру взаємної автентифікації. Тут вступає в силу автентифікація на рівні додатків.

При встановленні сеансу зв'язку між двома пристроями також часто необхідна процедура взаємної автентифікації на канальному рівні. Прикладом такої процедури є автентифікація по протоколах PAP і CHAP, що входить у сімейство протоколів PPP.

Автентифікація даних означає доказ цілісності цих даних, а також того, що вони надійшли саме від тієї людини, що оголосила про це. Для цього використовується механізм електронного підпису.

В обчислювальних мережах процедури автентифікації часто реалізуються тими ж програмними засобами, що й процедури авторизації. На відміну від автентифікації, що розпізнає легальних і нелегальних користувачів, система авторизації має справу тільки з легальними користувачами, які вже успішно пройшли процедуру автентифікації. Ціль підсистем авторизації полягає в тому, щоб надати кожному легальному користувачеві саме ті види доступу і до тих ресурсаів, які були для нього визначені адміністратором системи.

2.5 Технологія мережевої автентифікації в Active Directory

В сучасних операційних системах передбачаються централізовані служби автентифікації. Така служба підтримується одним із серверів мережі. Розглянемо технологію мережевої автентифікації, що підтримується в Windows Server 2003 при реалізації служби каталогів Active Directory.

Автентифікація відбувається перед входом клієнта в систему. Коли користувач сідає за комп'ютер із системами Windows 2000 або Microsoft Windows XP Professional і вводить Ctrl+Alt+Del, служба Winlogon локального комп'ютера перемикається на екран входу в систему і завантажує файл графічної ідентифікації та автентифікації Graphic Identification and Authentication (GINA) з бібліотеки динамічного компонування (DLL). За замовчуванням цей файл - Msgina.dll. Після того, як користувач ввів ім'я користувача, пароль і вибрав домен, GINA передає введені «вірчі грамоти» службі Winlogon. Winlogon передає інформацію локальній службі безпеки LSA (Local Security Authority). Служба LSA негайно застосовує до пароля користувача операцію одностороннього кешування та видаляє зрозумілий текстовий пароль, який користувач надрукував. Потім викликається відповідний провайдер захисту (SSP - Security Support Provider) через інтерфейс провайдерів захисту (SSPI - Security Support Provider Interface). Windows Server 2003 забезпечує два основні SSP-провайдери для мережевої автентифікації - Kerberos SSP і NT LAN Manager (NTLM) SSP. Якщо клієнти із системою Windows 2000, або пізнішою версією операційної системи, входять у мережу системи Windows 2000 або Windows Server 2003, вибирається SSP Kerberos, і інформація передається SSP. Потім SSP зв'язується з контролером домена для підтвердження справжньості користувача. Розпізнавальний процес із використанням протоколу Kerberos буде описаний далі в пункті 2.5.1 даного підрозділу.

Якщо процедура входу в систему пройшла успішно, це означає, що користувач автентифікований. При цьому програма Winlogon створила маркер доступу, який містить список всіх ідентифікаторів SID, пов'язаних з обліковим записом користувача, включаючи ідентифікатор SID самого облікового запису, ідентифікатори SID всіх груп, у які входить цей обліковий запис, і ідентифікатори спеціальних груп, до яких належить даний користувач (наприклад, Domain Admins

або INTERACTIVE). Сформований маркер доступу присвоюється сеансу роботи користувача та використовується при будь-якій наступній спробі доступу до ресурсів. Таким чином користувачеві наданий доступ до мережі. Якщо користувач увійшов в домен, і всі ресурси, до яких користувачеві потрібно звернутися, знаходяться у тому ж самому лісі, то це єдиний момент автентифікації користувача. Поки користувач не вийде із системи, всі дозволи, які він одержить у мережі, будуть засновані на початковій автентифікації.

2.5.1 Протокол Kerberos

Основний механізм автентифікації в Active Directory - це протокол Kerberos. Протокол Kerberos був вперше розроблений інженерами Массачусетського Технологічного інституту (MIT) наприкінці 80-х років. Поточна версія Kerberos - це версія 5 (Kerberos v5), що описана в документі RFC 1510. Реалізація Kerberos в Windows Server 2003 повністю сумісна з документом RFC-1510 з деякими розширеннями для автентифікації відкритих (public) ключів.

Протокол Kerberos є заданим за замовчуванням розпізнавальним протоколом для Active Directory систем Windows 2000 та Windows Server 2003.

В системі, основаній на протоколі Kerberos, є три компоненти. По-перше, клієнт, що повинен одержати доступ до мережевих ресурсів. По-друге, сервер, що управляє мережевими ресурсами та гарантує, що тільки належним чином завірені і уповноважені користувачі можуть одержувати доступ до ресурсу. Третій компонент - центр розподілу ключів (KDC - Key Distribution Center), що служить центральним місцем зберігання користувацької інформації та головною службою, що підтверджує справжність користувачів.

Протокол Kerberos визначає те, як ці три компоненти взаємодіють між собою. Ця взаємодія заснована на двох ключових принципах.

Насамперед, Kerberos працює, опираючись на припущення, що розпізнавальний трафік між робочою станцією і сервером перетинає незахищену мережу. Це означає, що ніякий конфіденційний розпізнавальний трафік ніколи не

пересилається по мережі відкритим, незашифрованим текстом, а користувацький пароль ніколи не пересилається по мережі, навіть у зашифрованій формі.

Другий принцип полягає в тому, що в основі протоколу Kerberos лежить розпізнавальна модель із загальним секретом. У цій моделі клієнт і сервер, що розпізнається, володіють загальним секретом, який нікому більше не відомий. У більшості випадків загальний секрет - це пароль користувача. Коли користувач входить у мережу, захищену протоколом Kerberos, пароль користувача використовується для шифрування пакета інформації. Коли сервер Kerberos одержує пакет, він розшифровує інформацію, використовуючи копію пароля, що зберігається на сервері. Якщо розшифровка пройшла успішно, то сервер знає, що користувачеві відомий загальний секрет, і йому надається доступ.

Однією із проблем загального секрету є те, що користувач і сервер, що управляє мережевим ресурсом, повинні мати деякий спосіб володіння загальним секретом. Якщо користувач намагається одержати доступ до ресурсу на деякому сервері, то обліковий запис користувача може бути створений на сервері з паролем, який знає тільки користувач. Коли користувач спробує звернутися до ресурсів на цьому сервері, він може представити загальний секрет (пароль) і одержати доступ до ресурсу. Однак у корпоративному середовищі можуть бути тисячі користувачів і сотні серверів. Управління різними загальними секретами всіх цих користувачів було б непрактичним. Протокол Kerberos вирішує цю проблему, використовуючи центр розподілу ключів (KDC - Key Distribution Center). Служба KDC виконується як служба сервера в мережі та управляє загальними секретами всіх користувачів у мережі. KDC має одну центральну базу даних для всіх облікових записів користувачів мережі і зберігає загальний секрет кожного користувача (у формі одностороннього хеша пароля користувача). Коли користувачеві потрібно одержати доступ до мережі і мережевих ресурсів, служба KDC підтверджує, що користувач знає загальний секрет, а потім підтверджує справжність користувача.

У реалізації Kerberos сервера Windows Server 2003 цей сервер називається контролером домена. Кожний контролер домена Active Directory є KDC. В Kerberos границя, що визначена користувацькою базою даних, розміщеною на одному KDC,

називається областю (realm). В термінології Windows Server 2003 ця границя називається доменом.

Кожна служба KDC складається із двох окремих служб: служби автентифікації (AS - Authentication Service) і служби надання квитків (TGS - Ticket-Granting Service). Служба AS відповідає за початковий вхід клієнта в систему і видає квиток TGT (TGT - Ticket-Granting Ticket) клієнтові. Служба TGS відповідає за всі квитки сеансу, які використовуються для доступу до ресурсів у мережі Windows Server 2003.

Служба KDC зберігає базу даних облікових записів, що використовуються для автентифікації протоколом Kerberos. В реалізації Kerberos Windows Server 2003 база даних управляється агентом системи каталогу (DSA - Directory System Agent), що виконується в межах процесу LSA на кожному контролері домена. Клієнти і додатки ніколи не отримують прямий доступ до бази даних облікових записів - всі запити ідуть через агента DSA, використовуючи один з інтерфейсів Active Directory. Кожний об'єкт в межах бази даних облікових записів (фактично, кожний атрибут кожного об'єкта) захищений за допомогою списку ACL. Агент DSA гарантує, що будь-які спроби звертання до бази даних облікових записів належним чином санкціоновані.

Коли Active Directory встановлюється на першому контролері домена в домені, створюється спеціальний обліковий запис, що називається krbtgt. Цей обліковий запис не можна видалити або переіменувати, його ніколи не можна дозволяти (enable). При створенні цього запису призначається пароль, що регулярно автоматично змінюється. Цей пароль використовується для створення секретного ключа, призначеного для шифрування і розшифровки квитків TGT, що видаються всіма контролерами домена в домені.

2.5.2 Процес автентифікації на базі протоколу Kerberos

На комп'ютерах із системою Microsoft Windows 2000 Professional або Windows XP Professional, на серверах з Windows 2000 Server або Windows Server 2003 автентифікація по протоколу Kerberos починається з того, що служба LSA

викликає провайдера захисту Kerberos. Коли користувач входить в систему, вводячи ім'я користувача і пароль, комп'ютер клієнта застосовує функцію одностороннього хешування до пароля користувача для створення секретного ключа, що кешується в надійній пам'яті на комп'ютері. Одностороннє хешування означає, що пароль не може бути відновлений виходячи з хеш-значення (hash).

Для здійснення процесу входу клієнта в систему клієнт і сервер виконують наступні дії.

Провайдер Kerberos SSP на робочій станції посилає розпізнавальне повідомлення службі KDC. Це повідомлення включає:

- ім'я користувача;
- область (realm) користувача (ім'я домена);
- запит на TGT-квиток;
- попередні розпізнавальні дані, які включають мітку часу.

Попередні розпізнавальні дані зашифровані за допомогою секретного ключа, отриманого з користувацького пароля.

Коли повідомлення досягає сервера, сервер досліджує ім'я користувача, і шукає по базі даних каталога своєю копію секретного ключа, пов'язаного з даним обліковим записом користувача. Сервер розшифровує зашифровані в повідомленні дані за допомогою секретного ключа і перевіряє часову мітку. Якщо розшифровка пройшла успішно, і часова мітка відрізняється від поточного часу на сервері в межах 5 хвилин, сервер готовий підтвердити справжність користувача. Якщо розшифровка є невдалою, це означає, що користувач ввів неправильний пароль, і автентифікація не відбувається. Якщо часова мітка відрізняється більш ніж на 5 хвилин від поточного часу на сервері, то автентифікація також зазнає невдачі. Причина такої маленької різниці в часі полягає в тому, що вона повинна запобігти можливій спробі перехоплення розпізнавального пакета з наступним повторенням його в подальшому. Задана за замовчуванням максимальна припустима різниця в часі, що становить 5 хвилин, може бути зконфігурована в політиці захисту домена.

Після автентифікації користувача сервер посилає клієнту повідомлення, що включає ключ сеансу і TGT. Ключ сеансу - це ключ шифрування, який клієнт буде

використовувати для взаємодії з KDC замість секретного ключа клієнта. TGT - це квиток сеансу, що надає користувачеві доступ до контролера домена. Протягом терміну служби TGT клієнт пред'являє TGT контролеру домена кожен раз, коли йому потрібно звернутися до мережевих ресурсів. Повне повідомлення від сервера зашифровано за допомогою секретного ключа користувача. Крім того, квиток TGT зашифрований за допомогою довгострокового секретного ключа сервера.

Коли пакет прибуває на комп'ютер клієнта, секретний ключ користувача використовується для розшифровки пакета. Якщо розшифровка пройшла успішно і часова мітка допустима, то комп'ютер користувача припускає, що центр KDC надійно ідентифікував користувача, тому що йому відомий його секретний ключ. Ключ сеансу потім кешується на локальному комп'ютері, поки не закінчиться строк його дії або поки користувач не зробить вихід із системи робочої станції. Цей ключ сеансу буде використовуватися для шифрування всіх майбутніх підключень до центра KDC, тобто клієнт більше не повинен пам'ятати секретний ключ, і останній, в свою чергу, видаляється з кеша робочої станції. Квиток TGT зберігається в зашифрованій формі в кеші робочої станції.

Протокол Kerberos містить в собі Authentication Service (AS) Exchange (Комутатор автентифікаціонної служби), що є підпротоколом, призначеним для виконання початкової автентифікації користувача. Описаний вище процес використовує підпротокол AS Exchange. Початкове повідомлення, послане клієнтом до центра KDC, називається повідомленням KRB_AS_REQ. Відповідь сервера клієнтові називається повідомленням KRB_AS_REP.

Користувач був розпізнаний, але він все ще не має ніякого доступу до мережевих ресурсів. TGT - це квиток сеансу, що надає доступ до центра KDC, але щоб одержати доступ до яких-небудь інших мережних ресурсів, користувач повинен отримати інший квиток сеансу від KDC центра. Робоча станція клієнта надсилає запит на квиток сеанса до центра KDC. Запит включає ім'я користувача, квиток TGT, наданий в процесі автентифікації, ім'я мережевої служби, до якої користувач хоче одержати доступ, і часову мітку, що зашифрована з використанням ключа сеансу, отриманого в процесі AS Exchange.

Служба KDC розшифровує квиток TGT, використовуючи свій довгостроковий ключ. Потім вона витягає ключ сеансу із квитка TGT і розшифровує часову мітку, щоб переконатися, що клієнт використовує правильний ключ сеансу, і гарантувати, що часова мітка допустима. Якщо ключ сеансу і часова мітка прийнятні, то KDC готовить квиток сеансу для доступу до мережевої служби.

Квиток сеансу включає дві копії ключа сеансу, які клієнт буде використовувати для з'єднання з необхідним ресурсом. Перша копія ключа сеансу зашифрована, використовуючи ключ сеансу клієнта, отриманий в процесі початкового входу в систему. Друга копія ключа сеансу призначена для мережевої служби і включає інформацію про доступ користувача. Ця частина квитка сеансу зашифрована, використовуючи секретний ключ мережевої служби, що невідомий робочій станції клієнта, але відомий і службі KDC і мережевій службі, тому що сервер, на якому розташований ресурс, є членом сфери KDC.

Робоча станція клієнта кешує обидві частини квитка сеансу в пам'яті.

Процес, описаний у кроках з 5-го по 8-ой, використовує підпротокол Ticket-Granting Service Exchange (Комутатор служби надання квитків). Запит на квиток сеансу, надісланий клієнтом, називається повідомленням KRB_TGS_REQ; відповідь сервера - повідомленням KRB_TGS_REP.

Тепер клієнт пред'являє квиток сеанса мережевій службі для одержання доступу.

Мережева служба розшифровує ключ сеанса, зашифрований в квитку сеансу, використовуючи довгостроковий ключ, яким вона володіє разом із центром KDC. Якщо ця розшифровка пройшла успішно, то мережева служба знає, що квиток виданий довіреною службою KDC. Потім мережева служба розшифровує інформацію про основний SID користувача, SID всіх груп, в які він входить, а також права і привілеї користувача, використовуючи ключ сеансу, і перевіряє користувацький рівень доступу. Запит клієнта включає також часову мітку, що зашифрована за допомогою ключа сеансу і перевірена сервером.

Процес, описаний на кроках 9 та 10, використовує підпротокол Client/Server (CS) Exchange. Запит клієнта називається повідомленням KRB_AP_REQ.

Після того, як автентифікація і перевірка дозволу пройшли успішно, клієнтові надається доступ до ресурсів сервера. Якщо клієнт має потребу в подальшому використанні ресурсу або служби, то квиток сеансу переміщається з кеша, призначеного для квитка клієнта, і передається на цільовий сервер ресурсу. Якщо термін дії квитка сеансу минув, клієнт повинен звернутися до KDC для одержання нового квитка.

