МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Секція інформаційно-комунікаційних технологій

ВИПУСКНА РОБОТА

на тему:

«Сервер система на базі технологій Active Directory»

Завідувач
випускаючої кафедри **Довбиш А. С.**

Керівник роботи **Власенко О. В.**

Студента групи КБ-61 **Волик А.В.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

«_____» _____2020 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-61 спеціальності «Кібербезпека» денної форми навчання Волика Андрія Вікторовича.

Тема: «Сервер система на базі технологій Active Directory»

Затверджена наказом по СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки: 1) інформаційний огляд; 2) постановка задачі та опис інструменту вирішення поставлених задач; 3) практична реалізація.

Дата видачі завдання «_____»_____2020 р.

Керівник випускної роботи _____ Власенко О.В.

Завдання прийняв до виконання _____ Волик А.В.

РЕФЕРАТ

Записка: 78 стор., 39 рис., 3 табл.,1 додаток, 17 джерел.

Мета роботи – дослідити основні аспекти створення сервер-системи на основі технології Active Directory.

Об’єкт дослідження – функціонування сервер-системи на базі технології Active Directory.

Предмет дослідження – технологія Active Directory.

Методи роботи – теоретично-критичний аналіз літератури з теми дослідження; зіставлення, узагальнення і синтезування здобутої інформації.

Результати – розроблено алгоритм послідовності дій розгортання серверу, було виконано тестове розгортання розробленої моделі каталогу Active Directory на базі серверної операційної системи Windows Server 2016 для центрального офісу компанії.

ACTIVE DIRECTORY, СЕРВЕР СИСТЕМА, DNS,
ДОМЕН,ЛІС, БАЗИ ДАНИХ LDAP

ЗМІСТ

ВСТУП

Актуальність роботи. У комп'ютерній мережі корпорації взаємодіє величезна кількість об'єктів, зокрема, файлові сервери, принтери, факс-сервери, додатки, бази даних, користувачі тощо. Для забезпечення надійної роботи і зберігання інформації необхідні спеціальні структури у вигляді каталогів.

Служба каталогу (directory service) забезпечує зберігання інформації у одному місці для зручного використання і керування нею, крім того, надає зручний доступ до відомостей про різні об'єкти мережі, допомагаючи користувачам і додаткам у пошуку цих же об'єктів. 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.

Служби Active Directory (служби активного каталогу) – це служба каталогів для використання в середовищі Windows Server, розподілена, ієрархічна структура бази даних, яка обмінюється інформацією про інфраструктуру для розміщення, захисту, управління та організації комп'ютерних та мережевих ресурсів. Active Directory – це власна служба каталогів Microsoft, яка використовується у доменних мережах Windows. Він надає функції аутентифікації та авторизації, а також надає можливості для інших таких послуг. Сам каталог – це база даних LDAP (легкий протокол доступу до каталогу), яка містить мережеві об'єкти. Active Directory використовує операційну систему Windows Server [1].

Метою роботи є дослідження основних аспектів створення сервер системи на базі технології Active Directory.

1. ЛІТЕРАТУРНИЙ ОГЛЯД

1.1 Загальне визначення серверу

Сервер – це програмне забезпечення або апаратний пристрій, що приймає і відповідає на запити, які виконані через локальну мережу або Інтернет. Пристрій, який робить запит і отримує відповідь від сервера, називається клієнтом. У мережі Інтернеті термін «сервер» зазвичай відноситься до комп’ютерної системи, яка отримує запит на веб-документ, і надсилає відповідь на запит клієнту. Більшість часу працює в автономному режимі, без втручання адміністратором. Існує багато типів серверів, включаючи веб-сервери, поштові сервери або файлові сервери. Кожен тип працює з програмним забезпеченням, яке є специфічним у залежності від призначення сервера [2, 3].

У якості серверу може бути використаний звичайний персональний комп’ютер, додавши відповідне програмне забезпечення. Проте великі підприємства використовують спеціально розроблене обладнання, яке розміщають на стійку. Ці системи, часто розміром 1U, займають мінімальний простір і мають додаткові корисні функції, такі як світлодіодні світильники стану та відсіки жорсткого диска з можливістю заміни. Кілька серверів, що встановлюються в стійку, можуть управлятись одними і тими ж моніторами та пристроями введення. Більшість серверів отримують доступ дистанційно за допомогою програмного забезпечення віддаленого доступу, тому пристрої введення часто навіть не потрібні [3].

Приклади серверних операційних систем:

1. Сервери Microsoft Windows;
2. Сервери Linux / Unix;
3. Хмарні або віртуальні сервери, які розміщені у відкритій мережі (хмарна платформа Google, Microsoft Azure та IBM Cloud) [1].

Для кожної з операційних систем існують спеціальні служби каталогів, які допомагають в управлінні. Розглянемо найбільш популярні з них.

1.2 Active Directory для Microsoft Windows

Active Directory – це база даних спеціального призначення. Каталог розроблений для обробки великої кількості операцій з читання та пошуку та значно меншої кількості змін та оновлень. Дані Active Directory є ієрархічними, масштабуються та розширюються. Типові приклади даних, які можуть зберігаються у каталозі – це дані черги друку принтера, дані контактів користувача та дані конфігурації мережі / комп'ютера. База даних Active Directory складається з об'єктів і атрибутів. У свою чергу об'єкти та визначення атрибутів зберігаються у схемі Active Directory.

Active Directory має три розділи: домен, схема та конфігурація. Розділ домену містить користувачів, групи, контакти, комп'ютери, організаційні підрозділи тощо. Оскільки Active Directory масштабується, існує можливість додавати власні класи та / або атрибути. Розділ схеми містить визначення класів та атрибутів. Конфігураційний розділ містить дані конфігурації для служб, розділів та сайтів [4]. На рисунку 1.1 показано розділ домену Active Directory:

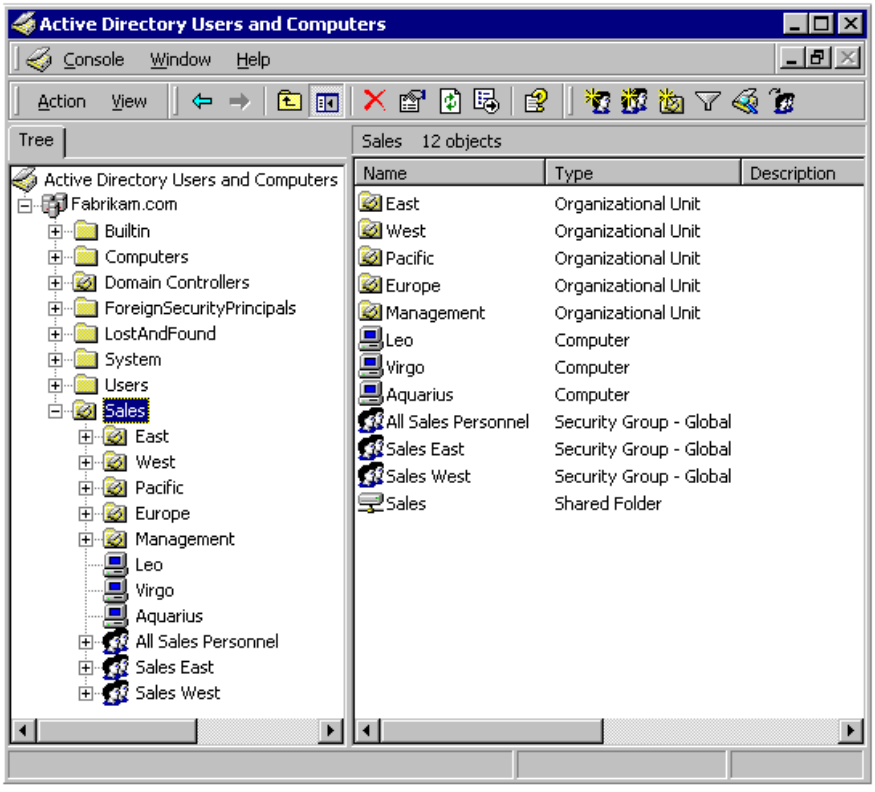


Рисунок 1.1 – Приклад розділу «Домен» Active Directory [4]

Контролер домену перевіряє ідентичність та авторизацію усіх користувачів і комп'ютерів в мережі типу домену Windows, призначення і застосування політик безпеки для всіх комп'ютерів і установка або оновлення програмного забезпечення. Наприклад, коли користувач входить у комп'ютер, що входить у домен Windows, відбувається перевірка паролю і відбувається перевірка типу користувача, тобто системний адміністратор це або звичайний користувач. У роботі використовується протокол LDAP версії 2 і 3, і версія Microsoft Kerberos і DNS.

1.3 Zentyal для Linux

Zentyal – це вбудована реалізація Microsoft Active Directory на Linux, що включає всі мережеві служби, необхідні для середовища малого і середнього бізнесу: Directory & Domain Server, Mail Server, Gateway і Infrastructure Server. Zentyal включає стандартні поштові сервери SMTP та POP3 / IMAP, побудовані на основі найбільш відомих технологій та протоколів. Надає можливість розгортати Zentyal як поштовий сервер, сервер домена та каталог з поштою або все на одному сервері. Дозволяє уніфікувати та легко керувати усіма основними послугами мережевої інфраструктури та пропонувати надійний та безпечний доступ до Інтернету. Він охоплює послуги від DNS/DHCP, CA, VPN та резервного копіювання до шлюзу, брандмауера та HTTP-проксі.

1.4 Хмарний сервер Microsoft Azure

Microsoft Azure – це публічна платформа хмарних обчислень – з рішеннями, що включають інфраструктуру як послугу (IaaS), платформу як послугу (PaaS) та програмне забезпечення як послугу (SaaS), які можна використовувати для таких служб, як аналітика, віртуальна обчислювальна техніка, сховище, мережа та багато іншого. Його можна використовувати для заміни або доповнення локальних серверів.

Azure може інтегруватися з Active Directory для доповнення ідентичності та можливостей доступу, а у свою чергу надає DNS глобальний доступ, централізоване управління та надійну безпеку. Жоден інший постачальник хмарних послуг не має можливості розширити сферу дії контролера домену та консолідувати управління AD, як Azure.

Якщо є кілька локацій або використовуються додаткові додатки або хмарні додатки, такі як Microsoft 365, інтеграція Active Directory з Azure стане центральним інструментом для управління та підтримки доступу до всіх цих інструментів.

Azure також дозволяє використовувати багатофакторну автентифікацію, додаючи новий рівень безпеки даним та програмам з мінімальними клопотами для користувачів. Існує можливість здійснити єдиний вхід хмарних додатків для Windows, Mac, Android та iOS.

1.5 Обґрунтування вибору інструмента для роботи

Для виконання випускної роботи було вирішено обрати саме Active Directory, тому що її служби мають широкі можливості масштабування. У лісі Active Directory може бути створене більш 2-х мільярдів об’єктів, що дозволяє впроваджувати службу каталогів у компаніях із сотнями тисяч комп’ютерів і користувачів. Ієрархічна структура доменів дозволяє гнучко масштабувати інфраструктуру на всі філії й регіональні підрозділи компаній. Для кожної філії або підрозділу компанії може бути створений окремий домен, зі своїми політиками, своїми користувачами й групами. Для кожного дочірнього домену можуть бути делеговані адміністративні повноваження місцевим системним адміністраторам. При цьому однаково дочірні домени підкоряються батьківським.

Крім того, служби Active Directory дозволяють налаштувати доступ до корпоративних ресурсів співробітникам іншої компанії – робота із загальними документами й додатками у рамках спільного проекту. Для цього між лісами

організацій можна налаштувати довірчі відносини, що дозволить співробітникам однієї організації авторизуватися в домені іншої.

При використанні домену Active Directory усі облікові записи користувачів зберігаються в одній базі даних, і всі комп'ютери звертаються до неї за авторизацією. Усі користувачі домену включаються у відповідні групи, наприклад, «Бухгалтерія», «Фінансово-плановий відділ». Досить один раз надати дозвіл для тих або інших груп, і всі користувачі отримають відповідний доступ до документів і додатків. Якщо в компанію приходить новий співробітник, для нього створюється обліковий запис, який включається у відповідну групу, – співробітник отримує доступ до всіх ресурсів мережі цієї групи.

У робочій групі всі комп'ютери рівноправні і жоден з комп'ютерів не може управляти іншим. При використанні єдиного каталогу Active Directory, усі користувачі й комп'ютери ієрархічно розподіляються по організаційних підрозділах, до кожного з яких застосовуються єдині групові політики, що задають єдині налаштування й параметри безпеки для групи комп'ютерів і користувачів. За допомогою політики можна централізовано призначити користувачам мережні принтери, установити необхідні додатки, задати параметри безпеки браузера тощо.

Найбільшою перевагою служб Active Directory є відповідність стандарту LDAP, який підтримується іншими системами, наприклад, поштовими серверами (Exchange Server), проксі-серверами (ISA Server, TMG). Причому це не обов'язково тільки продукти Microsoft. Наприклад, у випадку повної відмови сервера Exchange, уся його конфігурація залишиться незмінною. Для відновлення працездатності корпоративної пошти, досить буде переустановити Exchange Server у режимі відновлення.

2. МЕТОДИКА ВИРІШЕННЯ ПОСТАВЛЕНИХ ЗАДАЧ

Відповідно до мети роботи були визначені наступні завдання:

1) дати загально-теоретичну характеристику системи Active Directory;

2) провести дослідження особливостей створення сервер системи на базі технології Active Directory;

3) визначити ефективність реалізації запропонованих заходів.

2.1. Поняття та сутність системи Active Directory (AD)

Основними функціями AD є: інформаційна довідка про об’єкти та їх організація, керування доступом до об’єктів, встановлення правил безпеки. Кожний об’єкт має унікальний ідентифікатор назви та набір атрибутів:

- характеристики;
- даних, які об’єкт може містити, що залежать від типу об’єкта.

Атрибути є складовою базової структури об’єкта і визначаються схемою AD. Схема визначає, які типи об’єктів можуть існувати і складається з двох типів об’єктів схеми:

- класи;
- атрибути.

Один клас схеми визначає один тип об’єкта, а один атрибут схеми визначає атрибут, який об’єкт може мати [5]. Кожен атрибут може бути використаний у декількох різних класах схеми та дозволяють змінювати і доповнювати схему, у разі необхідності. Проте, кожен об’єкт схеми є частиною визначень об’єктів AD, тому деактивація або зміна цих об’єктів можуть мати серйозні наслідки, тому що в результаті цих дій буде змінена структура AD. Зміна об’єкта схеми виконується автоматично та створений об’єкт схеми не може бути видалений, його можна лише деактивувати. Зазвичай всі зміни схеми ретельно плануються. Контейнер є аналогічним до об’єкта, на відміну від нього, може лише містити групу об’єктів або інші контейнери.

Верхнім рівнем структури AD є ліс – це сукупність одного або декількох дерев домену, які не мають спільного батьківського домену. Домени ідентифікуються своїми структурами імен DNS – просторами імен. Усі дерева лісу мають однакову схему, конфігурацію, глобальний каталог та пов'язані довірчими відносинами за протоколом Kerberos. На рисунку 2.1 представлено приклад діаграми лісів [6-8].

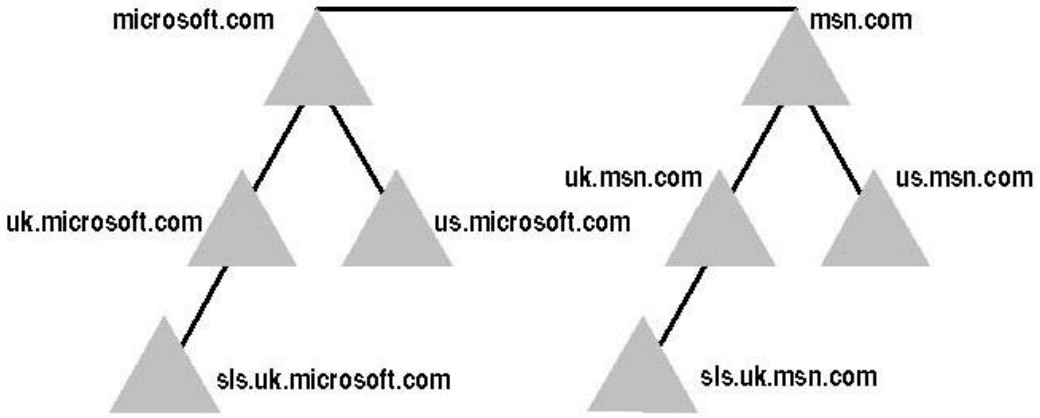


Рисунок 2.1 – Ліс дерев [8]

Об'єкти у домені можуть бути згруповані у підрозділи, які дозволяють створювати ієрархію всередині домену, спрощують його адміністрування і дозволяють моделювати організаційну та/або географічну структури компанії в AD. Підрозділ є найнижчим рівнем, на якому можуть делегуватися адміністративні повноваження (рис.2.2).