Процес одержання доступу до мережевого ресурсу показує, що центр KDC задіяний в процесі початкового входу клієнта в систему, коли клієнт вперше намагається звернутися до ресурсу, розміщеному на певному сервері. Коли користувач вперше входить у систему, йому видається квиток TGT, який надає клієнтові доступ до центра KDC протягом терміну служби квитка. Коли клієнт намагається з'єднатися з мережевим ресурсом, він знову входить в контакт із KDC і одержує квиток сеансу для доступу до цього ресурсу. Квиток сеансу включає відомості авторизації у вигляді списку SID, що включає SID користувача і SID груп, в які він входить. Коли ця інформація пред'являється серверу, на якому розташований ресурс, сервер визначає рівень доступу до ресурсу, що повинен мати даний користувач.

2.5.3 Автентифікація, що перетинає границі домена

Той же самий розпізнавальний процес застосовується і у випадку, коли при підтвердженні справжньості користувача відбувається перехід за границі домена. Наприклад, компанія може мати ліс із трьома доменами, як показано на рисунку 2.1.

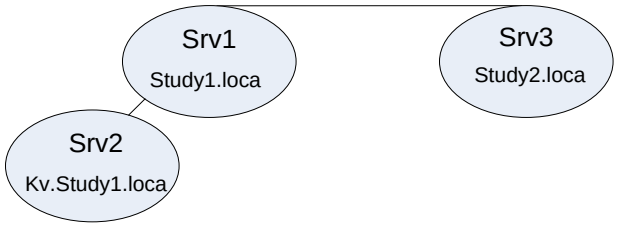

Рисунок 2.1 – Автентифікація, що перетинає границі домена

Якщо користувач, що має обліковий запис у домені Study2.local, перейде в домен Kv.Study1.local і спробує ввійти в мережу, робоча станція клієнта зможе з'єднатися з контролером домена в домені Study2.local. В цьому випадку комп'ютер клієнта надсилає початковий запит входу в систему на контролер домена Kv.Study1.local. Контролер домена визначає, що обліковий запис користувача розташований в домені Study2.local, так що потрібно переправити запити робочої станції клієнта до цього домена. Якщо всі домени були зконфігуровані зі скороченими довірчими відносинами (shortcut trusts), то контролер домена може прямо направити комп'ютер клієнта до контролера домена в домені Study2.local. Однак якщо скорочених довірчих відносин не було створено, то немає і прямої довірчої відносини між доменами Kv.Study1.local і Study2.local. У цьому випадку контролер домена Kv.Study1.local направить комп'ютер клієнта до контролера домена в домені Study1.local. Напрямок включає ключ сеансу, що надає доступ до контролера домена в домені Study1.local. Ключ сеансу створюється, коли домен Kv.Study1.local включається до лісу Study1.local і створюються початкові довірчі відносини між цими двома доменами. Ключ сеансу гарантує, що запит на вхід у систему надходить від довіреного домена. Потім комп'ютер клієнта надсилає розпізнавальний запит до домену Study1.local. Тепер клієнт направляється до контролера домена в домені Study2.local. Знову цей напрямок включає ключ сеансу, необхідний для доступу до контролера домена. Далі комп'ютер клієнта надсилає запит TGT на свій домашній контролер домена в Study2.local.

Аналогічний процес відбувається тоді, коли клієнт пробує одержати доступ до ресурсу, розташованому за межами домашнього домена користувача. В цьому випадку клієнт повинен одержати квиток сеансу від контролера домена, розташованого в тому домені, де перебуває ресурс, поки він не зможе з'єднатися із правильним контролером домена.

Розпізнавальний процес впливає на проект лісу, особливо якщо користувачі часто входять на домени, до яких вони самі не належать, або звертаються до ресурсів інших доменів. Якщо розробляється ліс із декількома доменами, клієнтові,

ймовірно, прийдеться перетинати весь шлях довірчих відносин між доменами. Якщо це відбувається часто, потрібно помістити контролери домена кореневих доменів ближче до користувачів. Можна також використовувати скорочені довірчі відносини, поняття яких було розглянуто раніше, щоб напрямки контролера домена посилалися потрібним доменам напряму.

2.5.4 Конфігурування Kerberos в Windows Server 2003

Як зазначалося вище, протокол Kerberos заданий за замовчуванням як розпізнавальний протокол для клієнтів із системами Windows 2000 та більш пізніми, які входять в Active Directory. Існує можливість зконфігурувати кілька властивостей Kerberos через політику безпеки домена.

Щоб звернутися до параметрів настроювання політики Kerberos, необхідно відкрити пункт Domain Security Policy із інструментів адміністрування та розгорнути дерево Windows Configuration/Security Settings/Account Policy/Kerberos Policy (Конфигурация Windows/Параметры безопасности/Политика учетных записей/Порлитика Kerberos). В таблиці 2.5 наведені існуючі політики настроювання протоколу Kerberos.

Таблиця 2.5 Політики настроювання протоколу Kerberos

Політика	Опис
Enforce User Logon Restrictions (Підсилення обмежень користувацького входу в систему)	Ця політика встановлює опцію служби KDC, по якій при кожному запиті на квиток сеансу перевіряються установки прав користувача на цільовому комп'ютері. Якщо ця політика включена, то користувач, що запитує квиток сеансу, повинен мати права Allow Log On Locally (Дозволити локальний вхід), якщо він увійшов в систему в інтерактивному режимі, або права Access This Computer From The Network на цільовому комп'ютері. Ці права призначаються в меню Local Policies\User

	Rights Assignment в пункті Domain Security Policy За замовчуванням ця політика включена.
Maximum Lifetime For Service Ticket (Максимальний строк придатності службового білету)	Ця політика встановлює максимальний час (в хвилинах), протягом якого квиток сеансу може використовуватися для доступу до певної служби. Якщо встановлено нуль хвилин, то строк придатності квитка необмежений. Якщо встановлено ненульову кількість хвилин, то він повинен бути більше, ніж 10 хвилин, і менше або дорівнювати значенню, встановленому для параметра Maximum Lifetime For User Ticket За замовчуванням ця установка становить 600 хвилин

Продовження таблиці 2.5 Політики настроювання протоколу Kerberos

Maximum Lifetime For User Ticket (Максимальний строк придатності для користувацького білету)	Ця політика встановлює максимальний час (в годинах), протягом якого може використовуватися TGT-квиток користувача. Після того як мине строк придатності TGT-квитка, існуючий квиток повинен бути відновлений, інакше потрібно вимагати новий квиток в центрі KDC. За замовчуванням ця установка становить 10 годин.
Maximum Lifetime For User Ticket Renewal (Максимальний строк, протягом якого можливе	Ця політика встановлює час (в днях), протягом якого TGT-квиток може бути відновлений (замість одержання нового TGT-квитка). За замовчуванням ця установка становить 7 днів.

обновлення користувацького білету)	
Maximum Tolerance For Computer Clock Synchronization (Максимальна допустима розбіжність в показаннях комп’ютерних часів)	Ця політика встановлює максимальну різницю у часі (в хвилинах) між часом на комп'ютері клієнта і часом на контролері домена, що забезпечує автентифікацію по протоколу Kerberos, яку протокол Kerberos вважає припустимою. Якщо різниця в часі між показаннями цих двох комп'ютерів більше, ніж припустимий рівень, всі квитки Kerberos будуть відкинуті. За замовчуванням ця установка становить 5 хвилин. У випадку зміни цієї установки при перезапуску комп'ютера вона повернеться до заданого за замовчуванням значення.

В більшості випадків параметри настроювання протоколу Kerberos, що задані за замовчуванням, є прийнятними. У середовищах з високим рівнем безпеки можна зменшити терміни служби квитків. Однак, в цьому випадку клієнти повинні будуть частіше підключатися до центра KDC, створюючи додатковий мережевий трафік і зайве навантаження на контролерах домена.

2.5.5 Протоколи автентифікації LAN Manager, NTLM і NTLMv2

Крім описаного мережевого протоколу перевірки справжньості Kerberos, існують такі мережеві протоколи автентифікації як LAN Manager, NTLM, NTLMv2.

Протоколи NTLM і NTLMv2 підтримуються для підтвердження справжньості в Active Directory з метою зворотної сумісності із клієнтами, що користуються старішими версіями операційних систем.

LAN Manager

Протокол LAN Manager (LM) розроблений Microsoft уже давно і застосовувався для мережевих клієнтів у складі ранніх версій Windows. Цей мережевий протокол перевірки справжньості заснований на запитах і відгуках і працює наступним чином.

1. Користувач вводить пароль.

2. LSA одержує хеш введеного пароля з використанням того ж алгоритму, яким зашифровані паролі в БД контролера домена, незашифрований пароль відкидається.

3. Клієнт ініціює процедуру перевірки справжньості на контролері домена, відправляючи йому своє ім'я користувача.

4. У відповідь контролер домена надсилає запит (challenge) — 16-розрядне випадкове число.

Зашифроване випадкове число використовується для запобігання атак повтором. Перехопивши це число, атакуючий не зможе використовувати його для автентифікації, оскільки не має хэша пароля, використаного для шифрування цього числа.

5. Клієнт, використовуючи хеш пароля як ключ, шифрує рядок запиту і відправляє його контролеру домена в одному пакеті з іменем користувача, цей пакет називається відгуком (response).

Перехоплений відгук може бути використаний для взлому пароля, у випадку, коли атакуючий зможе перехопити і випадкове число.

Контролер домена шифрує рядок запиту з використанням копії хеша пароля клієнта зі своєї БД. Два шифри порівнюються, і у випадку відповідності вважається, що клієнт пройшов перевірку.

Недолік протоколу перевірки справжньості LM виражається у використанні нестійкого пароля і методу його шифрування:

– всі букви переводяться у верхній регістр, тому паролі із великих і малих літер а також чисел еквівалентні. Взагалі, чим більше різних символів використано в паролі, тим він надійніше;

– пароль не може перевищувати 14 символів у довжину, але чим довший пароль, тим складніше його зламати, і тому він більш надійний.

– Процедурі шифрування також властивий недолік, який полягає в тому, що пароль розбивається на дві групи по 7 символів, які обробляються незалежно, а результати комбінуються. Такий пароль простіше зламати, оскільки підібрати два паролі довжиною по 7 символів легше, ніж один з 14 символів.

NTLM і NTLMv2

NTLM або протокол перевірки справжньості Windows NT LAN Manager, розроблений Microsoft для перших версій Windows NT. Цей протокол також заснований па запитах і відгуках і працює так само як і LAN за наступними виключеннями:

– пароль може бути набагато довший 14 символів, в Windows Server 2003 - до 128. Попередні версії Windows NT і Server 2000 не могли працювати з паролями такої довжини через недоліки графічного інтерфейсу (для введення довгих паролів потрібно було користуватися нестандартними доповненнями до інтерфейсу). В Windows Server 2003 довгі паролі підримуються стандартним графічним інтерфейсом;

– використовується MD5-хеш цілого пароля, а не його 7-символьних фрагментів, із збереженням регістра символів. Протокол NTLM також допускає використання будь-яких символів UNICOD, а LM - тільки деяких ASCII-символів. Тому зламати 14-символьний пароль NTLM набагато складніше, ніж пароль LM тієї ж довжини. Взагалі, для злому хеша, який NTLM виконує для стійкого пароля з використанням сучасних технологій, потрібно більше середньої тривалості людського життя;

– NTLMv2 дозволяє включити додатковий захист сеансу по взаємній згоді сторін, у тому числі перевірку цілісності та конфіденційність повідомлень з використанням 128-розрядного шифрування для додатків, що підтримують захищені сеанси (правда, таких додатків досить мало). В NTLMv2 була включена підтримка часових оцінок для захисту від повтору, що вимагає синхронізації годин сервера і клієнта з різницею в часі не більше 30 хвилин.

Групова політика

Однією із складових системи безпеки Active Directory є настроювання безпеки за допомогою групових політик.

В Active Directory існує три області безпеки, в яких застосовується групова політика, - це параметри безпеки, аудит і ведення журналу безпеки, а також аналіз і настроювання безпеки.

3 НАЛАШТУВАННЯ ACTIVE DIRECTORY ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Основні кроки налаштування Active Directory

Перед розгортанням доменної структури у мережі необхідно її спланувати і мати чітке уявлення про призначення окремих серверів і процесах взаємодії між ними.

Перед тим як створювати перший контролер домену необхідно визначитися з режимом його роботи. Режим роботи визначає доступні можливості і залежить від версії операційної системи. Розглянемо популярні режими : Windows Server 2003, 2008 і 2008 R2.

Режим Windows Server 2003 слід вибирати тільки тоді, коли у інфраструктурі вже розгорнуті сервера на даній ОС і планується використовувати один або кілька таких серверів в якості контролерів домену. В інших випадках потрібно вибирати режим Windows Server 2008 або 2008 R2 в залежності від куплених ліцензій. Слід пам'ятати, що режим роботи домену можна завжди підвищити, а ось знизити вже не вдасться (хіба що відновивши з резервної копії), тому підходити до цього питання потрібно обережно, з урахуванням можливих розширень, ліцензій в філіях і т.д. і т.п.

Потрібно звернути увагу на те, що в повноцінної структурі Active Directory контролерів домену має бути не менше двох. В іншому випадку це призведе до невиправданого ризику, так як в разі відмови єдиного контролера домену структура AD буде повністю знищена. Добре якщо буде актуальна резервна копія і з неї вдасться відновитися, в будь-якому випадку весь цей час мережа буде повністю паралізована.

Тому відразу ж після створення першого контролера домену потрібно розгорнути другий, незалежно від розмірів мережі і бюджету. Другий контролер повинен бути передбачений ще на стадії планування і без нього за розгортання AD навіть не варто братися. Також не варто поєднувати роль контролера домену з будь-

якими іншими серверними ролями, з метою забезпечення надійності операцій з базою AD на диску відключається кешування запису, що призводить до різкого падіння продуктивності дискової підсистеми (це пояснює і довге завантаження контролерів домену).

Всупереч поширеній думці, всі контролери в домені рівнозначні, тобто кожен контролер містить повну інформацію про всі об'єкти домену і може обслужити клієнтський запит. Але це не означає, що контролери взаємозамінні, нерозуміння цього моменту часто призводить до відмов AD і простою мережі підприємства. Чому так відбувається? Саме час згадати про роль FSMO.

Коли було створено перший контролер, то він містить всі доступні ролі, а також є глобальним каталогом, з появою другого контролера йому передаються ролі господаря інфраструктури, володаря RID і емулятора PDC. Що буде якщо адміністратор вирішив тимчасово вивести з ладу сервер DC1, наприклад щоб почистити від пилу? На перший погляд нічого страшного, домен перейде в режим "тільки читання", але працювати буде. Але потрібно пам’ятати про глобальний каталог і якщо у мережі розгорнуті додатки вимагають його наявності, наприклад Exchange, то в цьому випадку мережа працювати не буде.

З чого випливає висновок: в лісі має бути не менше двох глобальних каталогів, а найкраще по одному в кожному домені. Так як у нас домен в лісі один, то обидва сервера повинні бути глобальними каталогами, це дозволить без особливих проблем вивести будь-який з серверів на профілактику, тимчасова відсутність будь-яких ролей FSMO не призводить до відмови AD, а лише робить неможливим створення нових об'єктів.

Адміністратор домену, повинен чітко знати яким чином ролі FSMO розподілені між серверами і при виведенні сервера з експлуатації на тривалий термін передавати ці ролі іншим серверам. А якщо сервер містить ролі FSMO необоротно вийде з ладу, то мережа буде працювати і далі, так як будь-який контролер домену містить всю необхідну інформацію і якщо така неприємність все ж сталася, то потрібно буде виконати захоплення необхідних ролей одним з контролерів, це дозволить відновити повноцінну роботу служби каталогів.