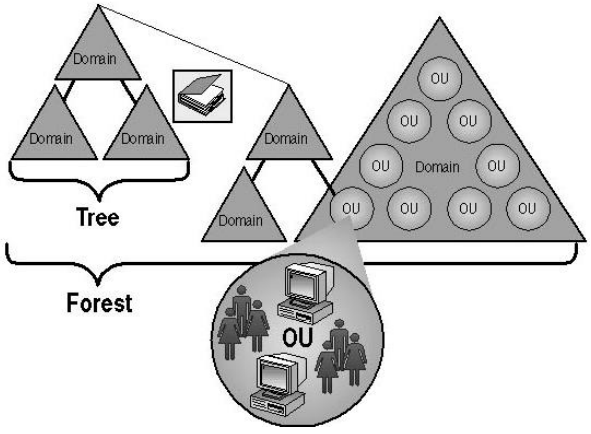


Рисунок 2.2 – Організація об'єктів у підрозділи [8]

Іншим способом поділу AD є сайти, які є способом фізичного групування на основі підмереж IP. Вони діляться на такі, що мають підключення низько швидкісними каналами або високошвидкісними. Сайт може мати один або декілька доменів, і навпаки. При проектуванні AD важливо враховувати мережевий трафік, що створюється при синхронізації даних між сайтами (рис.2.3).

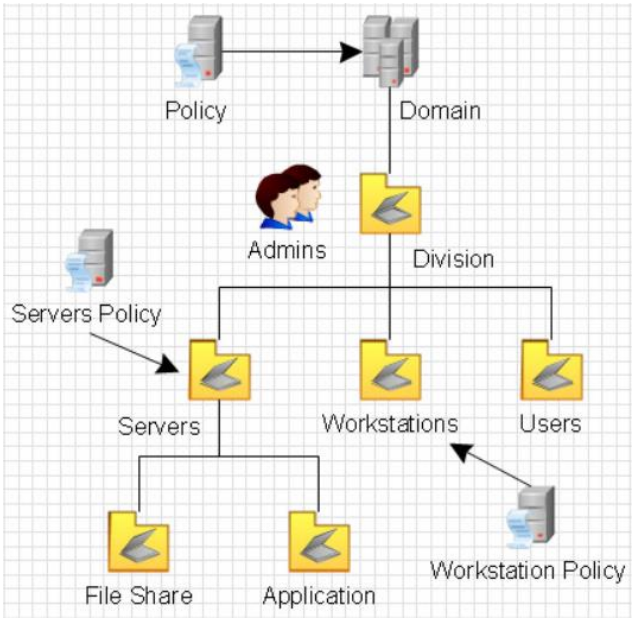


Рисунок 2.3 – Приклад організації структури через сайти [7]

Ключовим рішенням при проектуванні AD є рішення щодо поділу інформаційної інфраструктури на ієрархічні домени та підрозділи верхнього рівня. Типовими моделями, що використовуються для такого поділу, є моделі поділу за функціональними підрозділами компанії, за географічним розташуванням, і за ролями в інформаційній інфраструктурі компанії. Часто використовуються комбінації цих моделей.

Фізично інформація AD зберігається на одному або декількох рівнозначних контролерах доменів, які замінили основний і резервні контролери домену. Кожен контролер домену зберігає копію даних AD, призначену для читання та запису. Зміни, зроблені на одному контролері, синхронізуються на всі контролери домену при реплікації. Сервери, на яких служба AD не встановлена, але які входять в домен, називаються рядовими серверами.

Реплікація AD виконується за запитом, служба KCC створює топологію реплікації, яка використовує сайти, визначені у системі, для управління трафіком. Внутрішньо сайтова реплікація виконується автоматично засобом перевірки узгодженості. Реплікація між сайтами може бути налаштована для кожного каналу сайту (наприклад, DS3, T1, ISDN і т. д.) і трафік реплікації буде обмеженим, передаватися за розкладом і маршрутизація відбувається відповідно до призначеної оцінки каналу. Дані реплікації транзитно передаються через кілька сайтів за допомогою мостів зв'язку. Реплікація сайт-сайт виконується серверами-плацдармами на кожному сайті, які потім реплікують зміни на кожен контролер домену свого сайту. Внутрішньо доменна реплікація виконується за протоколом RPC за IP, міждоменна – може використовувати додатково протокол SMTP.

Якщо структура AD містить кілька доменів, для вирішення завдання пошуку об'єктів використовується глобальний каталог: контролер домену складається з усіх об'єктів лісу, але з обмеженим набором атрибутів (неповна репліка). Каталог зберігається на зазначених серверах глобального каталогу та обслуговує міждоменні запити.

Можливість операцій з одним головним комп'ютером дозволяє обробляти запити, коли реплікація з кількома головними комп'ютерами неприпустима. Є п'ять типів таких операцій:

1. PDC-емулятор – емуляція головного контролеру домену;
2. RID-майстер – головний комп'ютер відносного ідентифікатора;
3. майстер інфраструктури – головний комп'ютер інфраструктури;
4. майстер схеми – головний комп'ютер схеми;
5. майстер іменування доменів – головний комп'ютер іменування домену.

Перші три ролі унікальні в рамках домену, останні дві – унікальні для усього лісу.

Базу AD можна розділити на три логічні розділи:

1. «Схема» – шаблон для AD, визначає всі типи об’єктів, їхні класи та атрибути (всі дерева знаходяться в одному лісі, тому що у них одна схема).

2. «Конфігурація» – структура лісу і дерев AD.

3. «Домен» зберігає всю інформацію про об’єкти, створених у цьому домені. Перші два сховища здійснюють реплікацію на всі контролери доменів в лісі, третій розділ повністю реплікується між репліками контролерів в рамках кожного домену та частково – на сервера глобального каталогу [9].

2.2. Основні функції та можливості служби AD

Контролер домену виконує функції аутентифікації користувачів і обладнань у мережі, а також виступає в якості сховища бази даних. При спробі використовувати будь-який з об’єктів (сервер, принтер тощо) мережі, виконується запит до контролера домену, який або дозволяє відповідну дію або блокує його.

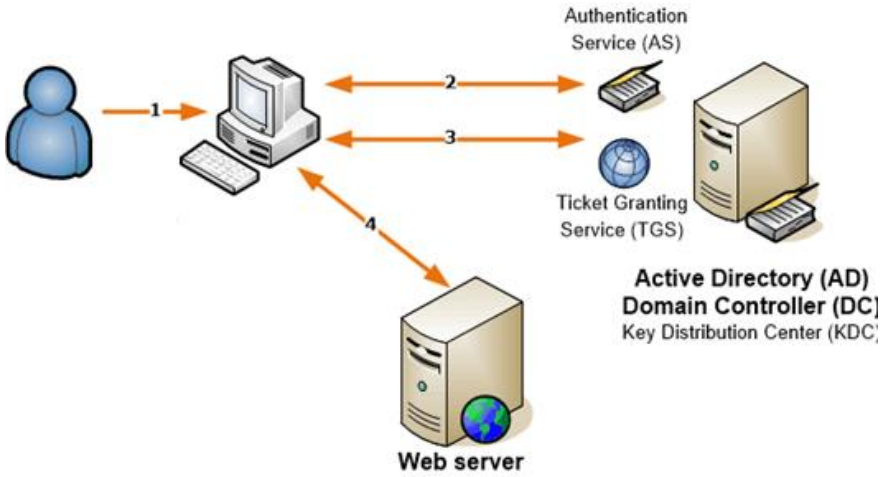


Рисунок 2.4 – Приклад виконання запитів до контролеру домена

Усі дані користувачів (логіни та паролі) зберігаються в єдиній базі даних, що суттєво спрощує роботу з ними. При авторизації всі комп’ютери звертаються до цієї бази даних, завдяки чому внесені зміни будуть застосовані

до всіх комп’ютерів мережі. Також за допомогою AD реалізується політика безпеки, завдяки якому можна обмежити доступ до певних серверів.

За допомогою AD можна поділити комп’ютери на робочі групи, що суттєво спрощує використання інфраструктури у двох випадках:

1. зміна існуючих налаштувань групи. Оскільки налаштування зберігаються в єдиній базі даних, при їхній модифікації, які будуть застосовані для всіх комп’ютерів, що відносяться до цієї групи;

2. додавання нового користувача, який автоматично отримує встановлені для його групи налаштування.

Залежно від користувача і його групи можна ввести обмеження на використання функціонала операційної системи. Наприклад, можна обмежити встановлення додатків усіма крім адміністраторів.

Служби AD покращують захист корпоративної мережі за рахунок того, що контролери домену захищені від зовнішнього доступу. Крім того, для аутентифікації в AD використовується протокол Kerberos (протокол для взаємної аутентифікації клієнта й сервера перед установкою з’єднання, у ньому врахована перехоплення й модифікації пакетів, що підвищує його надійність), який безпечніший у використанні за аналоги у робочих групах.

За допомогою AD реалізується технологія Distributed File System (DFS), яка використовується для управління файлами. Фактично, це розподілена мережа для зберігання файлів – фізично вони розташовуються на декількох серверах, але логічно перебувають в одному місці. Це зручна функція, що дозволяє масштабувати існуючу інфраструктуру, додаючи нові сервера, а не заміняючи ними старі.

Служби AD дозволяють організувати все устаткування та сервіси в єдину систему, так як підтримуються не тільки продукти Microsoft, але й сторонні рішення: IP-телефонія; 1С; шлюз віддалених робочих столів. Варто відзначити, можливість інтеграції з Windows Server використовуючи протокол RADIUS, завдяки якому можна використовувати VPN підключення для роботи поза офісом.

AD є центральним вузлом інфраструктури підприємства, тому у випадку його відмови всі ПК і сервера будуть недоступні. Тому необхідно виділити кілька основних пунктів, що дозволяють забезпечити безперебійне цілодобове функціонування системи, слід розгорнути один або більш дублюючих контролерів доменів і настроїти автоматичну реплікацію всіх змін. У цьому випадку, при виході з ладу одного з контролерів працездатність мережі не порушується.

Нові можливості служб домен AD Services (AD DS) поліпшують можливості організації у забезпеченні безпеки середовищ AD і допомагають їм переходити на хмарні й гібридні розгортання, де деякі додатки й служби розміщається в хмарі, а інші – локально. У них поєднуються всі кращі можливості веб-завдань, а також додані деякі поліпшення, серед яких:

1. Управління привілейованим доступом допомагає усунути проблеми безпеки в середовищах AD, які обумовлені методами крадіжки облікових даних, такими як Pass-the-hash, Spear phishing і аналогічні типи атак. Він надає нові рішення для адміністративного доступу, які налаштовуються за допомогою Microsoft Identity Manager (MIM).

PAM надає наступні відомості :

− новий ліс AD бастіону, який підготовляється MIM. Ліс бастіону має особливе відношення довіри PAM з існуючим лісом. Вона надає нове AD середовище, яке може бути без шкідливих дій, і ізоляція з існуючого лісу для використання привілейованих облікових записів.

− нові процеси в MIM дозволяють виконувати запити на адміністративні привілеї, а також нові робочі процеси на основі твердження запитів.

− суб’єкти безпеки з тіньової групи мають атрибут, який посилається на ідентифікатор безпеки групи адміністраторів в існуючому лісі. Це дозволяє тіньовій групі отримати доступ до ресурсів в існуючому лісі, не змінюючи списки управління доступом (ACL).

2. Користувач може бути доданий у групу тільки на певний час, необхідний для виконання адміністративного завдання.

3. Посилання зі стікаючим терміном дії доступні для всіх зв’язаних атрибутів. Але єдиним прикладом є зв’язок атрибутів Member/member of між групою й користувачем, коли повні рішення, наприклад PAM, попередньо налаштоване для використання терміну дії посилань.

4. Розширення центру поширення ключів вбудовані в AD контролери домену, щоб обмежити час дії протоколу Kerberos мінімальним значенням строку життя (TTL) у випадках, коли в адміністративних групах є кілька членів з обмеженим часом існування. Наприклад, якщо додається користувач до групи A з обмеженим часом життя, то при вході в систему час існування TGT (Ticket-Grant ticket) буде дорівнює часу, що залишився в групі A. Якщо користувач також є членом іншої групи B, яка має менше значення TTL, ніж група A, то час життя TGT дорівнює часу, що залишився в групі B.

5. Нові можливості моніторингу, що дозволяють швидко визначити, хто запросив доступ, який доступ був наданий і які дії були виконані.

Azure AD надає доступ до розширених можливостей ідентифікації для корпоративних, комерційних і освітніх клієнтів з поліпшеними можливостями для корпоративних і персональних обладнань.

Службам AD більше не потрібно особистий обліковий запис Майкрософт: тепер вони працюють із існуючими робочими обліковими записами користувачів, щоб забезпечити відповідність. Служби будуть працювати на комп’ютерах, які приєднані до локального домену Windows, а комп’ютери й обладнання, приєднані до клієнта Azure AD («Хмарний домен»).

У певному місці лісу Windows Server 2003 користувачі можуть увійти в мережу за допомогою ідентифікації основних користувацьких імен (UPN – User Principal Name), наприклад, mike@contoso.com. Після успішної ідентифікації їм буде наданий доступ до всіх мережевих ресурсів, до яких був наданий дозвіл, без необхідності реєструватися знову на різних серверах або доменах. Ім’я UPN є обов’язковим атрибутом об’єкта в обліковому запису користувача в AD, і воно встановлюється за замовчуванням, коли створюється новий обліковий запис користувача.

Одне з обмежень бази даних Windows NT 4 SAM полягає в тому, що адміністративні права доступні тільки у вигляді «все або нічого». Для того щоб надати користувачеві будь-який ступінь адміністративних потрібно зробити користувача членом групи Domain Admins. Цей рівень адміністративних прав надає користувачеві повний доступ в межах домену, включаючи право видаляти інших користувачів із групи Domain Admins. Такий метод делегування адміністративних функцій не є безпечним. З іншого боку, AD надає адміністраторам можливість делегувати адміністративні права. Використовуючи майстер Delegation Of Control Wizard або встановлюючи певні дозволи на об'єкти AD, адміністратори можуть частково надавати адміністративні права. Наприклад, можна призначити певному обліковому запису користувача адміністративне право скидати паролі в домені, але не створювати, видаляти або змінювати користувацький об'єкт.

Будь-які зміни в інфраструктурі AD повинні бути реалізовані відповідно до проекту. Окремий домен представляє одиницю інфраструктури, який може виконувати реплікацію на єдиний контролер домену і може підтримувати більш одного мільйона об'єктів, так що модель окремого домену підходить навіть для великих організацій (рис.2 5).

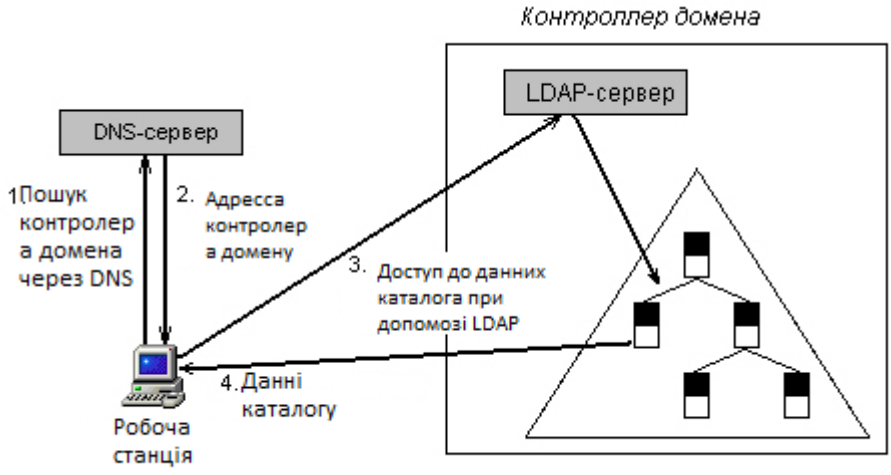


Рисунок 2.5 – Доступ до даних з використанням LDAP

У більшості сучасних мереж TCP/IP використовується служба DNS, головне призначення якої – перетворювати прості для запам'ятовування імена

типу company.com в IP-адреси. Для цього кожний комп’ютер-сервер DNS має набір записів з інформацією про ресурси. Кожний запис має деякий тип, що визначає характер і призначення інформації, що зберігається. Наприклад, запис типу A застосовується для перетворення доменного імені комп’ютера в задану IP-адресу, а запис типу MX – для пошуку поштового сервера в певному поштовому домені. Кожний DNS-сервер «знає» своє місце в глобальному просторі DNS-імен, що дозволяє передавати недозволені запити іншим серверам. Інтеграцію служб AD і DNS можна розглядати в трьох аспектах: домени AD і домени DNS мають однакову ієрархічну структуру й схожий простір імен.

Зони DNS можуть зберігатися в AD, якщо використовується сервер DNS, що входить до складу Windows 2000. Server, ті первинні зони, які занесені в каталог, реплікуються на всі контролери домену, що забезпечує кращу захищеність служби DNS.

У AD служба LDAP кожного домену Windows 2000 представлена SRV-записом служби DNS. Такий запис містить DNS-ім’я контролера цього домену, по якому клієнти можуть знаходити IP-адресу комп’ютера-контролера домену. Після того як потрібний контролер виявлений, для доступу до даних AD, що зберігаються на ньому, клієнт може використовувати протокол LDAP.

Протокол LDAP працює поверх TCP/IP і визначає способи доступу до каталогу з боку клієнтів. Крім механізму доступу даний протокол реалізує угоди по іменуванню інформації в каталозі, у явному виді описуючи структуру цієї інформації. Для клієнта всі дані, що зберігаються в базі LDAP, представляються у вигляді ієрархічного дерева. Кожний вузол дерева (об’єкт або елемент) може бути або контейнером, або листком. Відмінність між ними цілком очевидна: контейнери можуть містити інші елементи, а листки – ні.

Кожний елемент є деяким об’єктним класом, що визначає його властивості. Оскільки атрибути є й у контейнерів, і в листів, інформація, що зберігається в дереві каталогу, розподілена по всіх вузлах. Тип інформації, що зберігається в конкретній базі даних AD, задається схемою для цього каталогу.

Компанія Microsoft визначає стандартну схему, однак користувачі й розробники ПЗ можуть додавати нові класи й типи атрибутів. Зміна схеми каталогу – корисна функція, якою потрібно користуватися дуже обережно, оскільки такі зміни можуть мати наслідки.

Схема AD досить складна й містить сотні й сотні об'єктних класів і типів атрибутів. Нижче для прикладу перераховані деякі класи:

- user – описує конкретного користувача домену. Серед атрибутів цього класу: canonical name, user principal name (повне ім'я користувача), home postal address (домашня поштова адреса), telephone number (номер телефону), thumbnail photo (світлина);

- print queue – дозволяє клієнтові знаходити принтер. Серед атрибутів: location (місце розташування), print status (стан принтера) і print language (мова принтера).

- computer – ідентифікує деякий комп'ютер домену. Серед безлічі атрибутів цього класу: operating system (операційна система), operating system service pack, dns hostname і machine role (призначення комп'ютера; цей атрибут указує, чи є даний комп'ютер контролером домену, рядовим сервером або робочою станцією).

- organizational unit – описує підрозділи конкретного домену. Організаційні одиниці відіграють дуже важливу роль при структуруванні інформації, усередині домену.

Кожний елемент AD і кожний атрибут будь-якого елемента мають список управління доступом (ACL), який визначає права й можливості користувачів відносно доступу до конкретних елементів і атрибутів. Наприклад, список ACL може дозволити одним користувачам читати атрибути деякого елемента, іншим користувачам – читати й змінювати деякі з атрибутів, а іншим – заборонити який-небудь доступ до елемента. Ефективне управління доступом неможливо без достовірної аутентифікації клієнтів, AD використовує для цієї мети протокол Kerberos (рис.2.6).

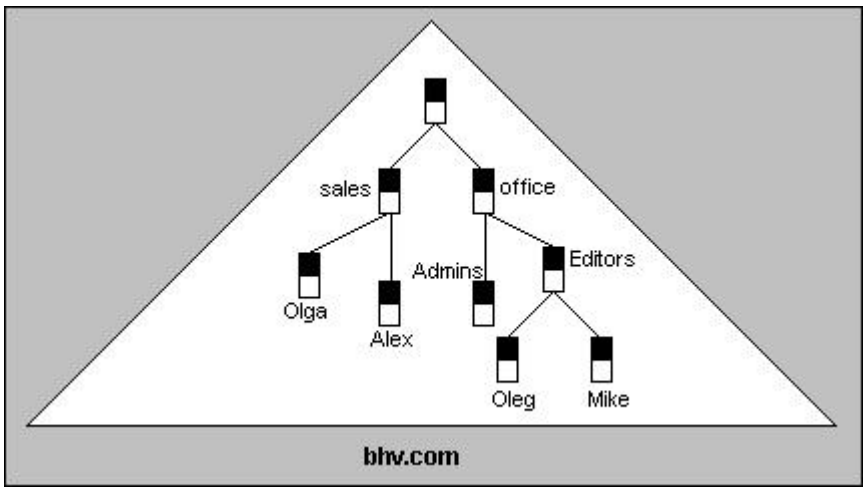


Рисунок 2.6 – Структура каталога простого домену Windows

Таким чином, очевидно, що служба каталогів повинна бути ретельно спроектована й розгорнута, з урахуванням усіх можливих нюансів, наприклад, пропускної здатності каналів між організаціями чи відділами (від цього прямо залежіть швидкість входу користувачів у систему, а також обмін даними між контролерами домену).

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ СЕРВЕР СИСТЕМИ НА БЕЗІ ТЕХНЛОГІЇ «ACTIVE DIRECTORY»

3.1 Аналіз серверної системи на підприємстві

Для роботи серверу потрібно 8-16 Гб і навіть більше. Самі серверні модулі пам’яті, як правило, мають функцію корекції помилок – ECC (error correction code). Завдяки цьому помилки запису й читання даних, викликані збоєм у роботі електроніки або дефектом мікросхем пам’яті, не приведуть до перебоїв у роботі програм або зависанню системи.

У більшості серверів дані зберігаються на швидких і ємних жорстких дисках, які поєднуються в raid-масиви. Тому що від сервера одночасно потрібні висока швидкість і відмовостійкість, ці формати масивів поєднують поділ даних по декільком жорстким дискам з дублюванням інформації на інших. Нерідко зустрічається й можливість відключати й підключати накопичувачі «на гарячу» – тобто не перериваючи роботу системи.

У таблиці 3.1. зроблений розрахунки компонентів серверного комп’ютера.

Таблиця 3.1 – Компоненти серверного комп’ютера

Компонент	Кількість	Ціна
Серверна материнська плата Intel S5500HCV	1	3 600 грн.
Процесор INTEL Xeon E3-1220 v2 3.1ГГЦ	2	14 660 грн.
Оперативна пам’ять Kingston 4Gb	2	2 940 грн.
Жорсткий диск SAS 1Tb Western Digital 1.3	2	14 900 грн.
Охолоджувач Zalman CNPS7000C-cu	1	851 грн.
Блок живлення Hewlett-Packard 750W CS HE Power Supply Kit	1	10 740 грн.
Відеокарта PCI-Ex 1024MB Gigabyte GV-N210D3-	1	1 328 грн.

1GI		
Мережева карта Intel EXPI9402PTBLK	1	6 061 грн.
Клавіатура Defender Element HB-520 Grey USB	1	300 грн.
Миша Dialog MOP-04BP Black USB	1	120 грн.
Гарнітура з мікрофоном Philips SHM3300	1	550 грн.
Разом		53 404 грн.

3.2 Встановлення та налаштування контролера домену AD

Існує два типи контролера домену:

- первинний контролер домену (PDC)
- резервний контролер домену (BDC)

Контролери домену, що працюють під управлінням Windows Server 2016, зберігають дані каталогу й управляють взаємодіями користувача й домену, включаючи процеси входу користувача в систему, перевірку дійсності й пошуки в каталозі. Контролери домену створюються при використанні майстра установки AD.

Контролер домену – це сервер на якому розташовується, база служби каталогів домену, а так само запущені служби, що дозволяють одержати доступ до цієї бази. Для доступу до бази використовується протокол LDAP і LDAPS. Контролерів домену відповідальних за той самий домен може бути небагато, у цьому випадку між ними виконується реплікація бази даних. Структура бази LDAP (рис 3.1):

До складу AD входить 5 служб:

1) AD DS (Directory Services) – служби за допомогою яких організована робота бази даних.

2) AD CS (Certification Services) – відповідає за видачу сертифікатів.

3) AD LDS (Lightweight Directory Services) – забезпечує роботу додаткових екземплярів баз даних служб каталогів. Це необхідно для роботи деяких додатків.

4) AD RMS (Rights Management Services) – служби управління правами користувачів.

5) AD FS (Federations Services) – дозволяє налаштувати довірчі відносини, між двома організаціями.

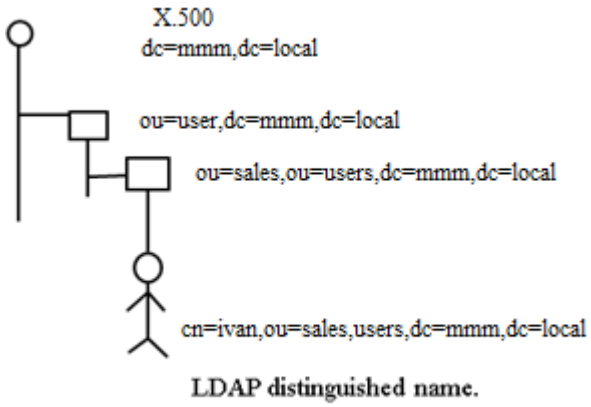


Рисунок 3.1 – Структура бази LDAP

LDAP – протокол прикладного рівня для доступу до служби каталогів X.500, відносно простий протокол, що використовує TCP/IP та дозволяє виконувати операції авторизації, пошуку і порівняння, а також операції додавання, зміни або видалення записів. Звичайно LDAP-сервер ухвалює вхідні з'єднання на порт 389 по протоколах TCP або UDP. Для LDAP-сеансів, інкапсульованих в SSL, звичайно використовується порт LDAPS-636.

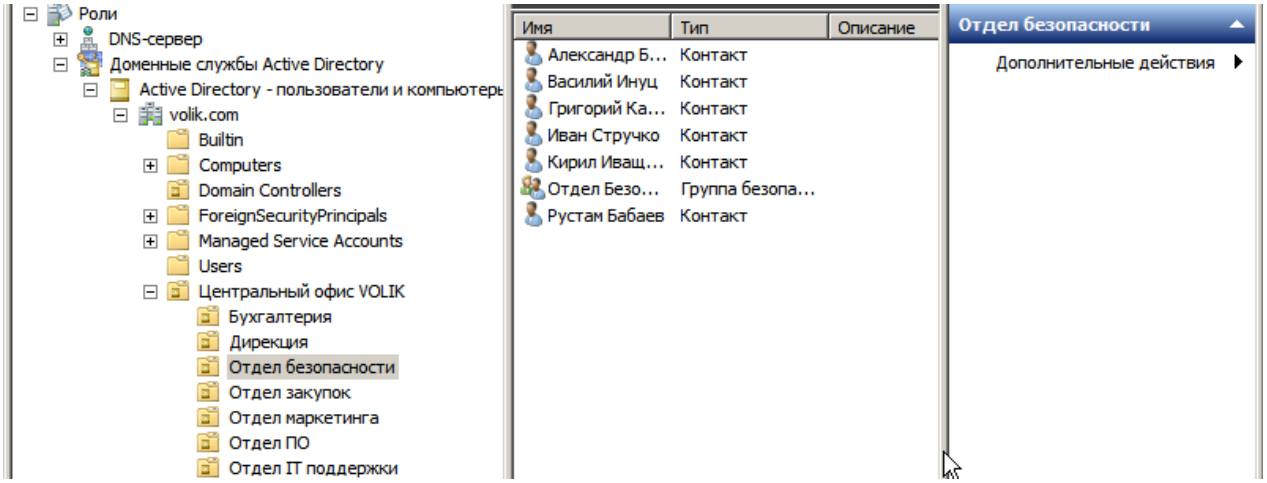


Рисунок 3.2 – База LDAP

Встановлення служб AD:

1) ПУСК – Виконати – «dcpromo»:

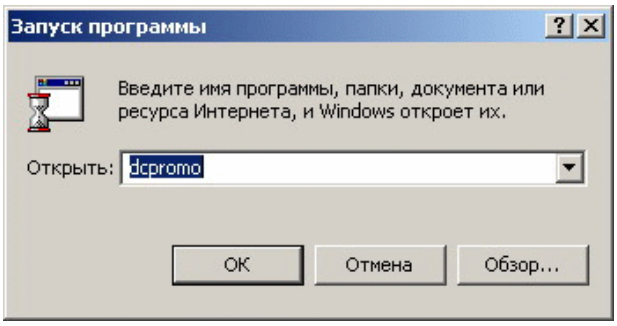


Рисунок 3.3 – Запуск програми

2) Далі виконується перевірка даних необхідних для установки AD після чого запуститься майстер AD. Так само можна використовувати розширений режим установки;

3) Обирається конфігурація розгортання існуючого або нового лісу;

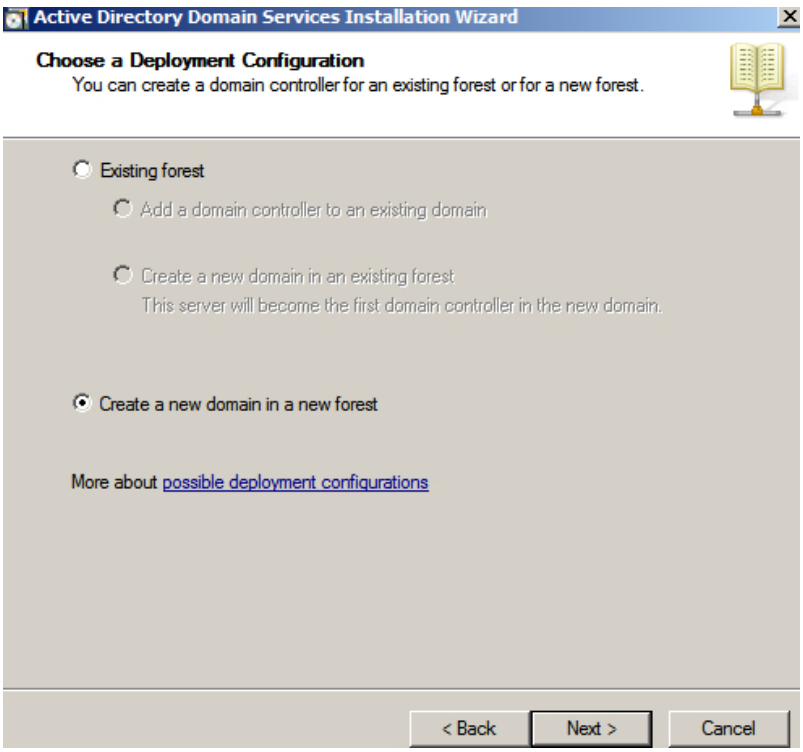


Рисунок 3.4 – Створення нового лісу при першій установці

4) Задання повного доменного ім’я так зване FQDN (Fully Qualified Domain Name), для нового домену лісу;

У роботі було використано ім'я домену volik.com;

5) Після перевірки ім'я було обрано режим роботи лісу.

Так як у мережі крім Windows server будуть ще використовуватися Windows 2003 Server, було обрано варіант для установки довірчих відносин, реплікації даних, створення складних топологій реплікації. У режимі роботи лісу Windows Server доступні всі можливості режиму Windows 2000, а також ряд додаткових:

- реплікація зв’язаного значення, що поліпшує реплікацію змін членів груп.
- ефективне створення складних топологій реплікації за допомогою KCC.
- довіра лісу, що надає організаціям зручність загального користування внутрішніми ресурсами в декількох лісах.

Усі нові домени, створені в цьому лісі, будуть автоматично функціонувати у режимі роботи домену Windows Server 2003.

6) Далі було обрано режим роботи домену. У основному режимі роботи домену Windows Server 2016доступні наступні можливості:

- універсальні групи;
- вкладення груп;
- перетворення типу групи;
- журнал SID;
- обмежене делегування, що дозволяє додатку скористатися перевагою безпечного делегування користувацьких облікових даних за допомогою протоколу перевірки дійсності Kerberos;
- відновлення Lastlogontimestamp: Атрибут lastlogontimestamp обновляється до часу останнього входу користувача або комп’ютера й виконує реплікацію по всьому домену.
- можливість задати атрибут userpassword у якості ефективного пароля для inetorgperson і користувацьких об’єктів;
- можливість перенаправляти контейнери «Користувачі» і «Комп’ютери»

для визначення нових відомих розташувань облікових записів користувачів і комп’ютерів.