Припустимо організація зростає і у неї з'являється філія в іншому кінці міста і виникає необхідність включити їх мережу в загальну інфраструктуру підприємства. Потрібно налаштувати канал зв'язку між офісами та розмістити в ньому додатковий контролер (рис.2.1). Для того щоб контролювати сервер майже без ризику несанкціонованого доступу, потрібно встановити особливий тип контролера: контролер домена доступний тільки на читання (RODC), дана функція доступна в режимах роботи домену починаючи з Windows Server 2008 і вище.

Контролер домену доступний тільки для читання містить повну копію всіх об'єктів домену і може бути глобальним каталогом, однак не дозволяє вносити ніяких змін в структуру AD, також він дозволяє призначити будь-якого користувача локальним адміністратором, що дозволить йому повноцінно обслуговувати даний сервер, але знову таки без доступу до служб AD.

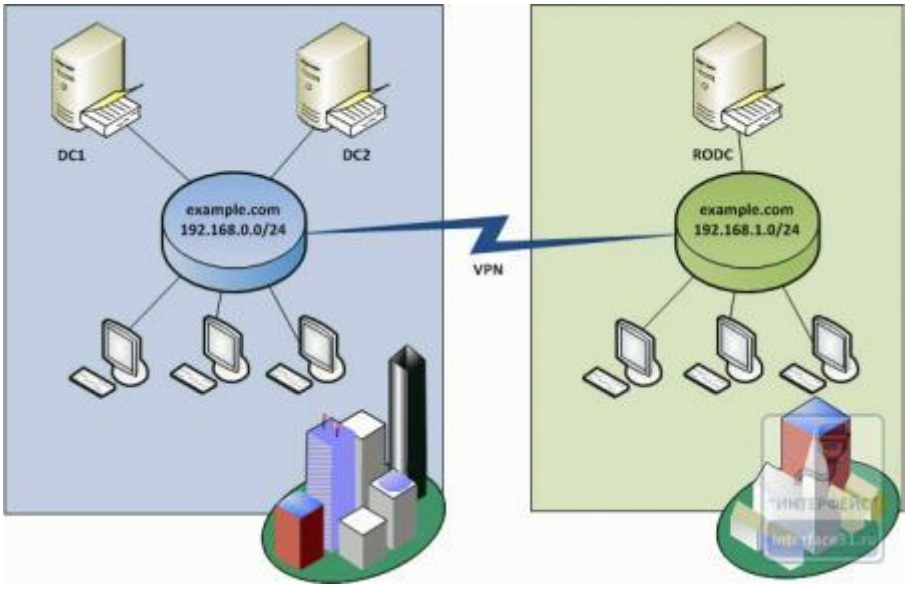

Рисунок 3.1 – Схема підключення філіалу організації

При налаштуванні в філії RODC, може виникнути проблема з довгим входом в систему, та дуже великий інтернет трафік. Причиною цього є повільний і завантажений канал зв’язку. А головна причина завантаженості каналу зв’язку це реплікація. Як відомо, всі зміни, зроблені на одному з контролерів домену,

автоматично поширюються на інші і називається цей процес реплікацією, він дозволяє мати на кожному контролері актуальну і несуперечливу копію даних. Служба реплікації працює незалежно від того на якій відстані знаходиться сервер, тобто працює не залежно від швидкості каналу і тому всі зміни в офісі тут же будуть реплікуватися до філії, завантажуючи канал і збільшуючи витрату трафіку.

Для того щоб виправити цю проблему потрібно налаштувати сайти Active Directory . Сайти Active Directory представляють спосіб фізичного поділу структури служби каталогів на області відокремлені від інших областей повільними та нестабільними каналами зв'язку. Сайти створюються на основі підмереж і всі клієнтські запити відправляються в першу чергу контролерам свого сайту, також вкрай бажано мати в кожному сайті свій глобальний каталог. У досліджуваній мережі потрібно створити два сайти: AD Site 1 для центрального офісу та AD Site 2 для філії (точніше один, так як за замовчуванням структура AD вже містить сайт, куди входять всі раніше створені об'єкти). Тепер розглянемо як відбувається реплікація в мережі з декількома сайтами на рисунку 3.2 .

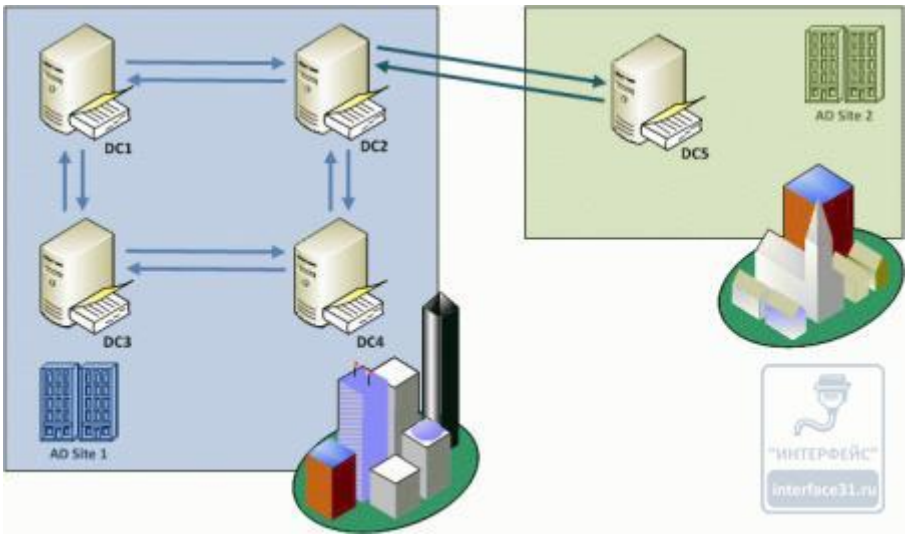

Рисунок 3.2 - Реплікація з налаштованими сайтами Active Directory

Організація розвилася і головний офіс містить цілих чотири контролери домену, реплікація між контролерами одного сайту називається

внутрішньосайтовою і відбувається моментально. Топологія реплікації будується за схемою кільця з умовою, щоб між будь-якими контролерами домену було не більше трьох кроків реплікації. Схема кільця зберігається до 7 контролерів включно, кожен контролер встановлює зв'язок з двома найближчими сусідами, при більшій кількості контролерів з'являються додаткові зв'язку і загальне кільце як би перетворюється в групу накладених один на одного кілець.

Міжсайтова реплікація відбувається інакше, в кожному домені автоматично вибирається один з серверів (сервер-плацдарм) який встановлює зв'язок з аналогічним сервером іншого сайту. Реплікація за замовчуванням відбувається раз в 3 години (180 хвилин), проте можна встановити будь-який розклад реплікації і для економії трафіку всі дані передаються в стислому вигляді. При наявності в сайті тільки RODC реплікація відбувається однонаправлено.

3.2 Розгортання доменної структури Active Directory

Перед тим як приступити до практичного втілення планів розгортання, необхідно виконати деякі кроки, а саме:

- Назначити майбутньому доменному контролера зручне для читання ім'я.
- Встановити для мережевого адаптера статичну IP адресу.
- Переймнувати вбудований обліковий запис адміністратора, використовуючи тільки латинські букви і символи.

Після того, як всі вищевикладені рекомендації виконані, було проведено установку ролі «Доменні служби Active Directory», це було виконано через оснащення Ролі в диспетчері сервера (рис. 3.3).

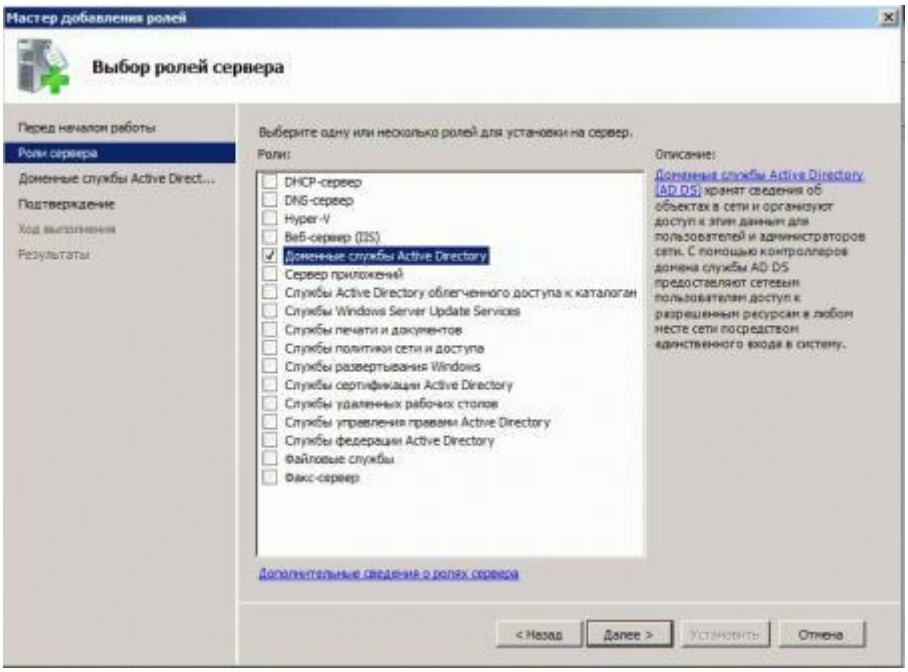

Рисунок 3.3 – Вибір ролі серверу

Установка даної ролі не робить даний сервер контролером домену, для цього необхідно запустити «Мастер установки доменных служб», що і було запропоновано зробити після закінчення установки (рис 3.4).

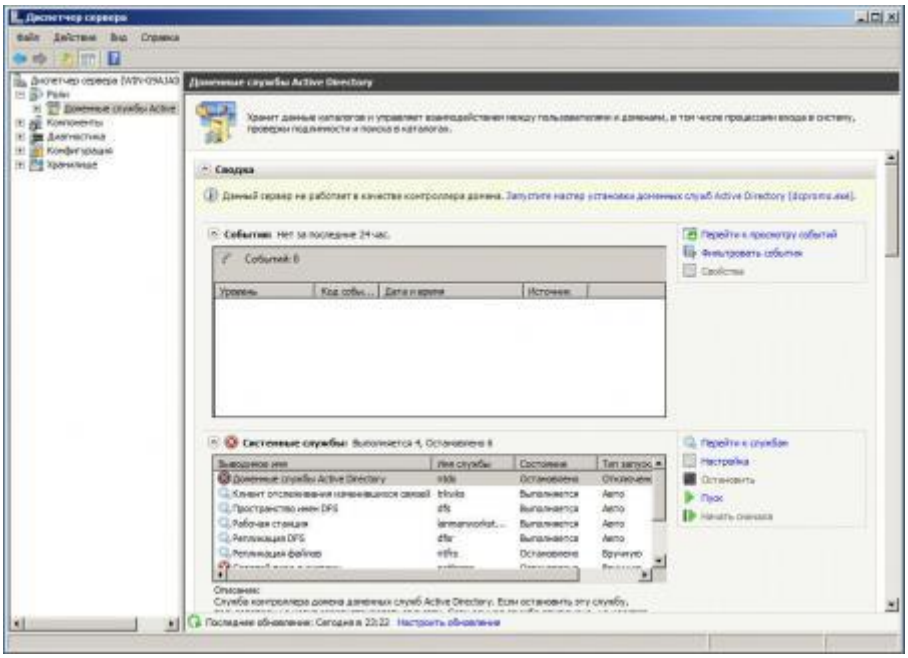

Рисунок 3.4 – Майстер завантаження доменних служб

Так як це наш перший контролер домену, то вибираємо Створити новий домен в новому лісі (рис 3.5).

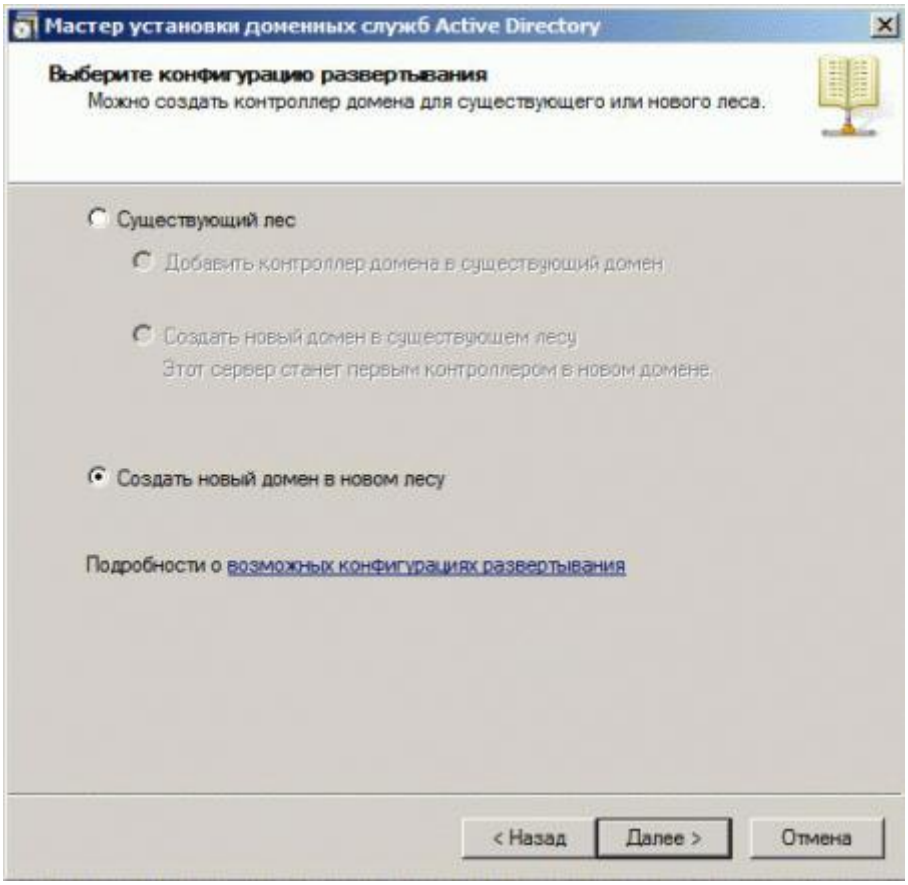

Рисунок 3.5 – Створення нового домену в новому лісі

Наступним кроком вказано ім'я домену. Не рекомендується давати домену інтернет ім'я зовнішнього домену, також не рекомендується давати ім'я в неіснуючих зонах першого рівня, типу .local або .test і т.д. Оптимальним варіантом для домену AD буде піддомен в просторі імен зовнішнього інтернет домену, наприклад corp.example.com. Як назначається ім’я показано на рисунку 3.6.

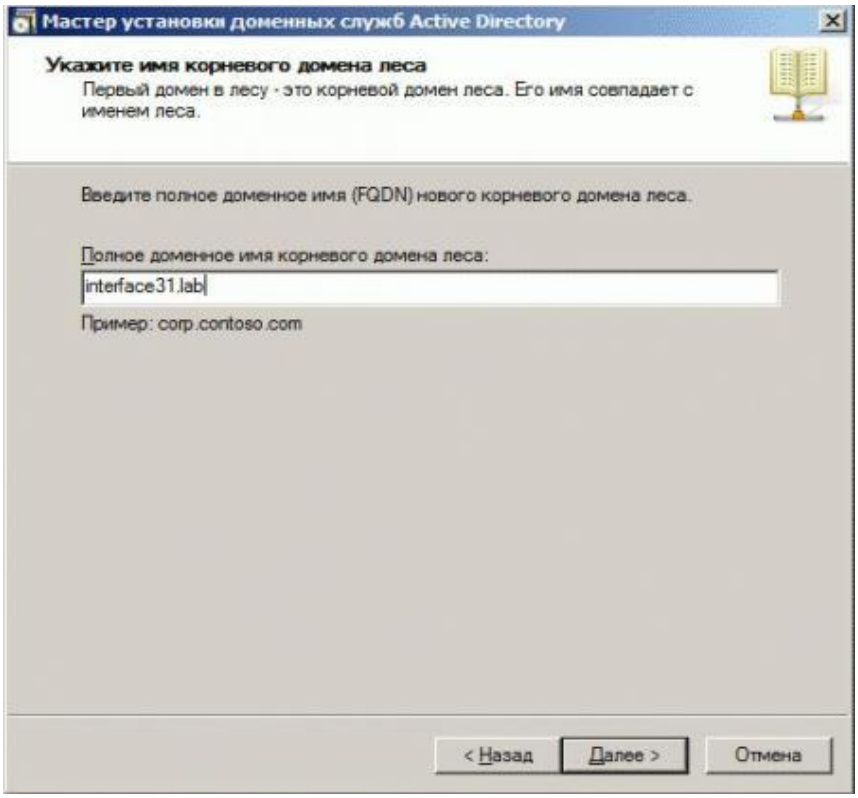

Рисунок 3.6 – Призначення імені кореневого домену ліса

Необхідно обрати режим роботи лісу (рис 3.7).