7) Далі встановлюються додаткові параметри контролера домену.

Перший контролер домену повинен бути сервером глобального каталогу і не може бути RODC. Рекомендується встановити службу DNS-сервера на перший контролер домену.

8) Для зберігання бази даних, файлу журналу використана тека SYSVOL – тека, у якій зберігається серверна копія загальних файлів домену, які повинні бути загальними для загального доступу й реплікації у всім домені, на контролері домену містить наступні елементи:

1 NET Logon є загальними. Звичайно це розміщення об’єктів політики для мережних комп’ютерів – клієнтів і сценаріїв входу в систему.

2 Сценарії входу користувачів для доменів, де адміністратор використовує AD – користувачі й комп’ютери.

3 Групова політика Windows.

4 З’єднання файлової системи.

5 Служба реплікації файлів (FRS) проміжної папки й файли, які повинні бути доступні та синхронізовані між контролерами домену.

9) Встановлюється пароль адміністратора для відновлення служб каталогів у випадку збою.

10) Перегляд обраних параметрів, необхідно зробити даний сервер першим контролером домену AD у новому лісі. Основні параметри:

- Ім’я нового домену volik.com. Це ім’я є також іменем нового лісу.
- Netbios – ім’я цього домену VOLIK.
- Режим роботи лісу: Windows Server 2003
- Режим роботи домену: Windows Server 2003
- Сайт: First-Site-Name

Додаткові параметри:

- Контролер домену тільки для читання: Немає
- Глобальний каталог: Так

- DNS-сервер: Так
- Створити DNS-делегування: Немає
- Папка бази даних: C:\Windows\NTDS
- Папка файлів журналу: C:\Windows\NTDS
- Папка SYSVOL: C:\Windows\SYSVOL
- Служба DNS-сервера буде встановлена на цьому комп’ютері.
- Служба DNS-сервера буде налаштована на цьому комп’ютері.
- Даний DNS-сервер буде основним DNS-сервером для цього комп’ютера.
- Пароль адміністратора нового домену буде таким же, як і пароль локального адміністратора цього комп’ютера.

11) Майстер доменних служб виконує налаштування доменних служб AD згідно з обраними параметрами. За бажанням можна перезавантажити систему автоматично, після чого натискаємо «Готово»

Налаштування контролера домену виконувалася майстром, тому необхідно створити необхідні підрозділи (OU), необхідних користувачів визначити для них права й дозволи, а також включити їх у відповідні групи.

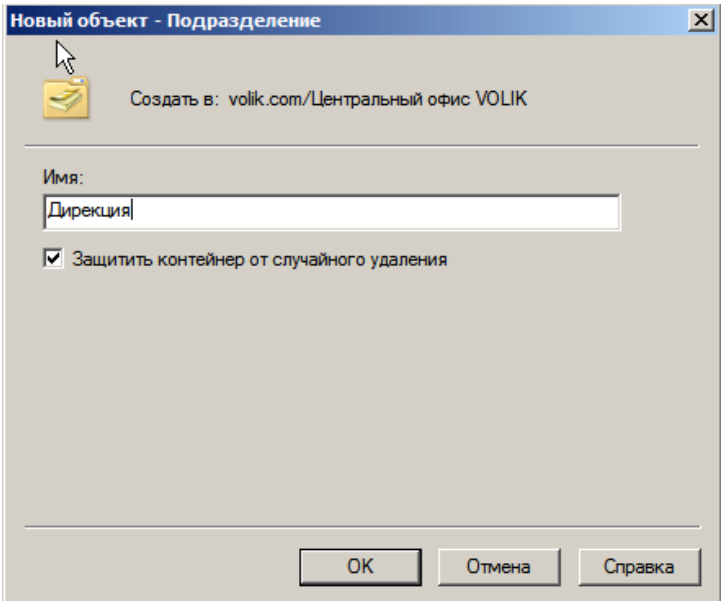


Рисунок 3.5 – Створення підрозділу

Створення групи користувачів (групи необхідні для зручності розподілу й пошуку необхідних користувачів, а так само для призначення групових політик).

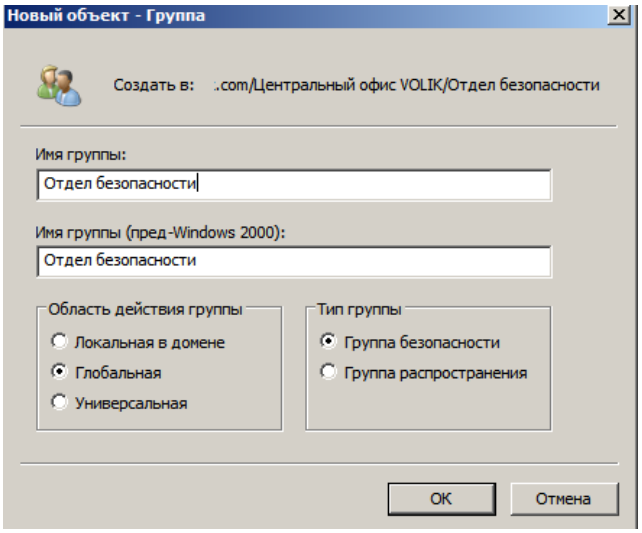


Рисунок 3.6 – Створення групи користувачів

Заповнення даних (Ім’я, Прізвище, login – ім’я користувача для входу в систему)

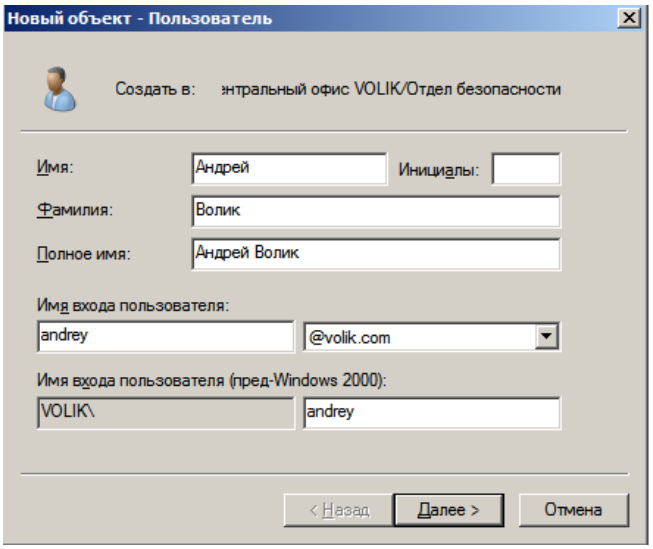


Рисунок 3.7 – Створення користувачів

Далі необхідно задати пароль (у нашому випадку, згідно з політиками, це повинен бути складний пароль). На підприємстві необхідно дати користувачеві можливість самостійно призначити собі пароль для цього необхідно, установити прапорець «Вимагати зміну пароля при наступному вході в

систему». Пароль користувача повинен знати тільки сам користувач.

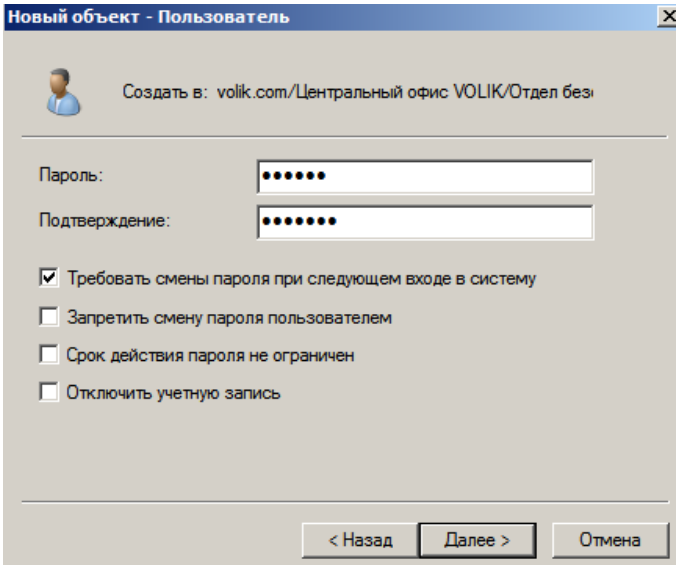


Рисунок 3.8 – Створення паролю

У додаткових властивостях користувача необхідно призначити, адресу електронної пошти, (це необхідно для обміну поштовими повідомленнями, а так само для служби управління правами RMS).

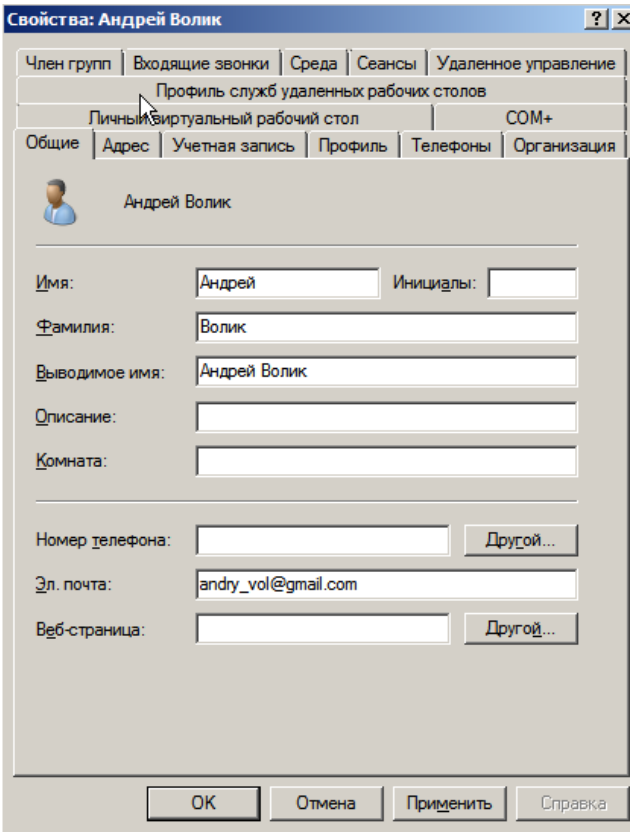


Рисунок 3.9 – Призначення електронної адреси

3.3 Налаштування DNS

DNS – комп'ютерна система розподілу для отримання інформації про домени. Структура DNS зон нашого підприємства.

Букви (імена) у трикутнику – це зони, за кожну зону може відповідати окремий сервер, що дозволить розподілити обов'язки по адмініструванню.

Домен «.» – є коренем дерева. Повне – абсолютне або повністю певне, fully qualified domain name – доменне ім'я закінчується точкою, що позначає корінь доменного дерева, але часто ця завершальна точка опускається. Доменами верхнього рівня виступають двобуквені національні домени або трибуквені домени ua, com, edu, org, net, gov, int, і т.д.

Рисунок 3.10 – Приклад доменів

Запис A (address record) або запис адреси зв'язує ім'я хосту з IP адресою. Наприклад, запит A – запису на ім'я referrals.icann.org поверне його IP адресу – 192.0.34.164.

Запис AAAA (Ipv6 address record) зв'язує ім'я хосту з адресою протоколу Ipv6. Наприклад, запит AAAA – запис на ім'я K.ROOT-SERVERS.NET поверне його Ipv6 адресу – 2001:7fd::1.

Запис CNAME (canonical name record) або псевдонім використовується для перенаправлення на інше ім'я.

Запис MX (mail exchange) або поштовий обмінник указує сервер обміну поштою для даного домену.

Запис NS (name server) указує на DNS-сервер для даного домену [10].

Запис PTR (pointer) або запис покажчика зв'язує IP хост з його псевдонімом. З метою зменшення обсягу небажаної кореспонденції (спама) одержувачі електронної пошти можуть перевіряти наявність PTR записів для хосту, з якого відбувається відправлення. У цьому випадку PTR запис для IP-адреси повинен відповідати імені поштового сервера, що відправляє повідомлення, яким він представляється в процесі SMTP сесії.

Запис SOA (Start of Authority) або початковий запис вказує, на якому сервері зберігається еталонна інформація про даний домен, містить контактну інформацію особи, відповідального за дану зону, таймінги (параметри часу) кешування зонної інформації й взаємодії DNS-серверів.

SRV-запис (server selection) указує на сервери для сервісів, використовується, зокрема, для Jabber і AD. SRV-запис є стандартом в DNS, що визначає місце розташування, тобто ім'я хосту і номер порту серверів для певних служб. Визначається в RFC 2782.

В DNS можна створити запис «SRV» для цього потрібно вибрати пункт меню «інші нові записи», у списку, що з'явився, потрібно знайти запис типу SRV.

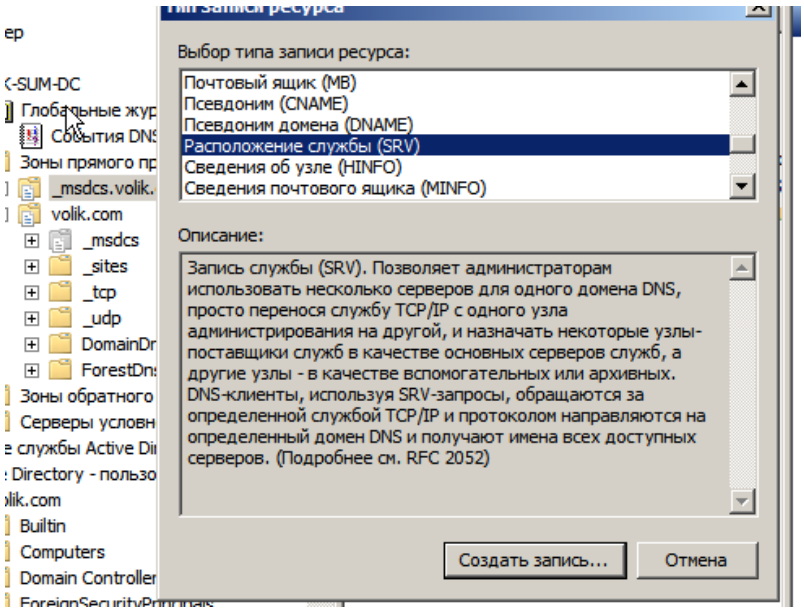


Рисунок 3.11 – Створення запису «SRV»

2) Заповнити необхідні поля, такі як (Служба для якої створюється SRV-запис, Протокол, Пріоритет, Вага й Порт), а так само потрібно вказати вузол служби:

Домен – доменне ім’я, для якого цей запис діє;

Служба – вказується символьне ім’я служби.

Протокол – транспортний протокол, який використовується сервісом, як правило TCP або UDP.

Пріоритет – пріоритет цільового хоста, більш низьке значення означає більш кращий.

Вага – відносна значимість для записів з однаковим пріоритетом.

Порт - – Порт TCP або UDP, на якому працює сервіс.

Вузол цієї служби – псевдонім машини, що надає сервіс.

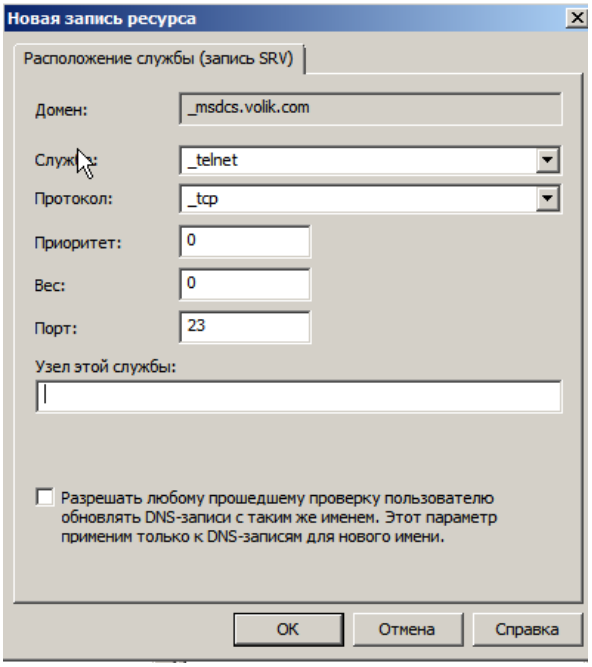


Рисунок 3.12 – Новий запис ресурсу

Запис SRV дозволяє адміністраторам використовувати кілька серверів для одного домену DNS, просто переносячи службу TCP/IP з одного вузла адміністрування на інший, і призначати деякі вузли-постачальники служб як основних серверів служб, а інші вузли – у якості допоміжних або архівних.

3.4 Встановлення й налаштування Rights Management Services

Windows Rights Management Services (RMS) (Служба Управління Правами) – це додаткова служба, що допомагає запобігти несанкціонованому звертанню до електронної інформації в онлайновому і автономному режимі, усередині границь корпоративного брандмауера й за його рамками.

RMS розширює стратегію безпеки підприємства, захищаючи інформацію за допомогою строгих політик використання, які супроводжують ці дані, куди б вони не потрапили. Співробітники, що працюють із інформацією, можуть чітко визначити, як адресат може використовувати отриману інформацію. Зокрема , можна визначити, хто може відкривати, редагувати, переадресовувати й/або виконувати інші операції із цією інформацією. Організації можуть створювати власні шаблони політик розмежування доступу, такі як «Конфіденційно-Тільки

для читання». Ці шаблони можна безпосередньо застосовувати до таких документів, як стратегічні бізнес-плани, фінансові звіти, специфікації продукції, відомості про клієнтів і електронні листи.

Вимоги для установки RMS:

1) Net framework 3.5 SP1;

2) Електронна пошта повинна бути зазначена у властивостях користувача.

WDS (Windows Deployment Services) або Служба розгортання Windows – призначена для централізованої установки систем на великій кількості комп'ютерів. За допомогою WDS можна встановлювати як чисті системи, так і попередньо створені образи, що включають у себе вже встановлене ПО й драйвера (такі образи те ж можна створювати засобами WDS).

Для роботи WDS необхідні наступні компоненти:

1) Deployment Server (Сервер розгортання) – забезпечує зберігання образів і роботу з ними.

2) Transport Server (Транспортний сервер) – здійснює передачу образів з Deployment Server на кінцевий клієнт.

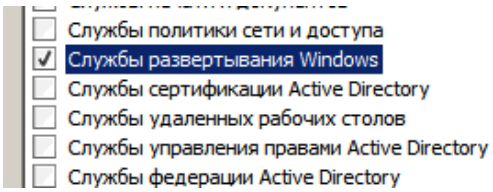
Для того щоб служба WDS працювала в мережі необхідно наступне:

1) AD DS (Directory Services) – служби за допомогою якої організована робота бази даних;

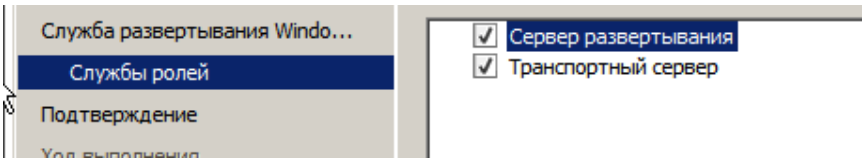
2) DNS;

3) DHCP (Dynamic Host Configuration Protocol) – це мережний протокол, що дозволяє комп'ютерам автоматично одержувати IP-адресу і інші параметри, необхідні для роботи в мережі TCP/IP. Даний протокол працює по моделі «клієнт-сервер». Для автоматичної конфігурації комп'ютер-клієнт на етапі конфігурації мережного обладнання звертається до так званого сервера DHCP, і одержує від нього потрібні параметри. Мережевий адміністратор може задати діапазон адрес, що розподіляються сервером серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості мереж TCP/IP.

1) Встановлення ролей «служби розгортання Windows»



2) Компоненти, які входять до складу служби WDS це «Сервер розгортання» і «Транспортний сервер».



3) Хід установки: запускаємо майстер. Попередньо був налаштований DHCP і створений додатковий розділ, на якому будуть зберігатися файли образів і файли відповідей. Вибираємо інший жорсткий диск (у нашому випадку, це розділ диска).

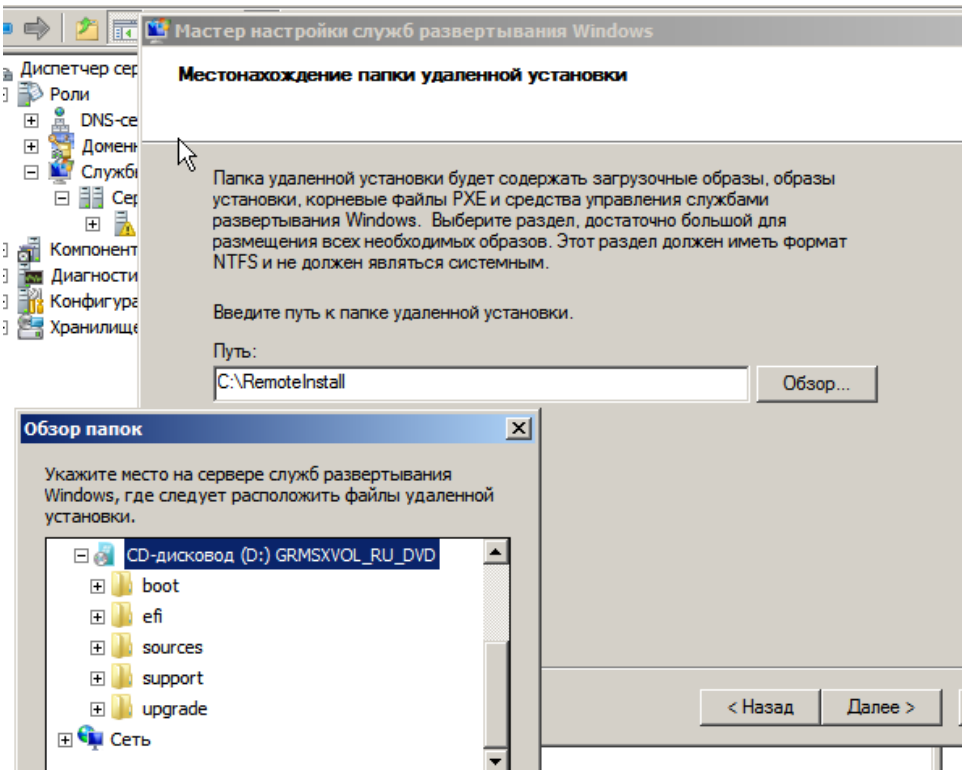


Рисунок 3.13 – Налаштування теки зберігання файлів

4) Так як сервіс DHCP буде, запущений на одному з роутерів, галочки «Не прослуховувати порт 67» і «Налаштувати для тегу 60 DHCP-параметра значення «PXE Client»» установлювати не потрібно, а 60-тег для DHCP потрібно настроїти на роутері зі службою DHCP у ручну.

5) Якщо на клієнтові немає операційної системи, або в налаштуваннях BIOS\boot у першому пункті встановлене значення «PXE UNDI …» – це означає що клієнт готовий для установки ОС. Отже, щоб уникнути установки ОС на небажані комп’ютери, було ухвалене рішення встановити галочку «Повідомляти адміністратора» – у такий спосіб адміністратор сам вирішує на які клієнтські комп’ютери будуть установлені та/або інша операційна система

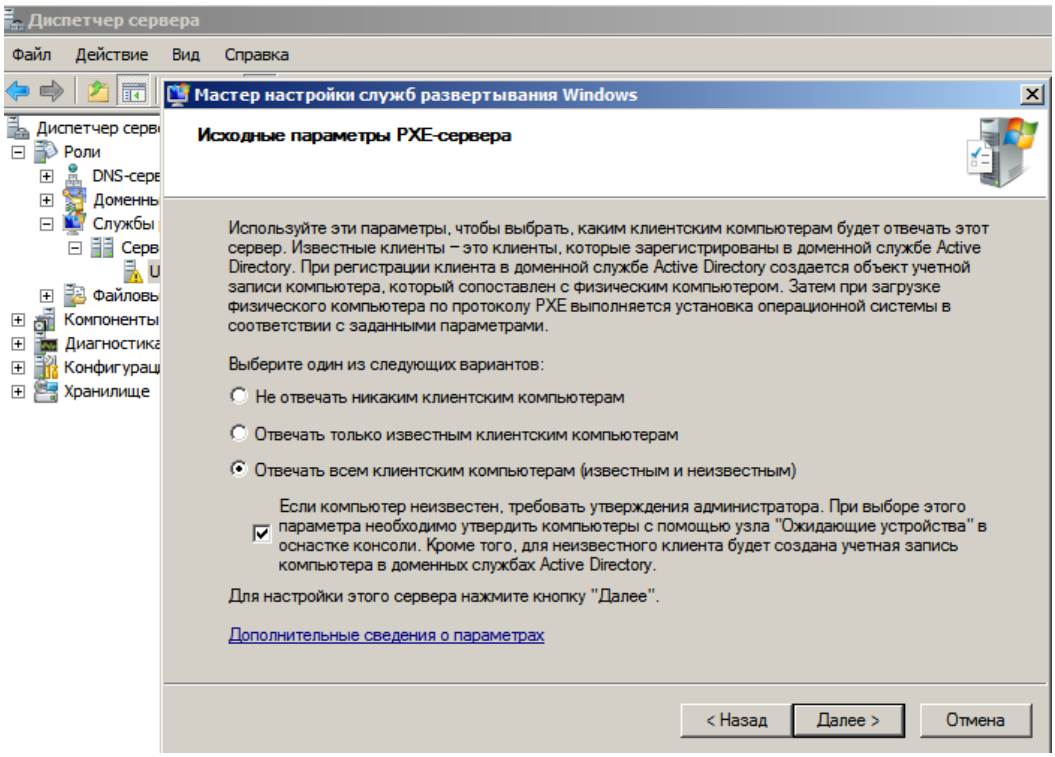


Рисунок 3.14 – Вихідні параметри PXE-сервера

Запуск служб розгортання:

1)додаємо образ установки (це весь Windows із програмами стислий в один файл із розширенням *.wim).

2) Образи можна розміщувати у групи для зручності, даємо ім’я цій групі "Windows 10 Enterprice".

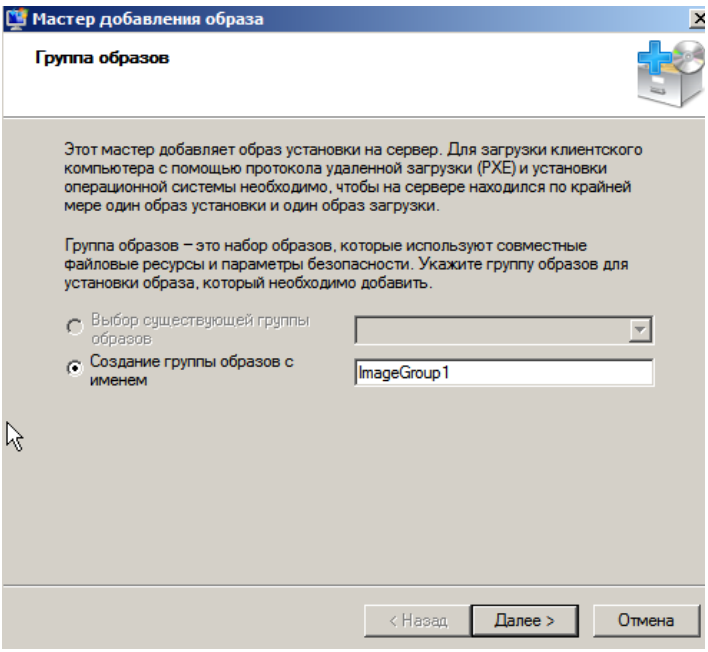


Рисунок 3.15 – Створення нового образу

3) Далі вибираємо теку з образами, у нашому випадку це другий розділ диска.

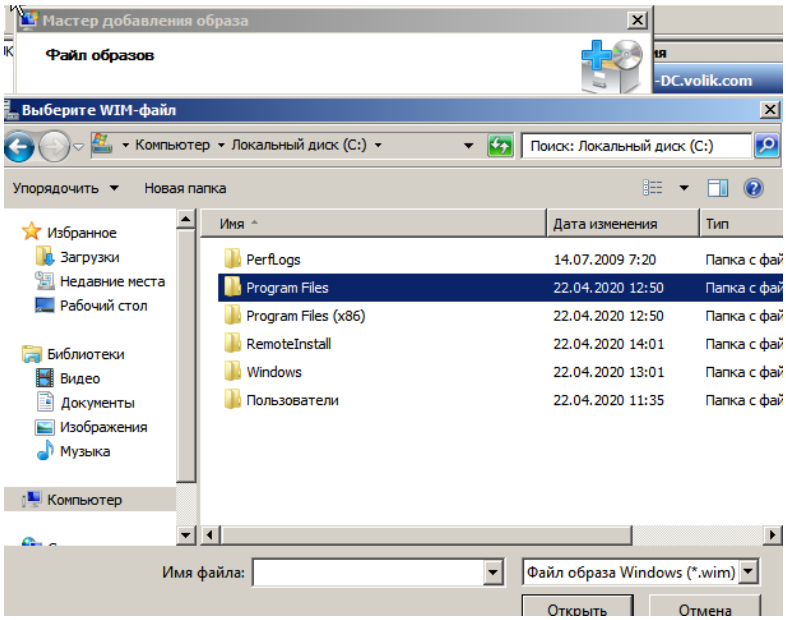


Рисунок 3.16 – Доступ до теки з образом

4) Після вибору теки і завершення дій, образи з’являться у вигляді списку, після чого до них можна буде підключати файли відповідей. Так само необхідно підключити й образи завантаження, у такий же спосіб.

3.5 Встановлення і налаштування WSUS локальної мережі домену

Report Viewer – програма для створення звітів по відновленням, наприклад на які комп’ютери, які відновлення були встановлені.

WSUS (Windows Server Update Services) – сервер відновлень Windows. Якщо такий сервіс присутній на підприємстві, то користувачам не потрібно звертатися за відновленнями в Інтернет, вони завантажують відновлення із сервера WSUS, що заощаджує Інтернет трафік. Сервер завантажує відновлення на свій диск, а клієнти при необхідності забирають потрібні відновлення сервера.

Для установки WSUS знадобіться пакет «WSUS30-KB972455-x86» і Report Viewer. Вибираємо повну установку сервера з консоллю адміністрування, указуємо папку з якої клієнти будуть одержувати відновлення, папку, у якій буде зберігатися база даних. Додатково можна вказати який Web-сайт буде використовуватися для Web-служб WSUS 3.0 SP2. Було ухвалене рішення встановити рекомендоване значення «Використовувати існуючий веб-вузол IIS за замовчуванням».

Конфігурування WSUS 3.0 SP2: так як це перший сервер, можна синхронізувати його із центром відновлення Microsoft. Далі набудовуємо проксі-сервер для виходу в Інтернет і встановлюємо з’єднання. Вибір відновлень, які потрібно завантажувати на сервер, для наступної установки їх на клієнтські комп’ютери. Відновлення, обраних програмних продуктів будуть завантажені на сервер WSUS.

Вибір класів для синхронізації , існує 9 класів відновлень:

- Драйвери – програмний компонент, призначений для підтримки нового обладнання.
- Критичні відновлення – виправлення для спеціальної проблеми, обумовленою критичною помилкою, яка не пов’язана із проблемою безпеки.
- Накопичувальні відновлення – накопичувальний набір виправлень, відновлення безпеки, критичні відновлення, упаковані відновлення разом, для

спрощення розгортання. Накопичувальні відновлення спрямовані на конкретні області, такі як "Безпека" або компонентів продуктів, таких як "IIS".

- Відновлення визначень – часто вихідні відновлення програмного забезпечення, що містять доповнення до бази визначень продукту. Бази даних визначень звичайно використовуються для виявлення об’єктів зі спеціальними атрибутами, таких як програми, написані зловмисниками, Web-вузли створені для несанкціонованого одержання закритих даних, або небажана електронна пошта.

- Відновлення системи безпеки – виправлення проблеми безпеки у певному продукті.

- Відновлення – виправлення для спеціальної проблеми, обумовленою некритичною помилкою, яка не пов’язана із проблемою безпеки.

- Пакети нових функцій – випуск функцій, які включаються в наступну версію продукту.

- Пакети відновлення – накопичувальний набір виправлень, відновлень безпеки, критичних відновлень, виправлень дефектів продукції знайдених у продукті з моменту його випуску. Пакети також можуть містити обмежене число клієнтів, яким надаються конструктивні зміни або особливості.

- Засоби – програма або функція, що допомагає у виконанні одного завдання або набору завдань.

Було ухвалене рішення вибрати всі класи тому що невідомо які класи відновлень знадобляться в майбутньому.

При налаштуванні автоматичної синхронізації було ухвалене рішення синхронізувати відновлення 1 раз у день о 8:00 ранку.

Опис рекомендацій інтеграції WSUS у сферу IT:.