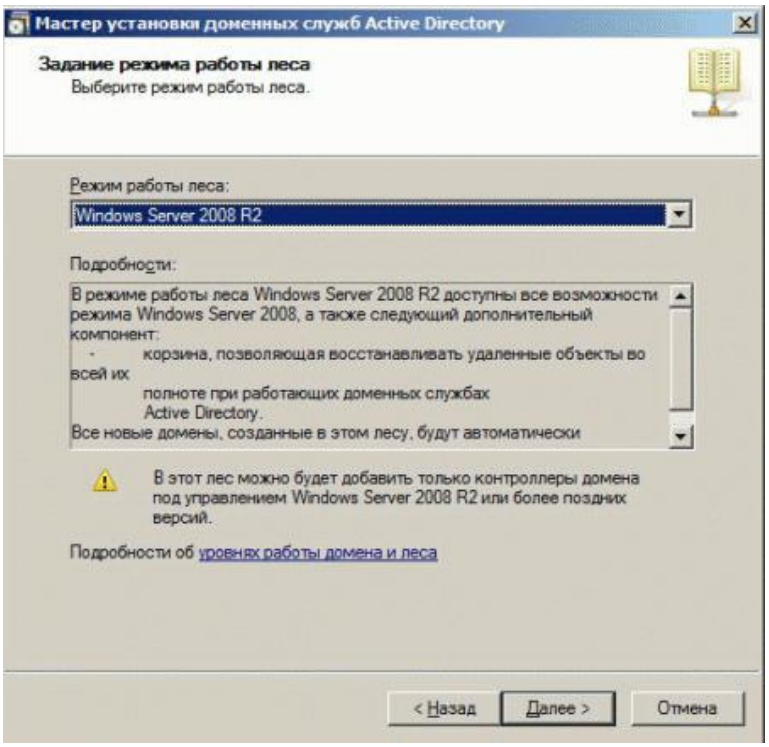

Рисунок 3.7 – Вибір режиму роботи лісу

У додаткових параметрах необхідно вказати опцію DNS-сервер. Так як Active Directory і служби DNS тісно пов'язані між собою, то необхідно робити кожен контролер домену DNS сервером(Рис 3.8).

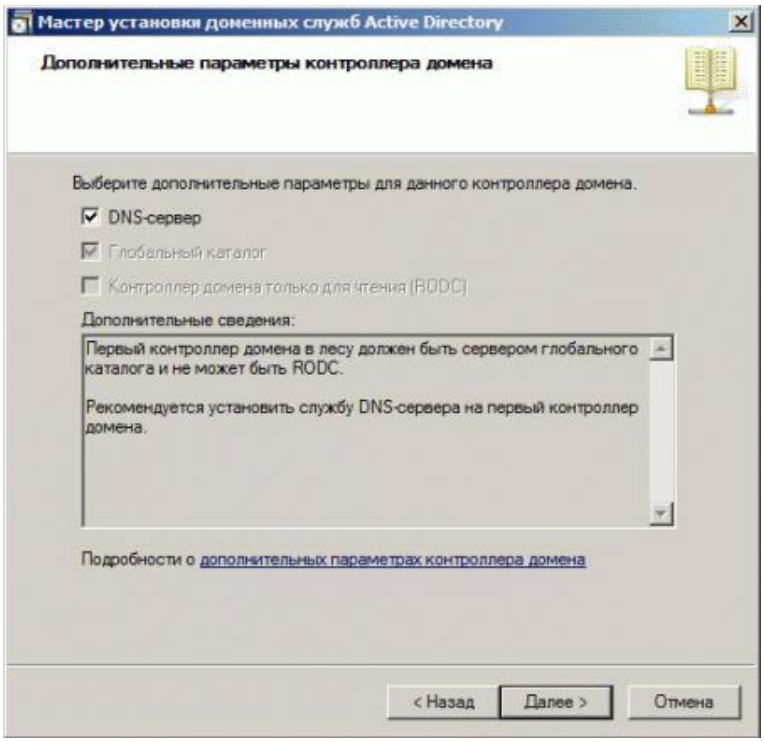

Рисунок 3.8 – Вікно додаткових параметрів контролерів домену

Необхідно вказати пароль адміністратора режиму відновлення служб каталогів (рис 3.9).

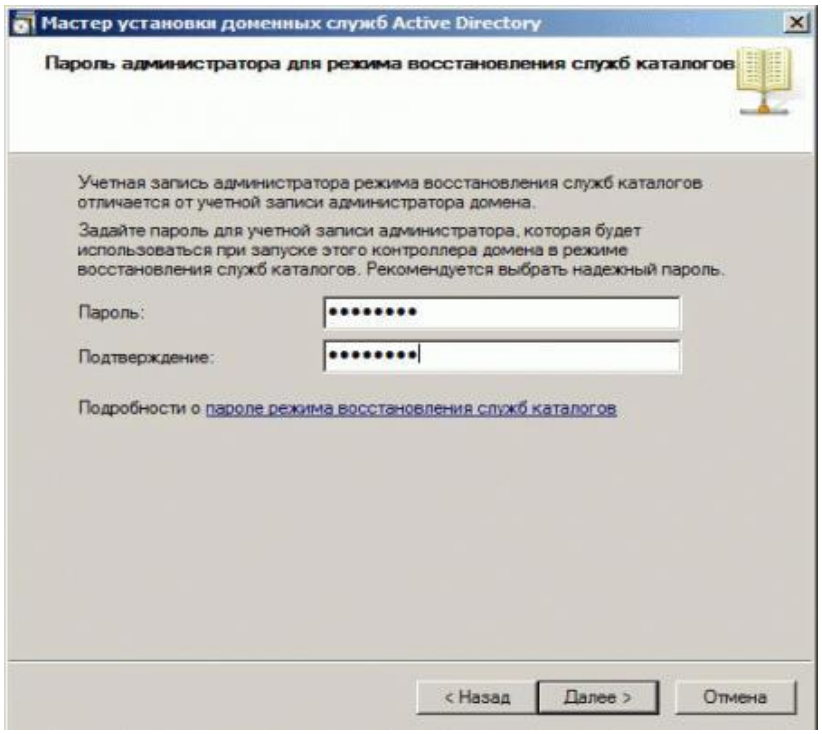

Рисунок 3.9 – Вікно введення паролю адміністратора режиму відновлення служб каталогів

Так як з цього моменту вже нічого змінити або виправити буде не можливо і якщо десь допущена помилка, то необхідно перевірити всі введені дані.

По завершенні роботи майстра необхідно перезавантажити сервер. Було налаштовано перший контролер домену, який також виконує роль DNS-сервера для мережі. Даний сервер буде містити записи про всі об'єкти вашого домену, при запиті записів, що відносяться до інших доменів, які він не зможе дозволити, вони будуть передані вищим серверам, т.зв. серверів пересилки.

За замовчуванням в якості серверів пересилки вказується адреса DNS-сервера з властивостей мережевого підключення, щоб згодом уникнути різного роду збоїв в роботі мережі слід явно вказати доступні сервера в зовнішній мережі. Для цього необхідно відкрити оснащення DNS в диспетчері сервера і обрати сервера пересилання для свого сервера. Також необхідно вказати не менше двох доступних зовнішніх серверів, це можуть бути як сервера провайдера, так і публічні DNS-служби (рис 3.10).

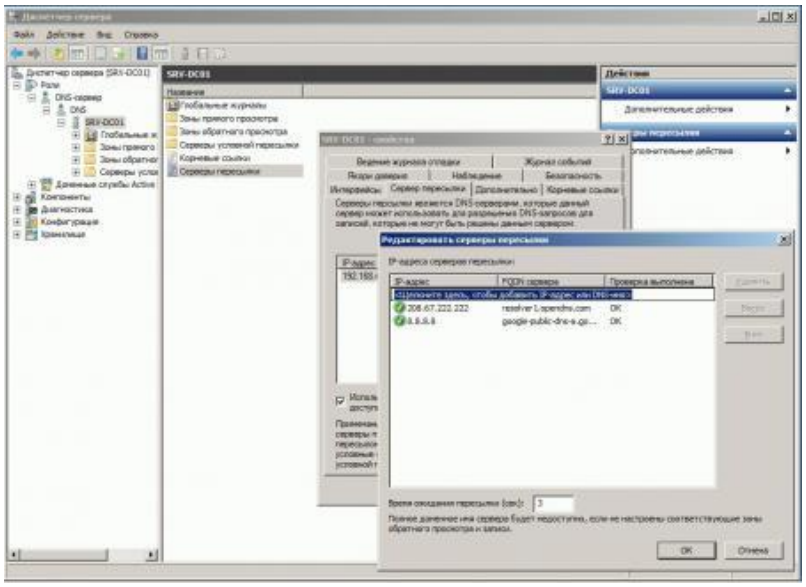

Рисунок 3.10 – Вікно сервера пересилання DNS

Необхідно перевірити, що у властивостях мережевого підключення контролера домену, який є DNS-сервером, як адресу DNS має бути вказано 127.0.0.1, будь-які інші варіанти записи є помилковими.

Створивши перший контролер домену, необхідно почати розгортання другого контролеру, без цього структура AD не вважається повноцінною і відмовостійкою. Як DNS-сервер потрібно вказати адресу першого контролера і ввести сервер в домен.

Після перезавантаження необхідно увійти доменним адміністратором і встановити роль Доменні служби Active Directory, після чого також запустити майстер. Принципових відмінностей в налаштуванні другого контролера немає. Обов'язково вказуємо, що це додавання нового контролеру в існуючий домен (рис 3.11).

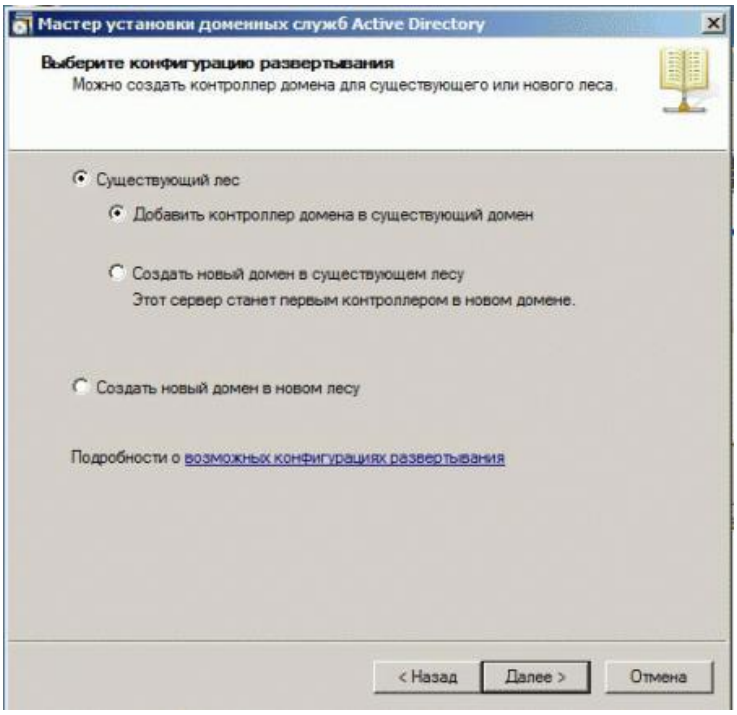

Рисунок 2.11 – Створення існуючого серверу в існуючий домен

Так як при відсутності глобального каталогу домен може виявитися непрацездатним, то рекомендується мати як мінімум два глобальних каталогу і додатково додавати глобальні каталоги в кожен новий домен або сайт AD (рис 3.12).

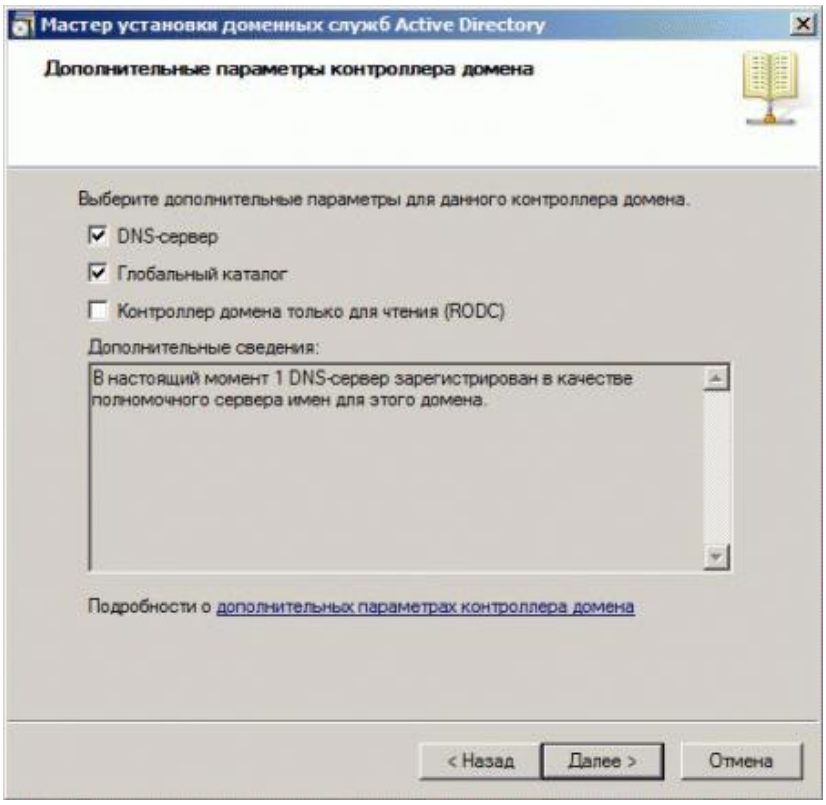

Рисунок 3.12 – Налаштування додаткових параметрі другого контролера домену

Інші налаштування повністю ідентичні. В ході розгортання другого контролера, в процесі якого виконані налаштування відповідних служб і проведена реплікація з першим контролером.

Закінчивши установку другого контролера необхідно перейти до налаштувань доменних служб: створювання користувачів, рознесення їх по групах і підрозділах, налаштування групової політики і т.д. і т.п. Робити це можливо на будь-якому контролері домена, для цього були використані відповідні пункти меню Адміністрування (рис. 3.13).