1. Використання SSL з WSUS – для захисту розгорнутої копії WSUS можна використовувати протокол SSL, який дозволяє клієнтським комп’ютерам і підлеглим серверам WSUS робити перевірку дійсності сервера WSUS. Протокол SSL також використовується WSUS для шифрування метаданих (відомостей про відновлення), якими обмінюються клієнти і сервери

WSUS. Слід зазначити, що протокол SSL використовується WSUS тільки для захисту метаданих, але не вмісту (самих файлів відновлень). Цей спосіб також використовується Центром відновлення Майкрософт для поширення відновлень.

2. Створення групи комп’ютерів – на цьому етапі на сервері WSUS створюються групи комп’ютерів. Будь-яка група, крім групи "Не призначені комп’ютери", може містити вкладені групи. Це нова функція версії WSUS 3.0.

3. Призначення комп’ютерів у групи з боку клієнта за допомогою групової політики – перед виконанням цієї операції необхідно створити групу комп’ютерів. Рекомендується створити новий об’єкт групової політики, що містить тільки параметри WSUS. Цей об’єкт групової політики необхідно зв’язати з підходящим контейнером AD. У простому середовищу можна зв’язати один об’єкт групової політики WSUS з доменом.

4. Автоматичне схвалення установки відновлень – адміністратор може встановити правила для автоматичного схвалення свіжих відновлень відразу після їхньої синхронізації. При такому схваленні можуть ураховуватися класи відновлень, продукти й групи комп’ютерів. Крім того, можна задати автоматичне схвалення нових редакцій відновлень, автоматичне видалення застарілих відновлень і автоматичне схвалення відновлень WSUS. Усі ці правила можна увімкнути або вимкнути в будь-який час.

Налаштування об’єктів GPO (об’єкта групової політики) на контролері домену для WSUS:

1) Створення GPO WSUS

2) Налаштування автоматичного відновлення (автоматичне завантаження та повідомлення про установку, встановлення за розкладом щодня в 3:00)

3) Вказується служба розміщення відновлень Microsoft в мережі, куди клієнти будуть, звертається за відновленням.

4) Частота пошуку автоматичних відновлень.

5) Дозволити негайну установку відновлень. Указує, чи буде служба автоматичного відновлення встановлювати деякі відновлення без переривання

роботи служб Windows і без його перезавантаження.

6) Указує, чи буде служба автоматичного відновлення доставляти з веб-сайту Центру відновлення Windows як важливі, так і рекомендовані відновлення.

Після того як WSUS і політики GPO будуть установлені та налаштовані необхідно виконати синхронізацію нашого сервера із сервером Microsoft.

Необхідно дочекатися завершення синхронізації, для того щоб WSUS міг визначити яким комп'ютерам необхідні відновлення. Орієнтовний час синхронізації склав 5 год 26 хв. (час може відрізняться залежно від вибору відновлень які синхронізуються і швидкості їх завантаження).

1) Пошук в отриманих відновленнях, знаходимо потрібне відновлення.

Було вирішено схвалити відновлення для Media Center Windows 7 (KB2284742). Для перевірки працездатності.

2) Схвалення відновлення Media Center Windows 710 (KB2284742) виконане.

Дії, які необхідно виконати на клієнтові:

1) Виконати пошук відновлень (Панель управління \ Система та безпека \ Центр відновлення Windows) Натискаємо на кнопку "Перевірка відновлень" Після чого виконається пошук доступних відновлень.

2)Установлюємо знайдені відновлення.

3) Підготовка до установки.

4) Якщо оновлення успішно встановлені з'явіться щит зеленого кольору.

5) Після установки необхідно перезавантажити комп'ютер.

6) Порівняння номерів відновлень.

3.6 Встановлення Linux (UBUNTU, CENT OS, OPEN BSD) по мережі

Клієнт завантажується по мережі за допомогою Pxe-завантажника, який отримує IP-адресу від DHCP-сервера вбудованого в програму tftpd32, яка встановлена на сервері. Після цього клієнт завантажує завантажник і чекає

введення команди:

1) ENTER – клієнт завантажиться з локального диску.

2) Dos – завантажиться досівська завантажувальна дискета, після чого починається встановлення Linux.

Завантажувальна дискета створюється попередньо на основі необхідного образу операційної системи (Ubuntu, Cent OS або Open BSD).

1) На комп’ютері під управлінням Windows повинен бути встановлений tftpd32 v3.500 (безкоштовний TFTP/DHCP сервер).

2) Клієнтський комп’ютер повинен підтримувати Pxe-завантаження.

3) Образ ОС яку потрібно встановити.

Встановлення TFTPD32 V3.50:

1) Завантажуємо і встановлюємо Tftpd. Залишаємо галочки як є, і вибираємо запуск після установки.

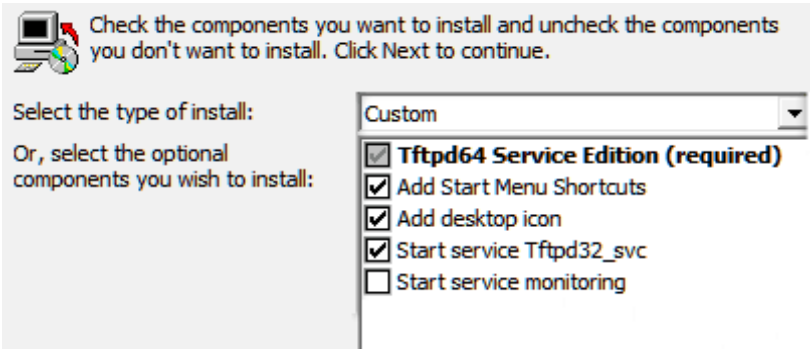


Рисунок 3.17 – Встановлення Tftpd зі стандартними налаштуваннями

3) Створюємо папку Tftpd у корені диска C:\ у ній створюємо папку root у якій будуть перебувати файли пов’язані з Linux.

5) Каталог Tftpd у корені диска C:\TFTPD\root був створений при установці Tftpd 32.

Налаштування Tftpd 32 V3.50

1) Після установки tftpd v3.500 заходимо в "Settings".

2) Потрібно переконатися в тому, що на вкладці "GLOBAL" обрані TFTP і DHCP.

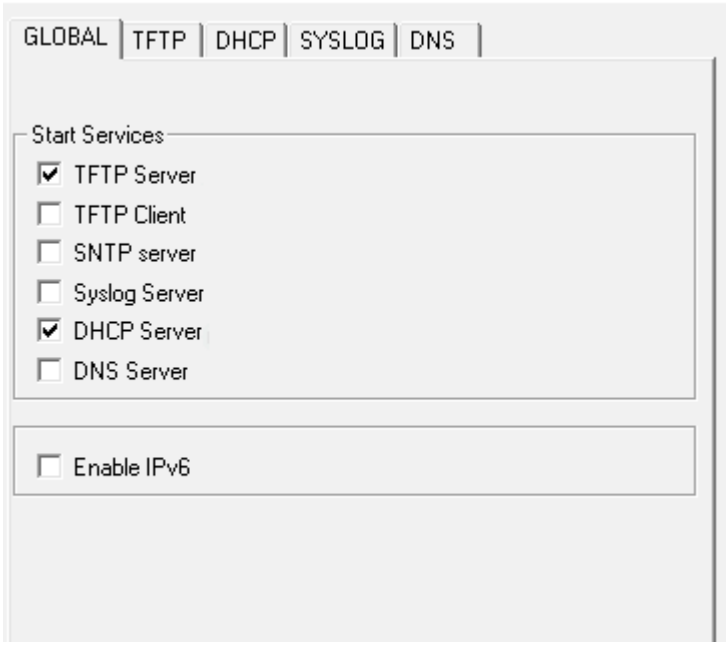


Рисунок 3.18 – Налаштування на вкладці "GLOBAL"

3) На вкладці TFTP необхідно вказати шлях до каталогу C:\TFTPD.

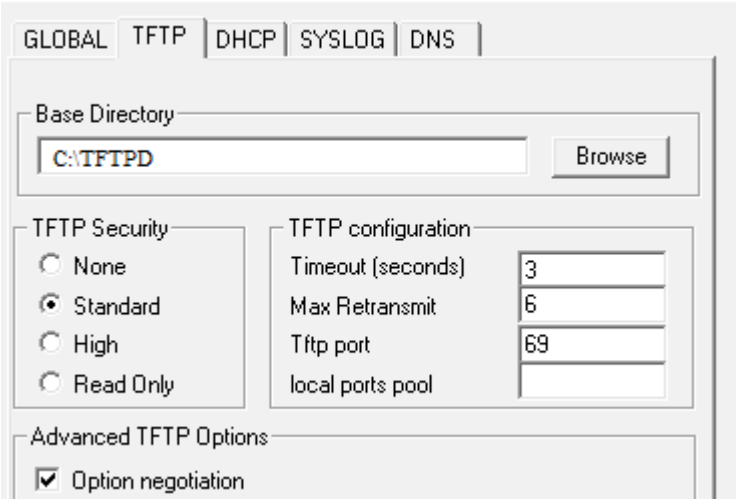


Рисунок 3.19 – Налаштування на вкладці TFTP

4) Необхідно налаштувати DHCP-сервер.

1) Указуємо початкову IP-адресу для видачі, кількість видаваних адрес не менш "1"

2) Ім’я завантажувального файлу Linux указуємо пізніше.

3) Аналогічно потрібно вказати:

DNS-сервер (172.16.100.1)

Шлюз (172.16.100.254)

Маску мережі (255.255.255.0)

Ім’я домену (volik.com)

Встановлення UBUNTU

1) Необхідно завантажити файли для мережевого завантаження після чого потрібно вибрати необхідну архітектуру.

2) Завантажений файл потрібно розпакувати в C:\TFTPD\root.

3) Необхідно скопіювати файл C:\tftpd\root\ ubuntu-installer\amd64\pxelinux.cfg\default в C:\tftpd\root\pxelinux.cfg

4) Після розпакування архіву вказати в налаштуваннях програми tftpd32 в DHCP завантажувальний файл pxelinux.0..

5) Потрібно переконається в тому, що на клієнтові в BIOS мережевий завантажник перебуває на першому місці.

3.7 Створення файлів відповідей

Файли відповідей необхідні для автоматизації установки ОС Windows.

1) Для створення файлів відповідей, необхідно установити додаткові компоненти з дистрибутива KB3AIK_RU.

Windows SIM – System Image Manager, який входить до складу AIK – Windows Automated Installation Kit .

При створенні файлу відповідей існує 7 етапів установки системи (передачі або проходи). Деякі проходи є обов’язковими при установці системи, у деякі систему потрібно переводити за допомогою спеціальних команд.

Сім етапів початкового конфігурування установки Windows за допомогою файлів відповідей:

Windows PE – перша фаза установки Windows яка закінчується копіюванням образа Install.wim (розбивка жорсткого диска, підключення до WDS додавання драйверів для Windows PE і т.д.). У WDS входить до складу Win2016R2 драйвер в образ Windows PE можна додавати через консоль WDS. У Win2016 потрібно користуватися або утилітами командного рядка (imagex,

dism), або за допомогою Windows SIM створювати відповідний файл відповідей. Тут ідеться тільки про ті драйвери, без яких не зможе початися встановлення системи (Мережева карта, HDD).

Offline Servicing – цей етап починається після копіювання образу але перед його конфігуруванням. На цьому етапі звичайно виконується встановлення додаткових драйверів, відновлень, мовні пакети.

Specialize – виконується на етапі конфігурування системи, але до появи вікна вітання. На цьому етапі можна налаштувати мережеві параметри, приналежність до домену, локалізацію системи, годинний пояс, ім’я комп’ютера.

OOBE System – фазу називають ще Windows Welcome. Це фінальне конфігурування системи, налаштування режиму відновлення, створення користувачів і т. д.

Audit System – у цю фазу можна ввійти тільки після виконання команди sysprep /audit. Це можна зробити натиснувши Shift+F12. У цьому режимі створюється тимчасовий обліковий запис адміністратора, і можна буде внести зміни в налаштування системи, не розпаковуючи її.

Audit User – налаштування профілю звичайного користувача. Налаштування застосовуються до профілю Default User, на базі якого створюються всі інші профілі. У цей режим можна ввійти командою sysprep / audit. У цьому режимі можна призначити тему робочого стола, розмістити ярлики на робочому столі тощо.

Generalize – перехід у нього виконується командою sysprep /generalize. Це видалення з ОС специфічної інформації, наприклад не очищати журнали системи при запечатуванні комп’ютера.

Приклад роботи «Файлу відповідей» знаходиться у Додатку А.

PXE завантажник – це мікро чіп на мережевій карті, який виконує пошук DHCP серверів і одержання IP-адреси, для подальшого зв’язку із сервером служб розгортання. Після одержання адреси від DHCP Pxe-завантажник, завантажує образ boot.wim – у якому розташовується невелика операційна

система, що дозволяє скачати образ Windows, і так само в ній зберігаються драйвера для мережевих карт і т. д.

Модифікація PXE завантажника необхідна для полегшення роботи й економії часу адміністратора, якому необхідно було б натискати кнопку F12 на кожному комп'ютері, на якому встановлюється операційна система. Для того щоб модифікувати завантажник необхідно змінити файл який використовує завантажник. За замовчуванням використовується файл pxeboot , його необхідно замінити на файл pxeboot.n12 x42б .

n12 – позначає "no F12" тобто не запитувати натискання клавіші F12.

При конфігуруванні було вирішено вимкнути натискання клавіші F12 для того щоб прискорити установку і заощадити час (який було б витрачено для виконання цієї дії на 100 клієнтських комп'ютерах).

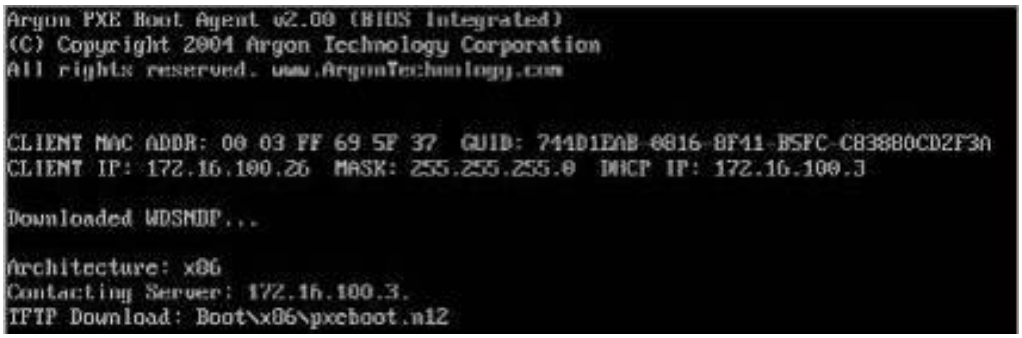


Рисунок 3.20 – Файл pxeboot.n12

1) Копіювання образу ОС Minipe.

2) починається Встановлення після якої повинні бути привітання.

3) Ліцензійна угода.

4) Відновлення або повне встановлення.

5) Створення або зміна жорсткого диска.

6) Вибір диска й розділу.

На всі ці й інші питання відповідає файл відповідей UNATTEND.xml.

7) Далі як звичайно починається копіювання файлів з образа Windows раніше створеного на WDS сервері.

8) Після всіх виконаних операцій система перезавантажиться й після завантаження з’явіться пропозиція натиснути CTRL+ALT+DEL.

9) Вхід у систему під доменним обліковим записом.

Опис використаного дистрибутива ОС Windows 7, для створення образів операційних систем:

1) Ім’я образу "Windows 7"

2) Редакція "Entrerprice"

3) Платформа "x86"

4) Мова – "RU"

5) VL – "Volume License необхідно активувати кожні 180 днів через kms сервер"

6) UPG – об’єднана позиція для переходу на Windows XP Professional.

7) Original Equipment Manufacturer – "Ліцензія на програмне забезпечення для продажу разом з новим комп’ютерним обладнанням.

Придбати повну версію операційної системи Windows можна або разом з повністю зібраною комп’ютерною системою, або разом з не периферійним компонентом комп’ютерного устаткування, наприклад, таким як модуль пам’яті. Додатки та серверне ПО може поставлятися тільки в складі повністю зібраних комп’ютерних систем.

8) Диск "DVD" 2,12 ГБ (ru_windows_7_enterprise_x86_dvd_x15-70945 x86)

9) Для установки ОС було використано служби розгортання Windows WDS, тому що ця служба значно спрощує установку операційних систем на велику кількість комп’ютерів).

Так само була передбачена необхідна кількість образів операційних систем для різних відділів. Кожний з перерахованих образів був оснащений файлами відповідей, тому що це дозволяє встановлювати кожний образ абсолютно автоматично, без втручання адміністратора або користувача, для установки операційної системи просто необхідно увімкнути комп’ютер і

почекати певний час. У кожному файлі відповідей визначені унікальні параметри для клієнтського комп’ютера.