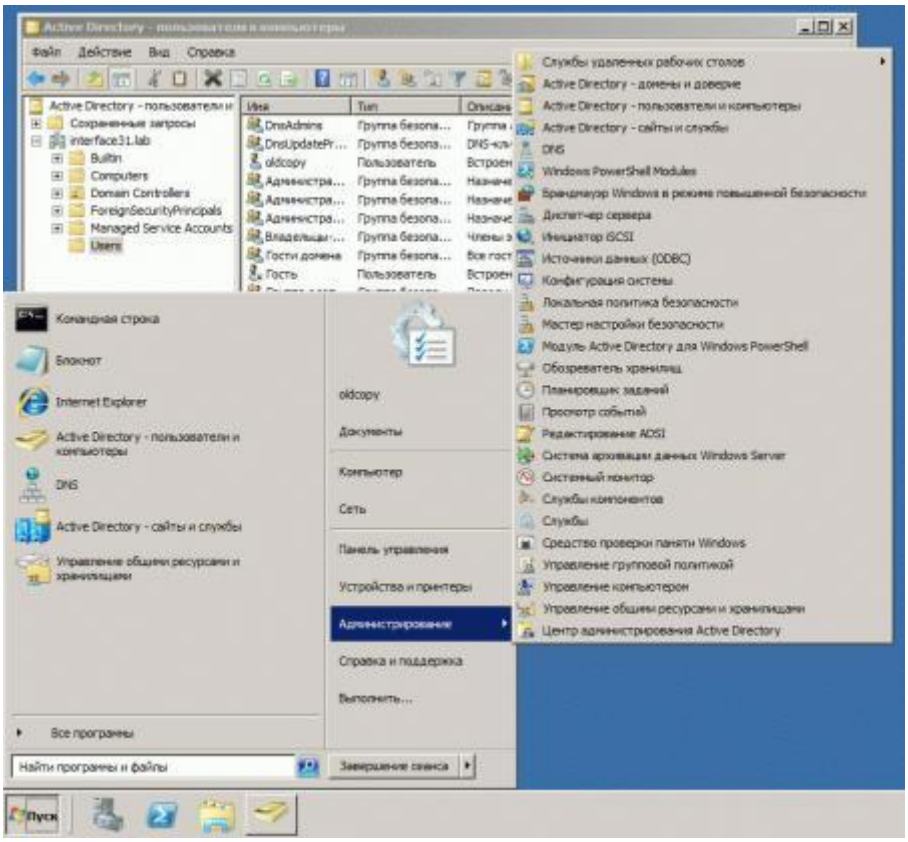

Рисунок 3.13 – Можливості адміністрування Active Directory

3.3 Налаштування DHCP

На відміну від DNS або AD, DHCP не дозволяє створити два повноцінних сервера і репліціювати дані між ними. Єдиний DHCP-сервер здатний доставити чимало проблем системному адміністратору, сервер з цією роллю навіть на профілактику вивести проблемно, не кажучи вже про збої.

Зазвичай DHCP-сервер суміщають з роутером, в простих мережах даний підхід виправданий, в структурі AD рекомендовано поєднати ролі контролера домену та DHCP-сервера. Для створення відмовостійкої схеми знадобилося два DHCP-сервера, між якими необхідно розділити пул адрес області. Рекомендується співвідношення 80/20, але можна відношення ставити будь-яке (рис. 3.14).

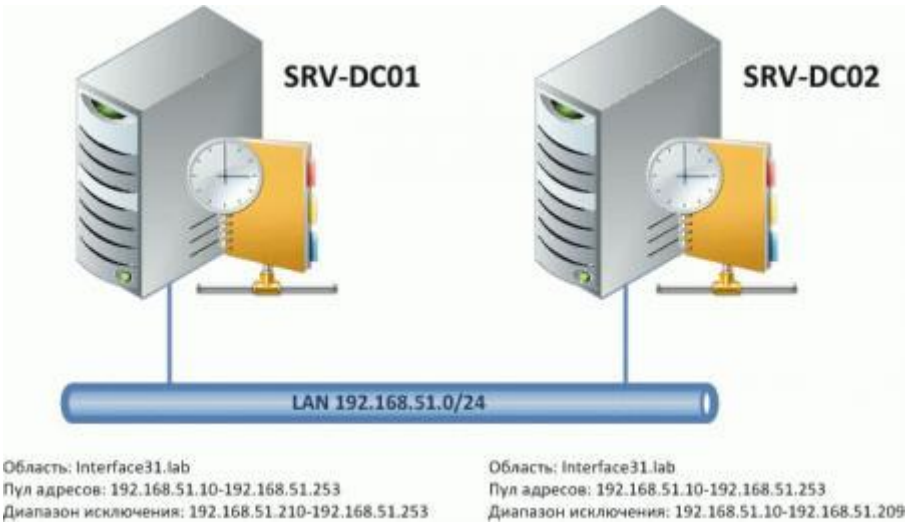

Рисунок 3.14 – Схема підключення DHCP серверів

Однак перед тим як розподілити пул адреси, варто зробити схему розподілу адрес у мережі.

В даній мережі , дотримуємося такої схеми показаної на рисунку 3.15.

Рисунок 3.15 – Схема розподілу адрес пулу

Основною перевагою даного підходу є те, що зустрівши IP-адресу 192.168.51.203 можна знати точно , що це один з мережевих принтерів, а 192.168.51.51 - Wi-Fi обладнання.

З урахуванням даної схеми було відділення пул DHCP-адрес і поділ його в співвідношенні 80/20. У даному випадку це діапазони до і після адреси (включно) 192.168.51.210.

Блок адрес 1-10 - не використовується, так як правило багато мережевих пристроїв налаштовані на використання адреси 192.168.x.1 за замовчуванням і мережеві зловмисники при спробі підключитися до мережі використовують адреси

з цього діапазону. Особливо це актуально для мереж діапазонів 192.168.0.0 і 192.168.1.0, тому краще вибрати для корпоративної мережі інший діапазон.

На першому контролері домену запускаємо Диспетчер сервера і додаємо роль DHCP-сервера (рис. 3.16):

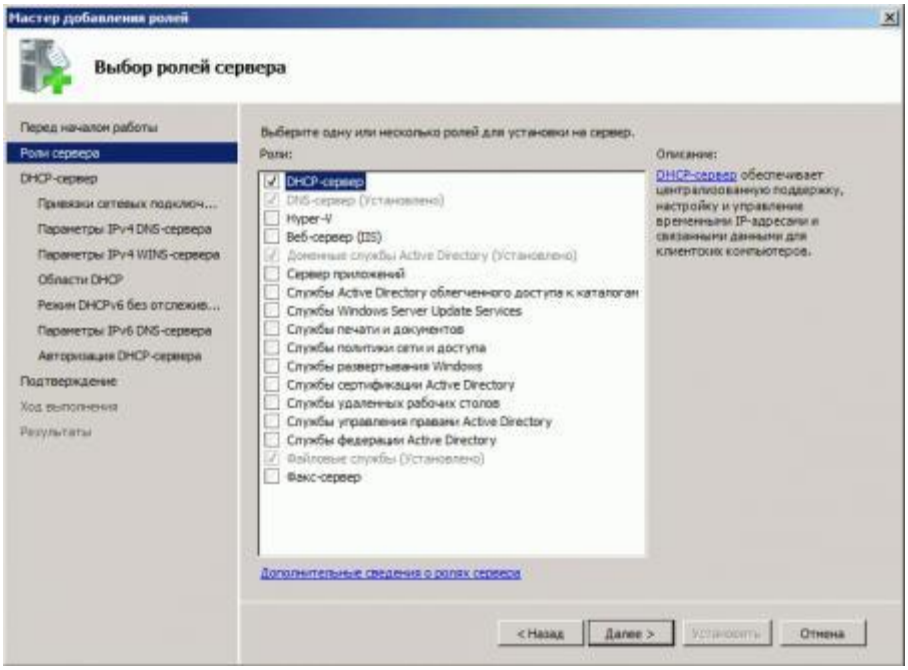

Рисунок 3.16 – Створення ролі DHCP-сервера

Як батьківський домен вказано домен AD, як DNS-серверів адреса контролера домену (рис. 3.17).

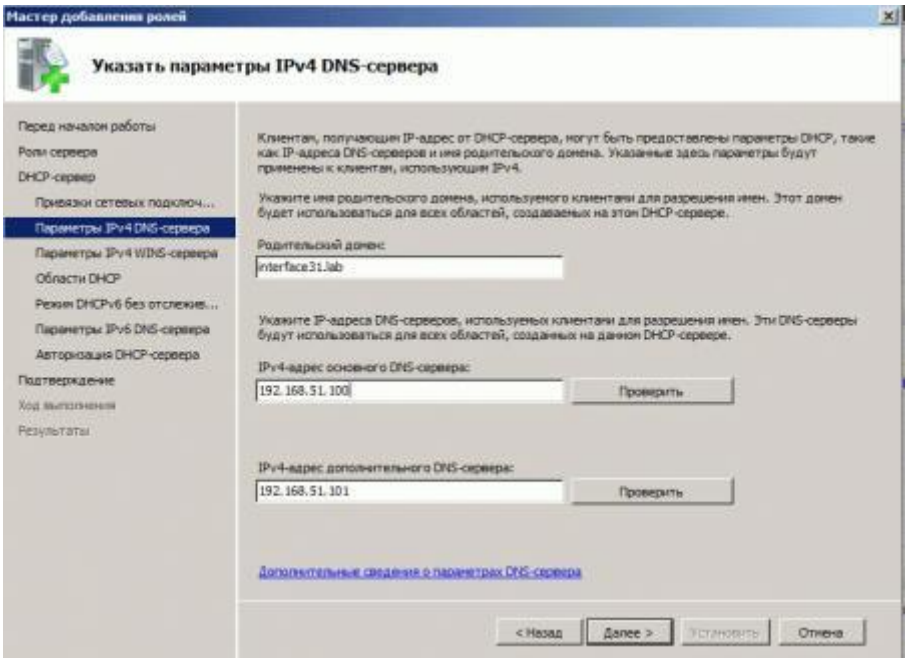

Рисунок 3.17 – Налаштування IPv4 DNS-сервера

Наступним кроком додаємо область, в налаштуваннях необхідно вказати повний діапазон адрес: 192.168.51.10-.192.168.51.253 (рис. 3.18).

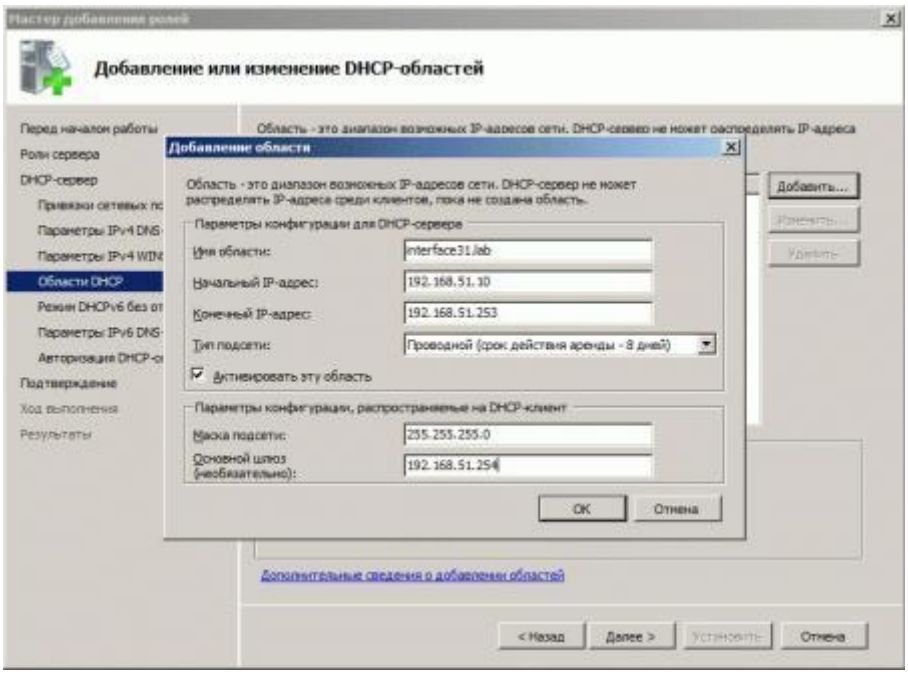

Рисунок 3.18 – Налаштування повного діапазону адрес

Потім DHCP-сервер потрібно авторизувати в AD, увійшли в систему як адміністратор домена додаткових дій не потрібно, інакше потрібно вказати облікові дані доменного адміністратора (рис. 3.19).

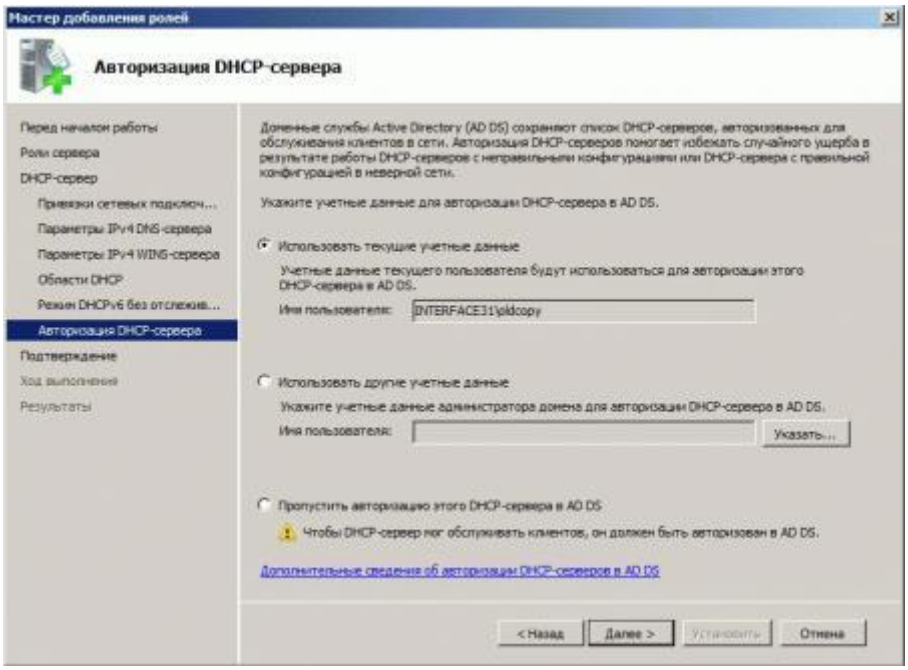

Рисунок 3.19 – Авторизація DHCP-сервера

Необхідно перевірити всі введені дані і встановити роль DHCP-сервера, перейти в оснастку управління цією роллю і задати діапазони виключення (рис. 3.20).

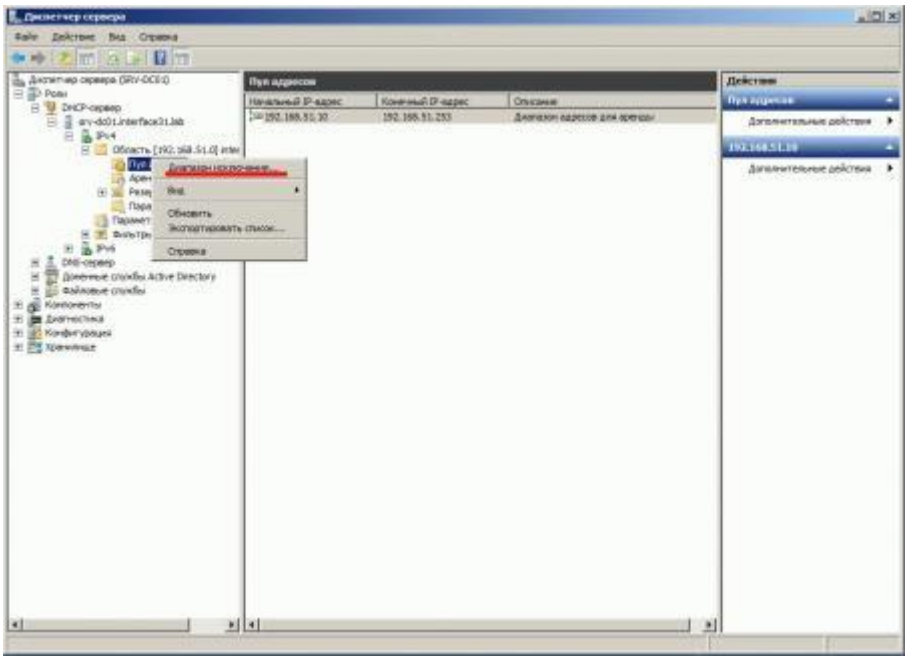

Рисунок 3.20 – Вікно параметрів серверу

В результаті повинно вийти налаштування зображене на рис. 3.21:

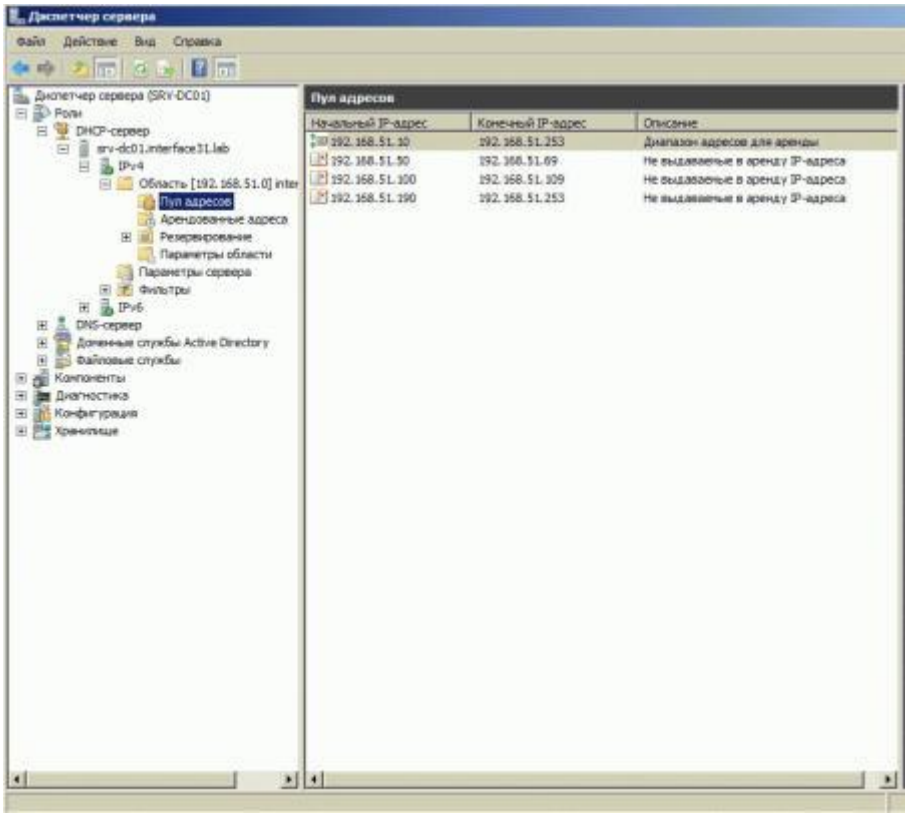

Рисунок 3.21 – Налаштовані виключені діапазони IP-адрес

Тепер аналогічним чином додаємо і налаштовуємо роль DHCP на другому контролері домену. Налаштуванню області особливої уваги не приділяємо, все одно її доведеться видалити (рис. 3.22):

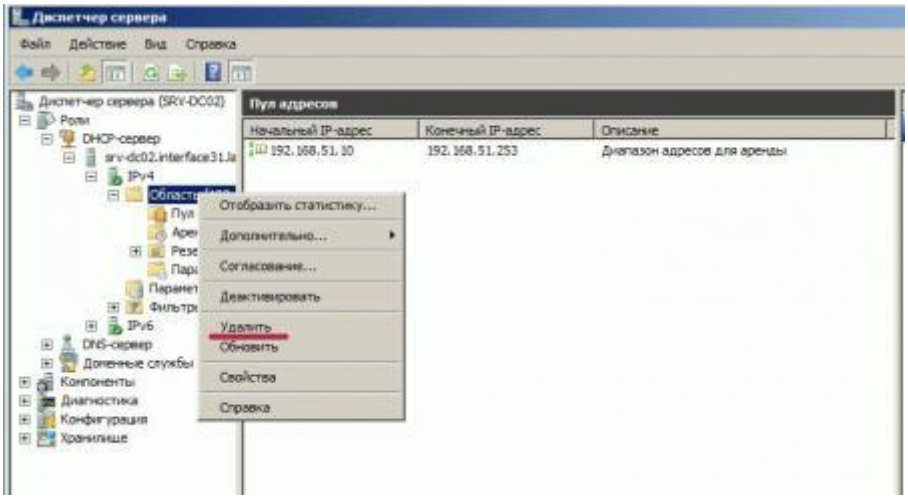

Рисунок 3.22 – Видалення налаштувань області

На другому контролері домену видаляємо створену область і знову переходимо на перший контролер домену. Необхідно відкрити DHCP-області і обрати Розділені області (рис. 3.23).

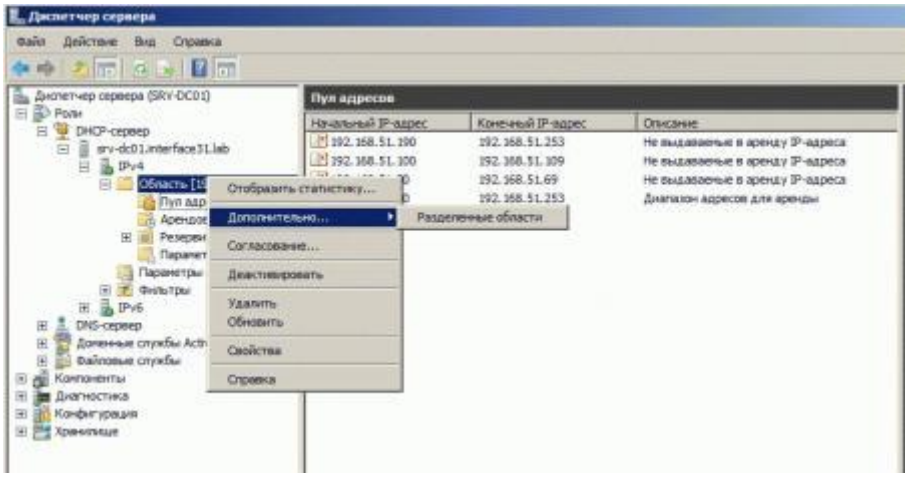

Рисунок 3.23 – Контекстне меню DHCP-області

У відкритому майстрі конфігурацій потрібно вибирати додатковий (другий) DHCP-сервер (рис. 3.24):

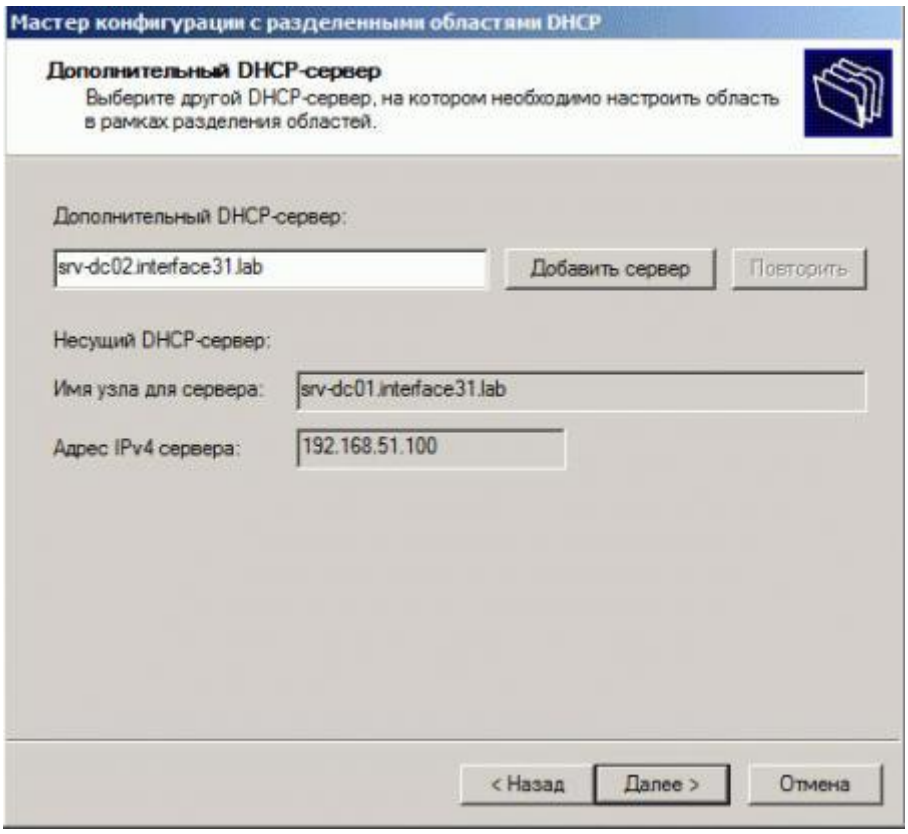

Рисунок 3.24 – Майстер конфігурацій с розділеними областями DHCP

Нербхідно вказати пропорції в яких слід розгорнути область. Більш точні налаштування можна задати вручну (рис. 3.25).

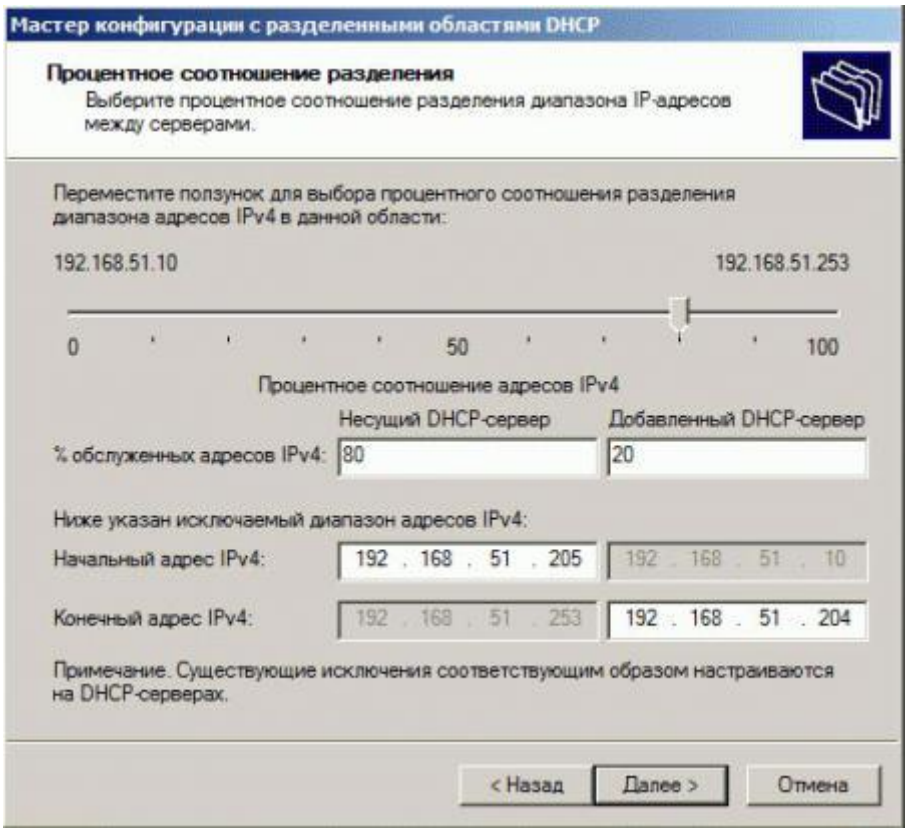

Рисунок 3.25 – Налаштування області DHCP-серверу

Потрібно вказати затримки відповіді серверів, так як перший сервер основний, то було зазначено для другого сервера затримку в 10 мс, це дозволить видавати всі адреси першим сервером, використовуючи другий тільки при відмові першого або заповненні його пулу адрес (рис. 3.26).

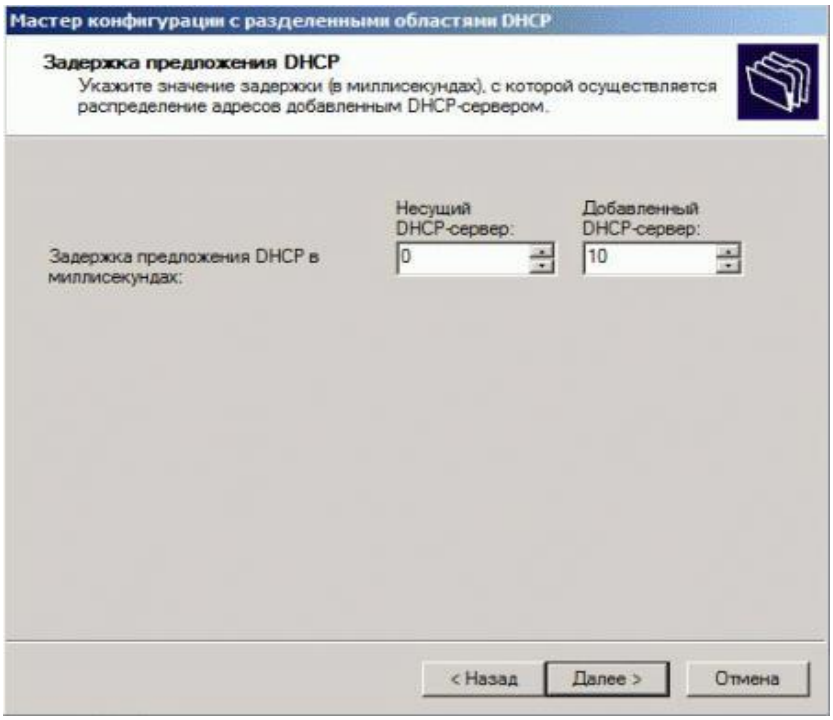

Рисунок 3.26 – Налаштування затримки відповіді DHCP-серверу

Після закінчення роботи майстра область буде розділена і на першому сервері вона набуде вигляду, як на рисунку 3.27:

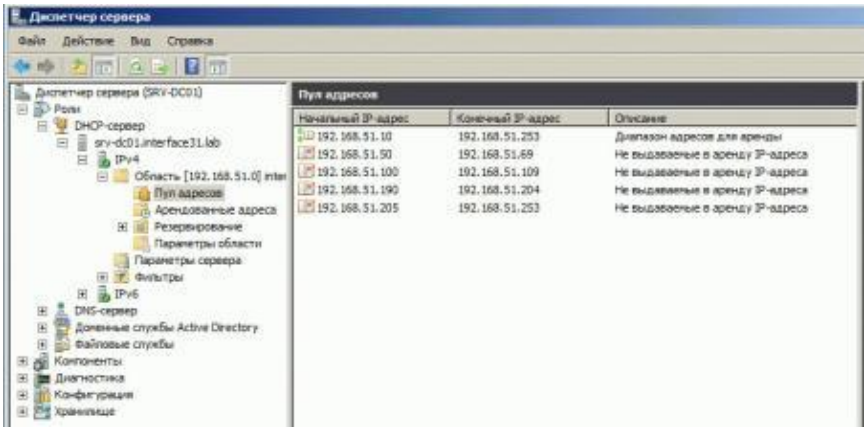

Рисунок 3.27 – Розділена область DHCP-серверу

На другому сервері, доведеться видалити зайвий діапазон виключення вручну, щоб діапазони не конфліктували (рис. 3.28):

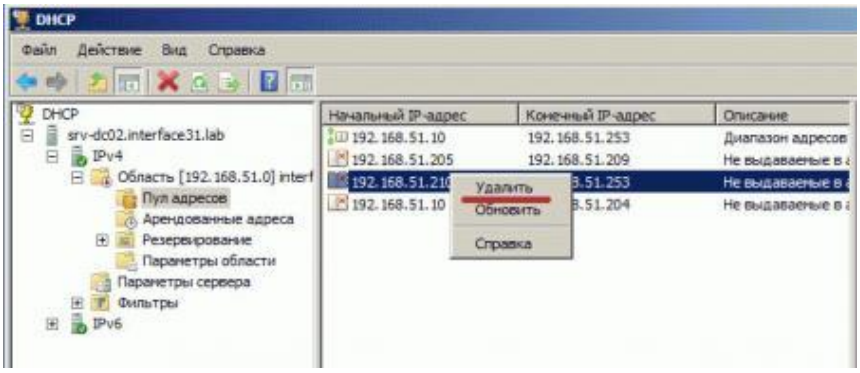

Рисунок 3.28 – Видалення непотрібного діапазону

Переконавшись що обидва сервера обслуговують непересічні частини області, необхідно активувати область на другому сервері (рис. 3.29):

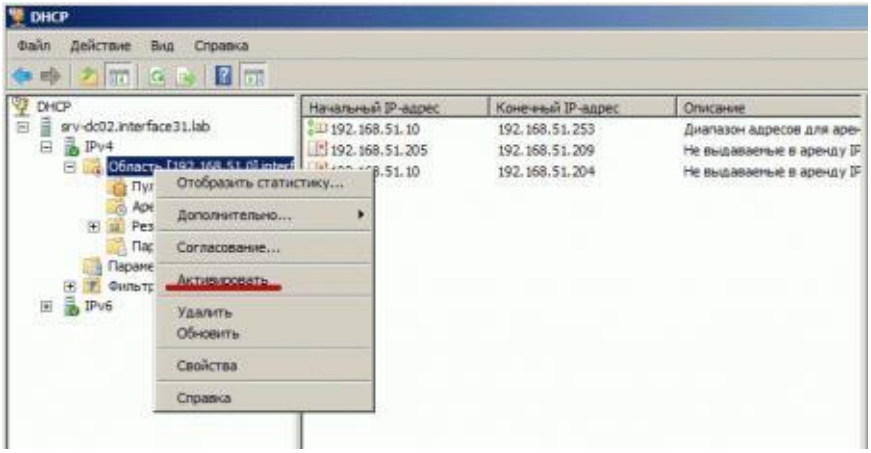

Рисунок 3.29 – Активування області IP-адресс

У разі відмови або виводу на профілактику основного DHCP-сервера, другий сервер обробить запити клієнтів з орендою адреси яка закінчується (за умовчанням 8 днів), якщо основний сервер вибув на більший термін, то на додатковому DHCP-сервері необхідно розширити пул адрес, в подальшому зробивши даний сервер основним, а інший сервер додатковим.