Розподіл образів по відділах (Дирекція, Бухгалтерія, Відділ продажів і закупівель, Відділ логістики, Відділ IT, Відділ маркетингу, Відділ ПО).

1) Дирекція
   a. 1 образ, 2 файлу відповідей UNATTEND.xml & IMAGE UNATTEND.xml
   b. MS Office 2010.
2) Бухгалтерія
   a. 1 образ, 2 файлу відповідей UNATTEND.xml & IMAGE UNATTEND.xml
   b. MS Office 2010.
3) Відділ продажів і закупівель
   a. 1 образ, 2 файлу відповідей UNATTEND.xml & IMAGE UNATTEND.xml
   b. MS Office 2010.
4) Відділ логістики.
   a. 1 образ, 2 файлу відповідей UNATTEND.xml & IMAGE UNATTEND.xml
   b. MS Office 2010.
5) Відділ IT
   a. 1 образ, 2 файлу відповідей UNATTEND.xml & IMAGE UNATTEND.xml
   b. Немає програмного забезпечення .
6) Відділ маркетингу
   a. 1 образ, 2 файлу відповідей UNATTEND.xml & IMAGE UNATTEND.xml
   b. MS Office 2010 , Photoshop CS4, Coreldraw .
7) Відділ ПО
   a. 1 образ, 2 файлу відповідей UNATTEND.xml & IMAGE UNATTEND.xml

Таким чином вийшло 7 образів ОС, для 7 організаційних підрозділів, на якому розташовуються файли.

Після установки всіх ОС на комп’ютери можна входити доменними користувачами, а комп’ютери необхідно розподілити по організаціях на контролері домену.

З метою безпеки, на всі образи операційних систем, був установлений

складний пароль для локального облікового запису Адміністратор і створений додатковий локальний обліковий запис Winuser з адміністративними правами, для якого так само був установлений складний пароль. Обліковий запис адміністратора був заблокований.

3.8. Встановлення та налаштування Key Management Service (KMS)

KMS – це сервіс багаторазової активації продуктів Windows. За допомогою KMS-ключа можна активувати кілька операційних систем, кількість яких залежіть від того, на яку кількість ОС здобувався був придбаний даний ключ.

Встановлення та налаштування KMS у корпоративному середовищі Windows Server:

Windows Server 2018 (Enterprise);

Windows Vista (Business / Enterprise);

Windows 10 (Enterprise);

Існує 2 типи корпоративних ключів:

1) MAK (Multiple Activation keys) – використовуються для активації одиночних комп’ютерів без використання KMS сервера.

a) Призначені для активації окремих систем по телефону або Інтернету.

b) Використовуються там, де немає підключення до KMS серверу протягом 180 днів.

c) Існують обмеження по кількості активацій.

d) Управління MAK ключами здійснюється за допомогою Volume Activation Management Tool.

e) MAK ключі необхідно вводити окремо на кожної ОС.

2) KMS – спеціальні ключі, що використовуються для активації продуктів усередині корпоративної мережі, за допомогою служби KMS. Реєстрація ключа повинна продовжується після закінчення 180 днів від першої активації. Такий тип активації не рекомендується використовувати, якщо співробітник компанії

перебуває у відпустці більш 6 місяців і не зможе одержати доступ до мережі підприємства, тому що це спричиніть не бажані наслідки.

Переваги KMS.

a) Можливість автоматичного введення ключа (операційна система знаходить у мережі запис DNS, і KMS-сервер одержить із нього ключ);

b) Можливість автоматичної активації;

c) Безпека ключа (ключ зашифрований і зберігається у сховищі довірених даних сервера, ключ не доступний для користувачів);

d) Ведення обліку використання ліцензій за допомогою (MSSCOM).

При реєстрації в корпоративній мережі KMS-хосту в DNS створюється SRV-запис, що вказує KMS-клієнтам куди звертатися за активацією

На рисунку 3.21 показані DNS Windows Server 2016 і Host KMS як окремі системи. У нашій роботі усі ці сервіси перебувають на одному комп'ютері.

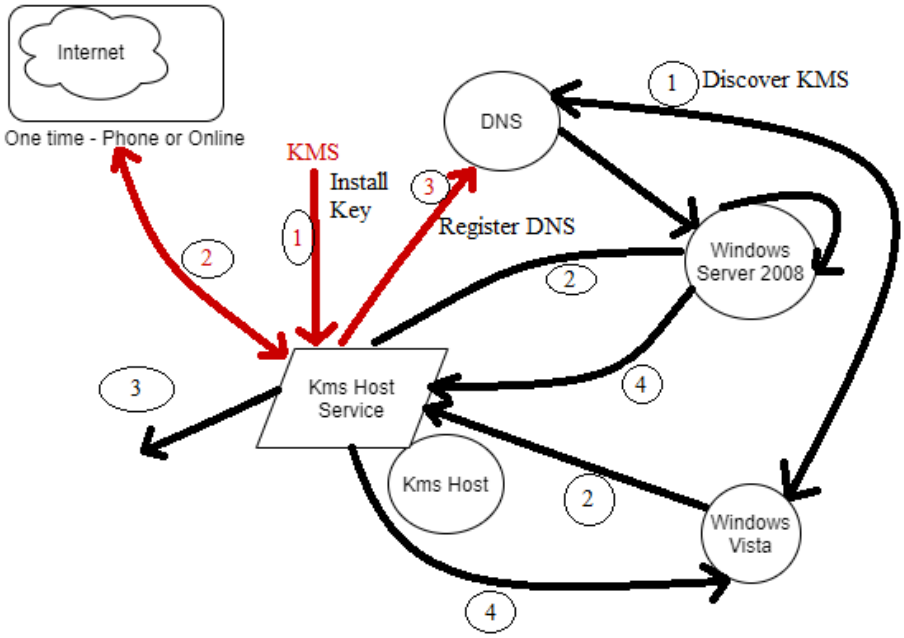


Рисунок 3.21 – DNS Windows Server 2016 і Host KMS як окремі системи

KMS Host – (так само є сервером KMS) на ньому виконана активація за допомогою KMS або MAK ключа, через Інтернет або за допомогою телефону, на ньому встановлений сам сервер KMS, установлений ключ KMS, створений запис SRV на DNS сервері.

Операційна система по запису DNS, знаходить сервер KMS і здійснює

запит ключа й виконання активації.

Встановлення ключа, його активація та створення запису.

1) Установлюємо ключ KMS.

2) Реєструємо його в Інтернеті.

3) Створюється запис SRV в DNS автоматично або в ручну (у роботі створювався запис у ручну, для демонстрації настроювань SRV записів).

Пошук KMS-сервера, KMS-ключів і активація Windows на стороні клієнта.

1) Комп'ютер шукає KMS-сервер за допомогою запису в DNS.

2) Клієнт звертається до KMS-серверу для одержання ключа.

3) KMS вибирає один із ключів, згідно з редакцією ОС установленої на клієнтові.

4) KMS-сервер відправляє ключ клієнтові для активації.

5) На клієнтові відбувається активація ОС за допомогою ключа отриманого від KMS-сервера.

На клієнтові може бути встановлена будь-яка операційна система, головне щоб на сервер були внесені ключі для цих ОС. У нашому випадку це ОС:

1) Windows 2016 Server.

2) Windows 10.

Вимоги використання служби KMS у локальній мережі

Таблиця 3.2 – Обмеження по кількість комп'ютерів

Windows Server 2008	Windows Vista	KMS Host	Activation Count on KMS Host	KMS Activation Status
4	1	1	5	Windows server 2008 Only
1	4	1	5	Windows server 2008 Only
1	1	1	2	None
4	22	1	26	Both

Встановлення служби MKS може, здійснюється тільки на операційні системи Windows Server 2016.

До складу Windows 2016 Server – служба KMS входить за замовчуванням.

2) Сервер DNS і доступ до нього через порт 1688.

3) Доступ сервера KMS до мережі Інтернет (для первісної реєстрації) не обов'язково, тому що можна активувати сервер KMS за допомогою MAK ключа по телефону.

Дії необхідні для налаштування KMS сервера

1) Зміна дозволів SRV-запису на сервері DNS

a) Необхідно створити глобальну групу KMS-hosts в AD.

b) Додати в створенню групу обліковий запис майбутнього сервера KMS.

c) В DNS надати права даній групі на створення записів SRV.

2) Автоматична публікація KMS у домені

a) Необхідно створити в реєстрі запис шлях (HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ Current Version \ SL)

b) Запис DNS domain publish list типу Multi-String Value.

c) Потрібно змінити суфікс домену volik.com

d) Запустіти знову службу Software Licensing Service.

3) Встановлення сервера KMS

a) На майбутньому сервері KMS необхідно дати команду:

script C:\windows\system3slmgr.vbs /ipk < указати Kms- Ключ>

b) Далі потрібно активувати систему за допомогою Інтернет за допомогою команди:

script C:\windows\system3slmgr.vbs /ato

c) І запустити знову службу Software Licensing Service.

Налаштування KMS-сервера

1) Створення глобальної групи безпеки.

2) Додавання сервера KMS у групу.

3) Створення запису в реєстрі.

4) Створення SRV-запису в DNS

5) Заповнення полів SRV-записи.

6) Необхідно зупинити й запустити наступні служби: 1) Зупинка й запуск служби "Активація Windows"

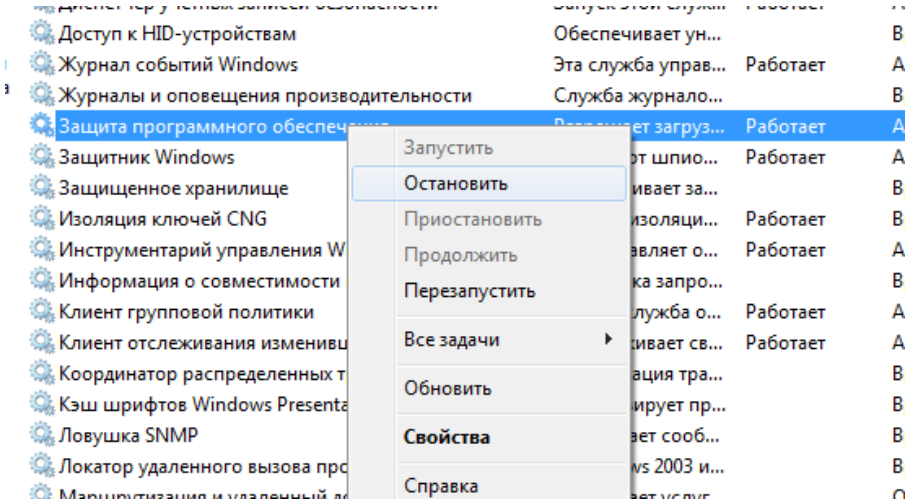
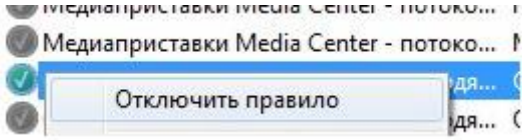


Рисунок 3.22 – Зупинка й запуск служби "Захист програмного забезпечення"

7) Встановлення KMS ключа на сервер:

8) Налаштування Firewall (необхідно відключити вхідне правило):



Демонстрація роботи KMS неможлива з кількох причин.

1) Недостатньо місця для установки необхідної кількості ОС.

2) Немає необхідних ключів для активацій ОС Windows 10 і Windows 2016 Server.

3) Windows 10 enterprise неможливо активуватися за допомогою ключів MAK, KMS, а так само за допомогою активаторів.

3.8 Формування групи безпеки

AD включає два типи груп безпеки і поширення домену з трьома областями локальна в домені, глобальна і універсальна.

Групи безпеки – відносяться до принципів безпеки з SID-ідентифікаторами, а тому вважається найпоширенішим і групи такого типу можна використовувати для управління безпекою та призначення дозволів доступу до мережевих ресурсів в списках «ACL».

У AD існує три області дії груп:

– локальна група в домені – призначена для управління дозволами доступу до ресурсів. У локальну групу в домені можуть входити користувачі, комп'ютери, глобальні та локальні групи в поточному домені, будь-якому іншому домені лісу, а також універсальні групи в будь-якому домені лісу. У зв'язку з цим, локальні групи в домені зазвичай використовують для надання правил доступу у всьому домені, а також для членів довірчих доменів.

– глобальна група – може містити користувачів, комп'ютери та інші глобальні групи тільки з одного домену, може бути членами будь-яких універсальних і локальних груп.

– універсальна група – дозволяє управляти ресурсами, розподіленими на декілька доменів, тому вважаються найбільш гнучкими. Вони визначаються в одному домені, але реплікуються в глобальний каталог. Універсальна група може бути членом іншої універсальної або локальної групи домену в лісі, а також може використовуватися для управління ресурсами. Ці групи доцільно задіяти тільки в лісах, що складаються з безлічі доменів для їх об'єднання.

Групи безпеки спрощують надання дозволів користувачам, оскільки встановити дозволи групі і додати користувачів в цю групу набагато простіше, ніж окремо призначати дозвіл численним користувачам і управляти ними, а коли користувачі входять в групу, для зміни того чи іншого дозволу всіх цих користувачів достатньо однієї операції.

3.9 Розробка моделі доступу до інформаційних ресурсів

Для розгортання лісу і домену у відповідності із спланованою раніше структурою був запущений «Майстер установки доменних служб AD. Далі був створений новий домен в лісі, як ім’я кореневого домену лісу було вирішено використовувати «Volik.com». Як функціональний рівень було вирішено використовувати «Windows Server 2016», що означає, що всі домени в лісі будуть працювати на рівні Windows Server 2016. На сторінці «Розташування для бази даних, файлів журналу і папки «SYSVOL» дані були прийняті задані за замовчуванням. Далі був заданий пароль для запуску доменних служб AD у режимі відновлення служб каталогів для завдань, що виконуються в автономному режимі. Потім був запущений процес налаштування AD DS, по закінченні якого необхідно перезавантажити сервер.

Як видно з рисунку 3.23, після розгортання домену була перенесена організаційно-штатна структура компанії на прикладі головного офісу в Києві.

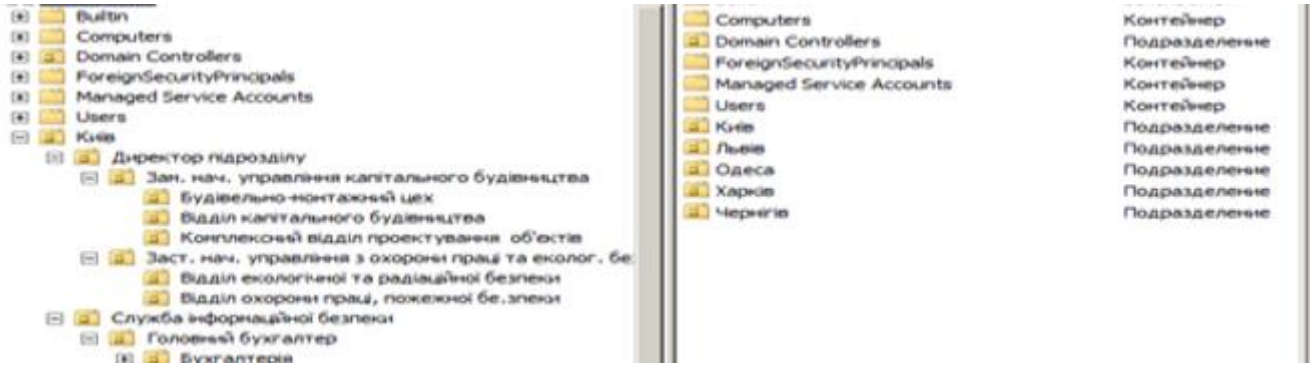


Рисунок 3.23 – Організаційно-штатна структура

Потім у кожному із сформованих підрозділів було створено по 3 робітника і по одному керівнику, що відносяться до різних груп безпеки.

Далі в організаційному підрозділі «Users» були створені групи безпеки у відповідності з обраними раніше вимогами. Для того щоб створити обліковий запис об’єкта групи було відкрите оснащення AD – користувачі і комп’ютери. Потім після запуски команди для створення групи з’явиться нове вікно з заголовком «Новий об’єкт – група».