У будь-якому випадку даний підхід дозволяє забезпечити безперебійне функціонування мережевої інфраструктури незалежно від працездатності окремих вузлів.

3.4 Перенесення облікових записів в домен

Отже, є робоча станція за якою працює співробітник, яку потрібно ввести в домен. В першу чергу необхідно переконатися що ПК має бажане ім'я і при необхідності перейменувати комп'ютер, а також перезавантажитися. Необхідно правильно налаштувати мережу, так як в мережі розгорнутий DHCP-сервер, досить встановити автоматичне отримання мережевих параметрів і переконатися в отриманні правильних значень (рис. 3.30).

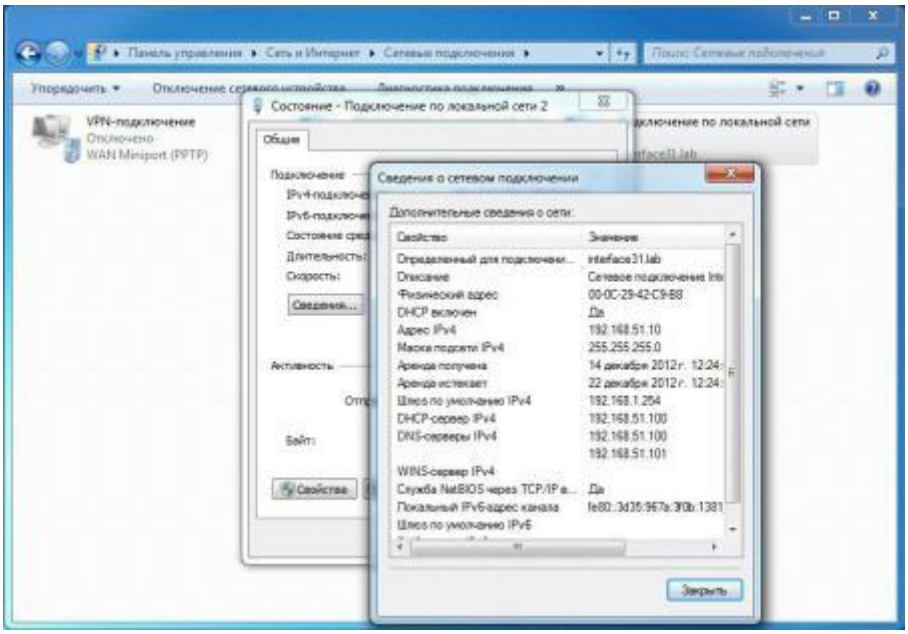

Рисунок 3.30 – Перевірка мережевих параметрів

Для серверів, які повинні мати статичні мережеві параметри необхідно вказати необхідні значення вручну, особливу увагу слід приділити DNS-серверам, це повинні бути адреси двох будь-яких контролерів домену (які поєднують роль DNS-сервера), в іншому випадку не вийде ввести такий комп'ютер в домен.

Якщо потрібно щоб будь-яка робоча станція мала статичну адреса, то не варто вказувати його вручну, правильно буде використовувати таку функцію DHCP-сервера як резервування. Це дозволить в подальшому змінювати налаштування мережі без необхідності вносити зміни на кожній робочій станції

(наприклад поміняти адресу шлюзу). Для резервування потрібно відкрити «оснащення управління DHCP-сервером», перейти в папку «Орендовані адреси» та клацнути на потрібному хості правою кнопкою миші, вибрати «Додати до резервування». Цими діями виділена адреса закріпиться за комп'ютером на постійній основі (рис. 3.31).

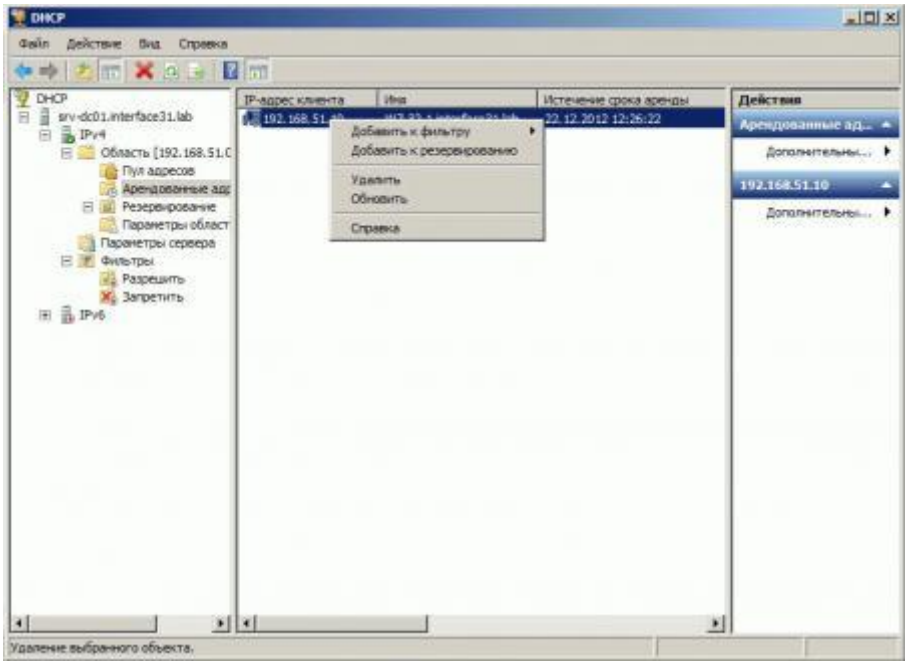

Рисунок 3.31 – Закріплення IP-адреси за обраною робочою станцією

На даному етапі необхідно включити комп'ютер в домен. Для цього потрібно перейти в «Свойства системы - Имя компьютера» і натиснути кнопку «Изменить», вибрати «Является членом домена» і вказати ім'я домену в який потрібно увійти, натиснути ОК, та вказати ім'я та пароль користувача який має право на включення комп'ютера в домен (за замовчуванням адміністратор домену)(рис. 3.32).

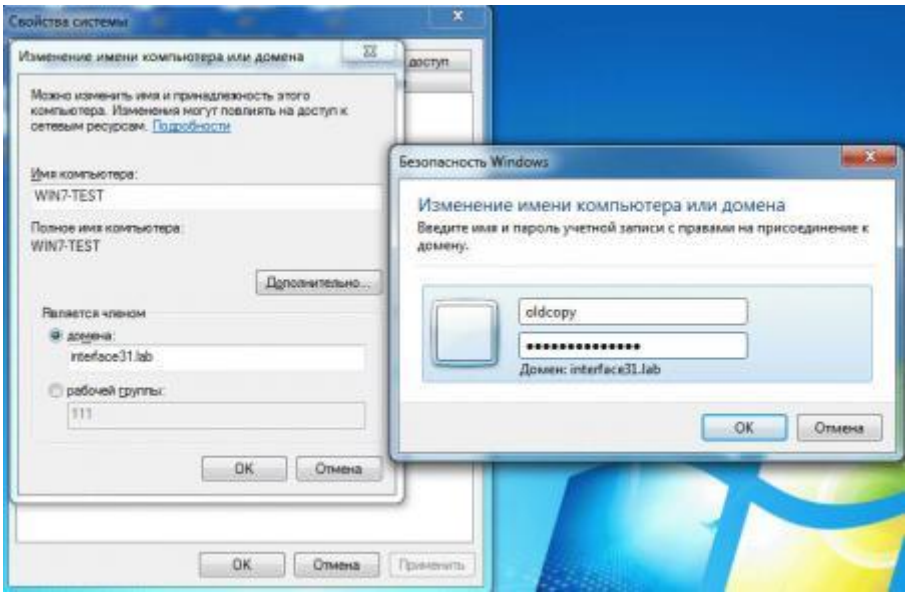

Рисунок 3.32 – Додавання комп’ютеру в домен

Після перезавантаження можна увійти під доменним обліковим записом, який потрібно попередньо створити на будь-якому з контролерів домену. Для цього потрібно відкрити оснащення «Active Directory - пользователи и компьютеры», перейти в папку «User» і створити там нового користувача (рис. 3.33).

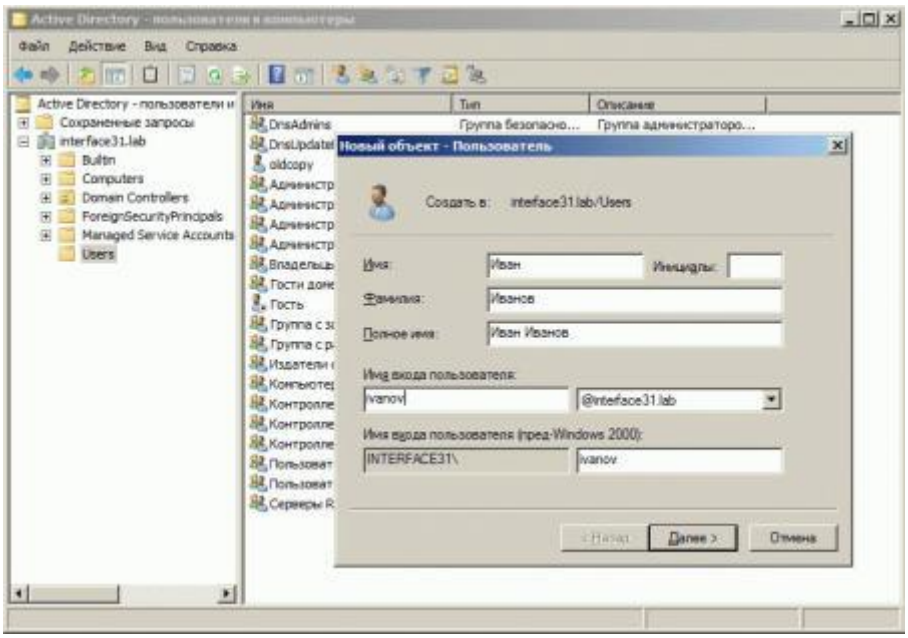

Рисунок 3.33 – Створення нового користувача

В систему можна увійти під ім'ям нового користувача. І переконатися в тому, що працюючи під локальним обліковим записом користувач мав звичним чином розташовані файли, папки і ярлики, програми були відповідним чином налаштовані, крім того мінявся обліковий запис пошти, закладки браузера і т.д. Був отриманий чистий профіль, який необхідно налаштовувати заново (рис 3.34).

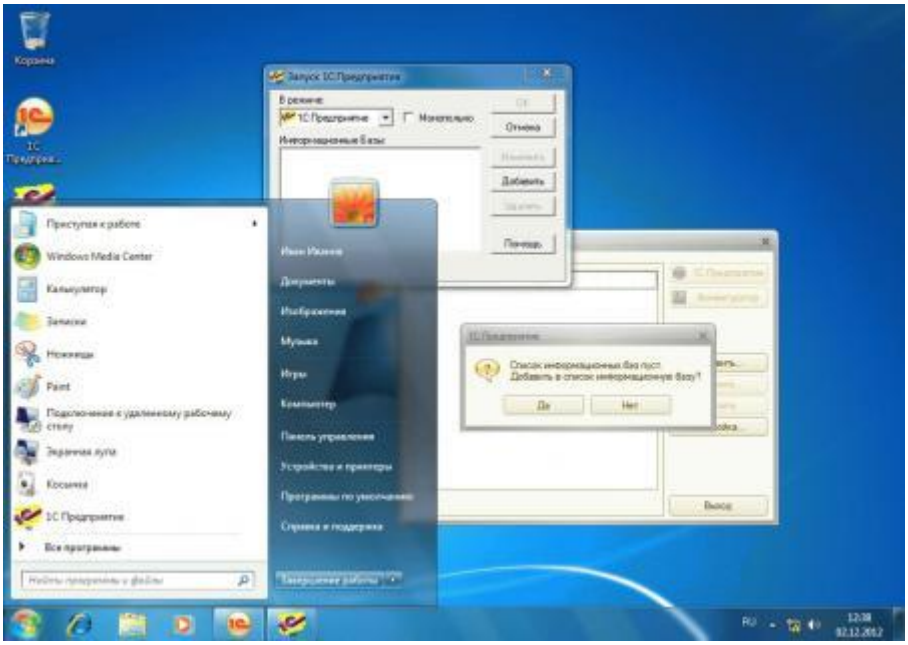

Рисунок 3.34 – Вигляд тільки-но створеного користувача

На цьому єтапі необхідно перенести профіль локального облікового запису в доменний. Для цього було використано інструмент User State Migration Tool, який входить до складу Пакета автоматичної установки Windows (AIK), так як даний пакет немає необхідності встановлювати на всіх ПК, цілком достатньо буде установки на комп'ютер адміністратора або один з серверів. Цей набір утиліт знаходиться в папці C: \ Program Files \ Windows AIK \ Tools \ USMT потрібно скопіювати їх на цільову систему або зробити доступними по мережі (рис. 3.35).

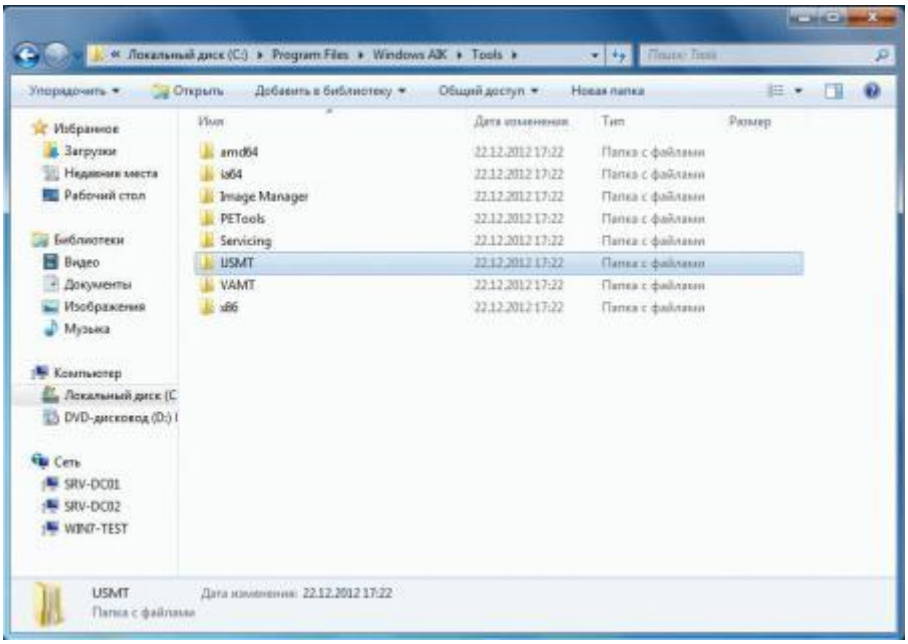

Рисунок 3.35 – Знаходження набору утиліт

Процес перенесення профілю складається з двох етапів: створення файлу перенесення з даними і параметрами зазначеного користувача і відновлення профілю з файлу перенесення, причому зробити це можна на будь-якому ПК, що дозволяє швидко перенести профіль з одного ПК на інший при заміні комп'ютера. Але необхідно пам’ятати, що можна перенести профіль з 32-х розрядної системи в 64-х розрядну, однак зворотній перенос з 64-х розрядної в 32-х розрядну неможливий.

Для створення файлу перенесення використовувалась утиліта ScanState. У цьому випадку буде переноситись локальний профіль користувача WWW в профіль доменного користувача ivanov. Для створення файлу перенесення необхідно увійти в систему під обліковим записом адміністратора домену, перейти в папку з потрібною версією USMT (32 або 64 біт) і виконати наступну команду: scanstate C: \ Migration \ User /i:miguser.xml /i:migapp.xml / v: 13 / ue: * \ * / ui: WWW /l:C:\Migration\scan.log

Синтаксис команди переводиться як: перший аргумент вказує розташування файлу перенесення, ключ / i: вказує які правила перенесення слід використовувати, ключ / v: задає необхідний рівень деталізації лога, поєднання ключів / ue: і / ui:

виключає з перенесення всіх користувачів окрім WWW, а ключ / l: визначає розташування балки.

Результатом виконання команди буде короткий звіт який зображений на рисунку 3.36:

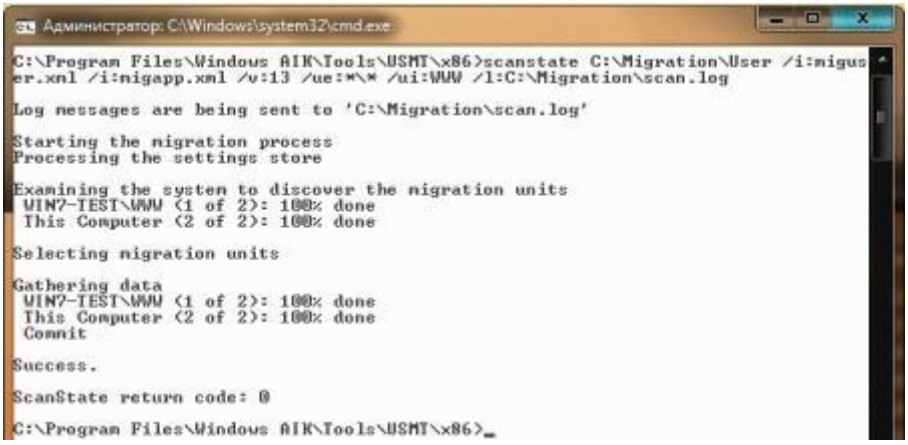

Рисунок 3.36 – Звіт команди scanstate

Файл перенесення створений, але так як в цю систему вже здійснювався вхід під цільовим користувачем, то необхідно видалити або перейменувати папку з профілем в каталозі C: \ Users і видалити відповідний профілю розділ в гілці реєстру: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ ProfileList (рис. 3.37)

Так як в іншому випадку при спробі відновлення профілю буде отримано помилку з кодом 71: LoadState return code: 71.

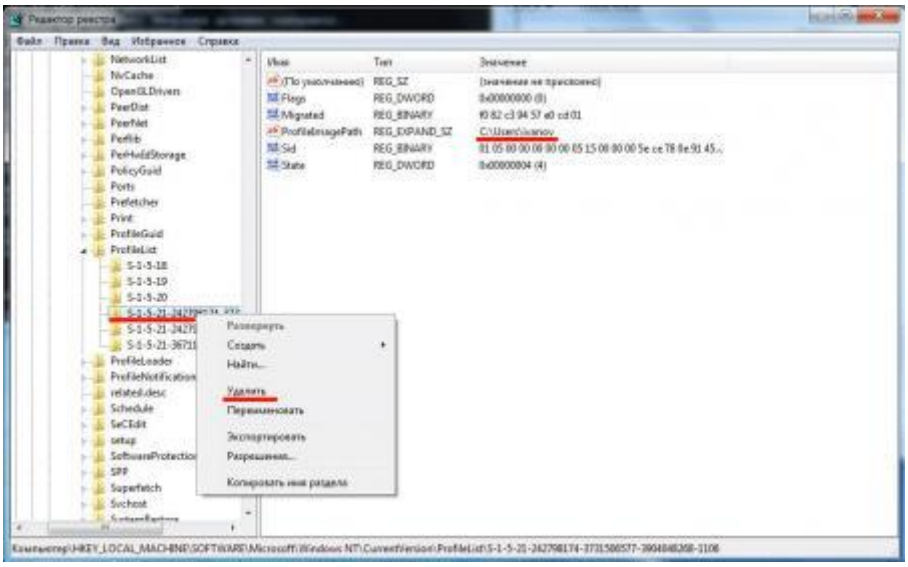

Рисунок 3.37 – Видалення профілю в редакторі реєстру

Відновлення профілю буде виконано за допомогою утиліти LoadState. Для перенесення профілю необхідно використати наступну команду: loadstate C: \ Migration \ User /i:miguser.xml /i:migapp.xml / v: 13 /mu:WWW:interface31.lab\ivanov /l:C:\Migration\load.log

Структура команди багато в чому схожа на попередню, однойменні ключі мають аналогічне значення, ключ / mu: вказує вихідний профіль і профіль призначення, доменні облікові записи вказуються як Domain \ User. У цьому випадку профіль локального користувача WWW буде відновлений в профіль користувача interface31.lab \ ivanov (рис. 3.38).

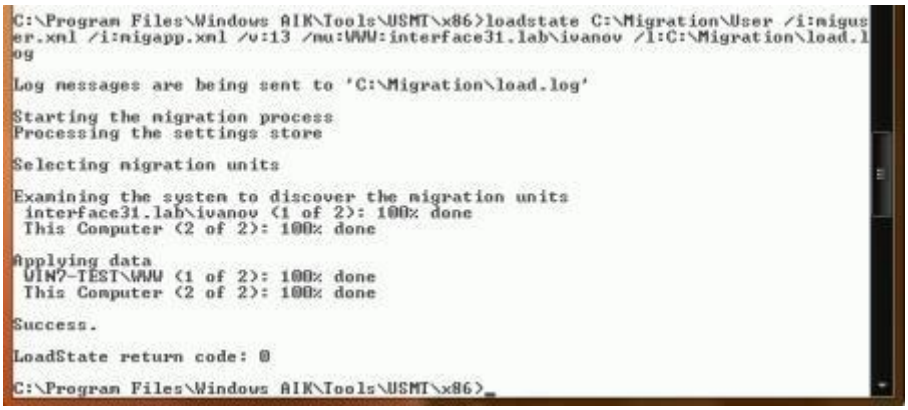

Рисунок 3.38 – Звіт команди loadstate

Тепер, ввійшовши під доменним обліковим записом користувач виявить звичне робоче оточення, як видно на рисунку 3.39, переноситься навіть вміст кошика.

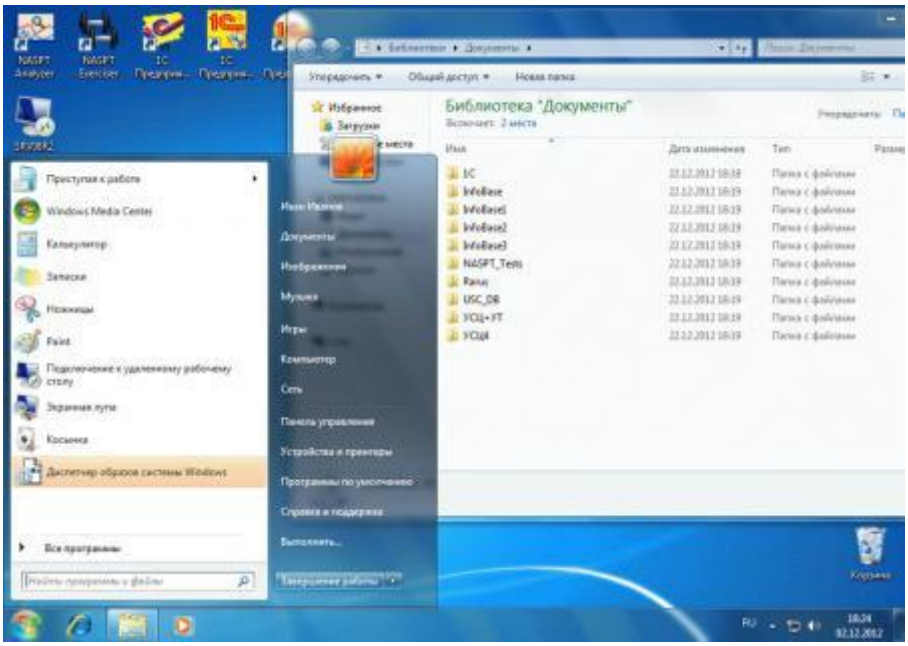

Рисунок 3.39 – Вигляд перенесеного профілю

Даний метод можна використовувати для операційних систем Windows Vista / 7, для перенесення профілів в середовищі Windows XP також можна використовувати USMT дещо змінивши синтаксис команд, але краще скористатися утилітою moveuser, яка входить до складу Windows Server 2003 Resource Kit Tools. Необхідності встановлювати пакет на кожну машину немає, достатньо скопіювати утиліту moveuser яка знаходиться в папці C: \ Program Files \ Windows Resource Kits \ Tools (рис. 3.40).

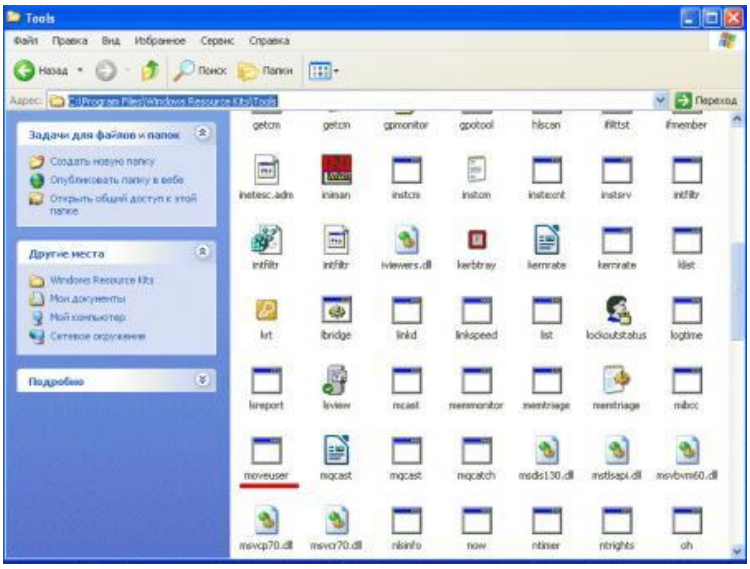

Рисунок 3.40 – Знаходження утіліти moveuser

Для перенесення профілю необхідно увійти на цільовий ПК як адміністратор домена і виконати команду: moveuser www interface31.lab\ petrov / y (рис. 3.41)

Синтаксис даної утиліти набагато простіше. Ключ /y дозволяє перезаписати профіль навідь якщо він існує, тобто можна попередньо виконати вхід доменним користувачем на цю машину, це ніяк не завадить переносу, після перенесення вхід під локальним користувачем буде неможливий, якщо необхідно використовувати локальний профіль, потрібно додатково вказати ключ / k.

Рисунок 3.41 – Виконання команди moveuser

Виконаємо вхід під доменної записом користувача Петров і переконаємося що він може продовжувати роботу в домені зі звичним робочим оточенням (рис 3.42).

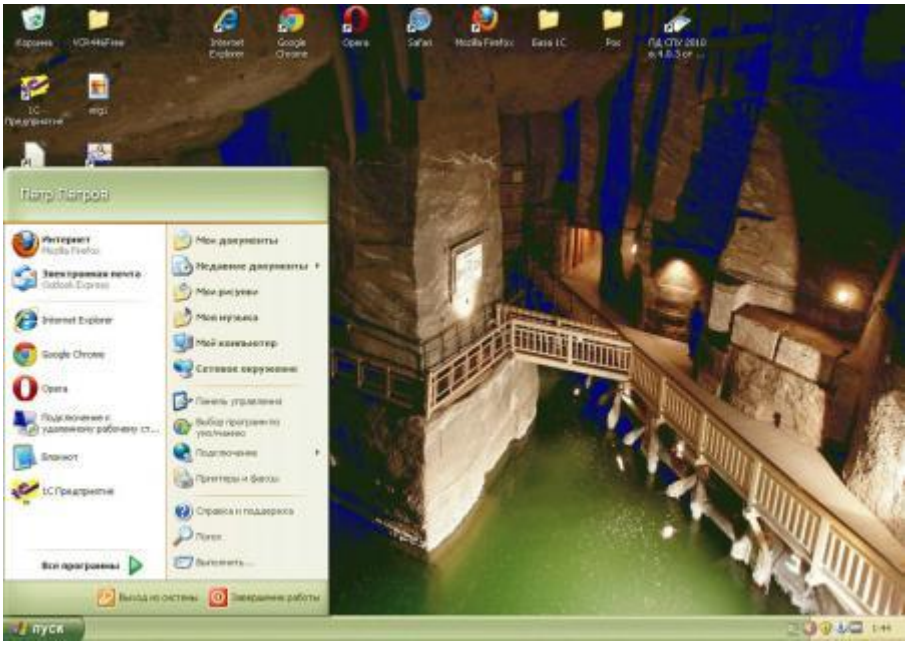

Рисунок 3.42 – Робочий стіл користувача після переносу профілю

ВИСНОВКИ

В ході виконання магістерської роботи було розглянуто основні методи підвищення функціонування корпоративної мережі. Була побудована модель інформаційно-телекомунікаційної системи (інфраструктури) підприємства з використанням локальних корпоративних доменів, що управляються за допомогою контролеру домену, а саме компонента Active Directory.

Active Directory було обрано як основний інструмент через його широко профільний фунціонал, гнучкість та можливість локального налаштування політик для різних вимог користувачів.

Практична значущість роботи полягає в реалізації на практиці заходів з проектування та налагодженню доступу до загальних ресурсів локальної мережі, таким як спільне використання мережевих папок, а також для розділення різних підрозділів всередині корпоративної мережі.

В ході реалізації було виконано наступні дії: аналіз існуючих технологій, підбір апаратно-програмних засобів, налаштування обладнання.

Після виконання даної роботи, було виявлено, що цю мережу можна легко проектувати, просте розширення, висока та стабільна робота сервісів та захист інформації. Дану мережу можна використовувати у будь-яких фірмах від малого великого бізнесу. Простий та зручний інтерфейс дає можливість керувати даними користувачів без прямої взаємодії з ними, що в наш час дуже актуально.