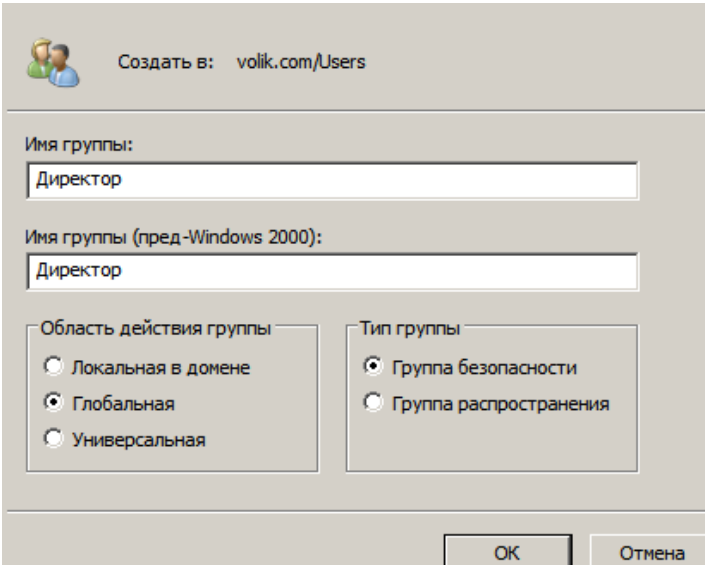


Рисунок 3.24 – Створення групи

У вікні в полі «Ім’я групи» було введено ім’я групи «Директор». Потім для даної групи був обраний тип «Група безпеки» і область дії «Універсальна». Після цього створений обліковий запис об’єкта група з’явиться в обраному раніше підрозділі «Users».

Аналогічним чином в тому ж підрозділі були створені групи безпеки «Керівники підрозділів» (Глобальна) і «Робітники» (Локальна).

Далі в групи в якості членів були додані облікові записи користувачів, створені раніше. Для цього в AD були відкриті властивості облікового запису в підрозділі «Директор підрозділу». У вікні «Властивості: Артем Глевський» була відкрита вкладка «Член груп». Варто зазначити, що обраний обліковий запис вже входить до групи «Користувачі домену». Після натискання кнопки «Додати» відкриється нове діалогове вікно «Вибір групи», у якому було введено ім’я «Директор». Після цього користувач «Артем Глевський» став членом групи «Директор» .

Далі у властивостях груп «Керівники Підрозділів» і «Робітники» на вкладці «Члени групи» після натискання кнопки «Додати» відкрилося нове діалогове вікно через яке були додані нові члени вищезазначених груп.

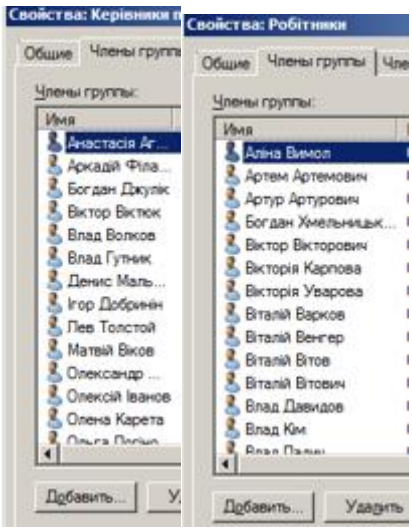


Рисунок 3.25 – Додавання нових членів груп

Потім для кожної з груп були створені індивідуальні налаштування політики безпеки. У «Windows Server 2016» політику паролів і блокування в домені можна замінити новою політикою паролів і блокування. Цю політику можна застосовувати до однієї або декількох груп користувачів в домені.

Для створення об’єкта «PSO», що застосовує дану політику паролів до членів груп «Керівники підрозділів» було відкрите оснащення «Редагування ADSI», потім у вікні оснащення на вузлі «Редагування ADSI» було викликано контекстне меню в якому була обрана команда «Підключення до…». Після цього в новому вікні з заголовком «Параметри підключення», зображено на рисунку 3.26, в полі «Ім’я» було введено ім’я домену – «Volik.com».

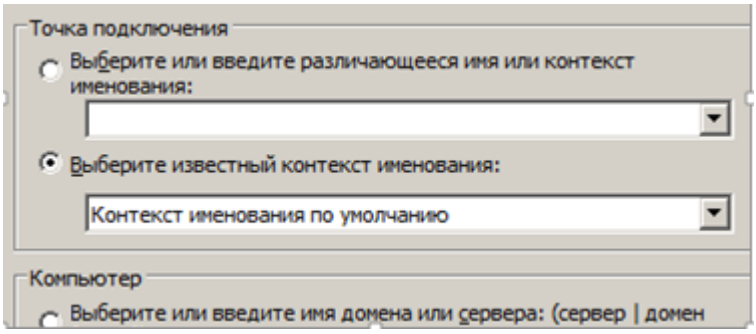


Рисунок 3.26 – Параметри точки підключення

У вікні «Редагування ADSI» покроково розгорнуті теки «DC=Volik, DC=com, CN=System» і відкритий елемент «CN=Password Settings Container». Всі об’єкти «PSO» створюються і зберігаються в контейнері параметрів паролів «PSC», який на початку порожній. У контейнері «PSC» запускається команда створення нового об’єкту.

Після цього на екран було виведено нове діалогове вікно з заголовком «Створення об’єкта», в якому необхідно було вибрати тип створюваного об’єкта. Тут представлений тільки один тип: «msDS-Password Settings», який є технічним ім’ям класу об’єкта «PSO».

Потім були вказані значення для наступних обов’язкових атрибутів:

1) Загальне ім’я: «Керівники підрозділів» – назва політики.

2) Параметр msDS-PasswordSettingsPrecedence: «1», відповідає якості за пріоритетність, чим вище значення у налаштування пароля PSO, тим менше значення цього параметра.

3) Параметр msDS-PasswordReversibleEncryptionEnabled: «False» – визначає можливість оборотного шифрування пароля.

4) Параметр msDS-PasswordHistoryLength: «25» – визначає кількість неповторюваних паролів.

5) Параметр msDS-PasswordComplexityEnabled: «True» – включення вимоги дотримання складності паролів.

6) Параметр msDS-MinimumPasswordLength: «12» – визначає мінімальну довжину паролів.

7) Параметр msDS-MinimumPasswordAge: «1: 00: 00: 00» – визначає мінімальний термін дії паролів, тобто 1 день.

8) Параметр msDS-MaximumPasswordAge: «25: 00: 00: 00» – 25 днів максимальний термін дії паролів.

9) Параметр insDS-LockoutThreshold: «5» – після 5 невдалих спроб авторизації спрацьовує механізм блокування облікового запису.

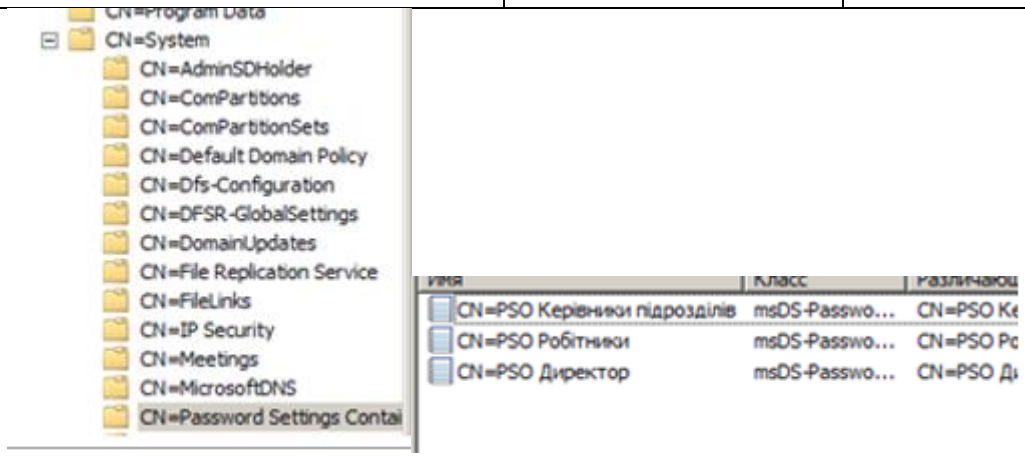
10) Параметр msDS-LockoutObsewationWindow: «0: 01: 00: 00» період скидання лічильника блокувань облікових записів.

11) Параметр msDS-LockoutDuration: «1: 00: 00: 00» 1 день тривалість блокування заблокованих облікових записів.

Потім, на сторінці атрибуту msDS-LockoutDuration, були відкореговані додаткові атрибути. Аналогічні дії були пророблені для груп «Робітники» і «Директор». Дані які були введені при налаштуванні нових «PSO» зазначені у таблиці 3.3.

Таблиця 3.3 –Переваги використання одного і кількох доменів

Атрибути	PSO Директор	PSO Робітники
msDS-PasswordHistoryLength	20	20
msDS-PasswordComplexityEnabled	True	True
msDS-MinimumPasswordLength	15	10
msDS-MinimumPasswordAge	1:00:00:00	1:00:00:00
msDS-MaximumPasswordAge	20:00:00:00	25:00:00:00
insDS-LockoutThreshold	3	5
msDS-LockoutObsewationWindow	0:01:00:00	0:01:00:00
msDS-LockoutDuration	1:00:00:00	1:00:00:00



У тому випадку, якщо компанія має кілька філіалів, кожен з яких має своє територіальне розташування необхідно встановити в кожному філіалі по контролеру домену. Необхідно забезпечити виконання двох завдань:

1) Кожен клієнт при аутентифікації повинен звертатися до найближчого контролеру домену для отримання протоколу Kerberos. При цьому і групові політики також повинні застосовуватися з найближчого контролера.

2) Реплікація змін усередині сайту здійснюється згідно зі схемою повідомлень за розкладом. Реплікація ж між контролерами, що знаходяться в різних сайтах відбувається тільки за розкладом.

Щоб ці завдання виконувалися ефективно необхідно конфігурувати сайти, які, по суті, є логічним угрупованням клієнтів і контролерів, пов'язаних швидкісними з'єднаннями.

Коли встановлюється AD, створюється єдиний сайт з ім'ям «Default-First-Site-Name» (надалі сайт можна перейменувати). Якщо не створюються додаткові сайти, то всі наступні контролери домену будуть додаватися до цього сайту. Однак, якщо компанія розташована в декількох місцях з обмеженою пропускною здатністю між ними, то необхідно створити додаткові сайти за допомогою інструменту адміністрування «AD – сайти і служби».

Після введення імені сайту було вибрано зв'язок сайту, який буде використовуватися для з'єднання цього сайту з іншими сайтами. Кожен сайт пов'язаний з однією або більше підмережами IP в AD. Далі була створена додаткова підмережа в контейнері «Subnets» в інструменті «AD – сайти і служби» і пов'язана з новим сайтом.

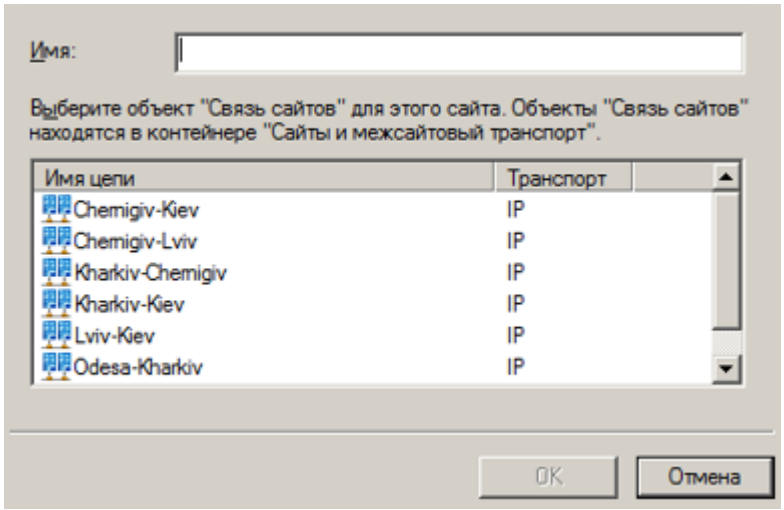


Рисунок 3.27 – Створення нового сайту

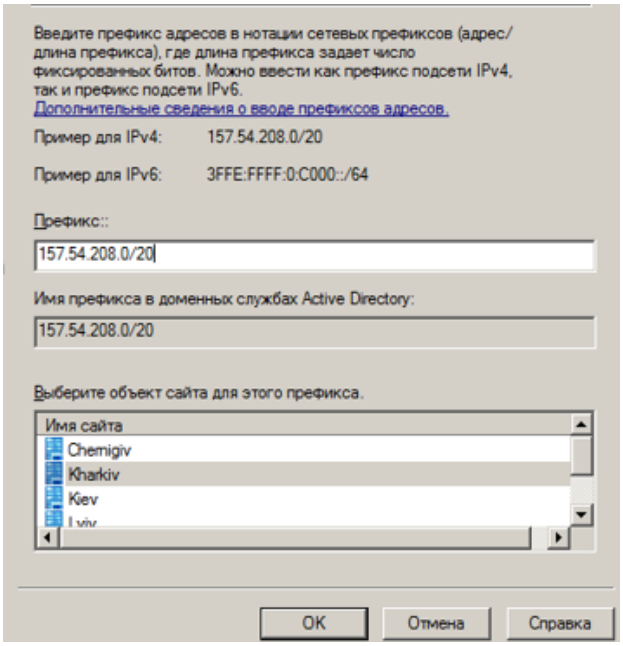


Рисунок 3.28 – Створення нової підмережі

Кожен сайт повинен мати мінімум один контролер домену. Щоб перемістити існуючий контролер домену в сайт, потрібно клацнути правою кнопкою миші на об’єкті контролера домену в його поточному контейнері «Servers» і вибрати «Перемістити». Потім буде запропонований вибір сайту, в який можна перемістити контролер домену. Якщо встановлюється новий контролер домену, то він буде автоматично розташований в тому сайті, в якому підмережа IP відповідає IP-адресою контролера домену.

З’єднання AD, які пов’язують сайти разом, називаються «зв’язками сайту». При установці створюється єдиний зв’язок сайту з ім’ям «DefaultIPSiteLink». Якщо не будуть створені ніякі додаткові зв’язки сайту перш, ніж будуть створені додаткові сайти, то кожен сайт включається в заданий за замовчуванням зв’язок сайту.

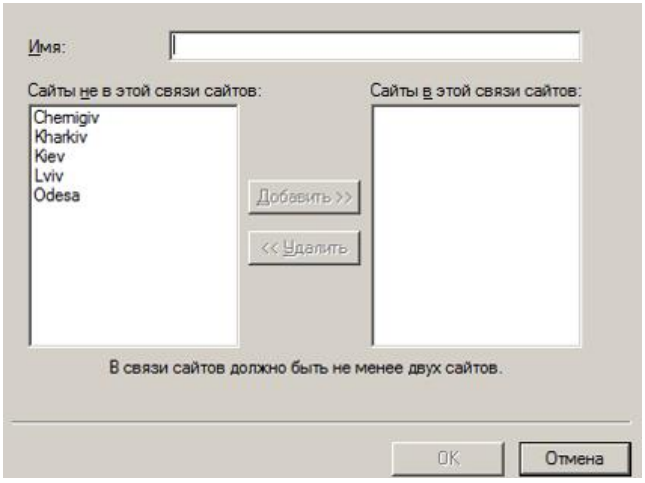


Рисунок 3.29 – Створення зв’язку сайтів

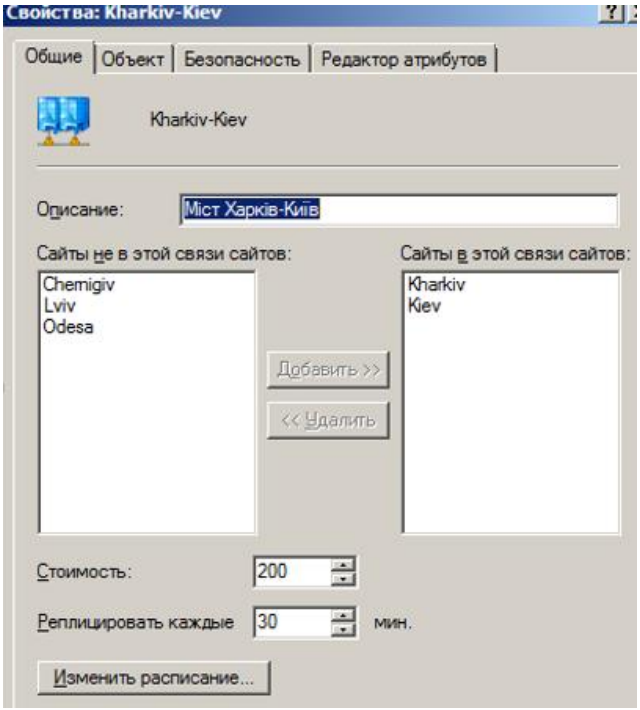


Рисунок 3.30 – Налаштування зв’язку

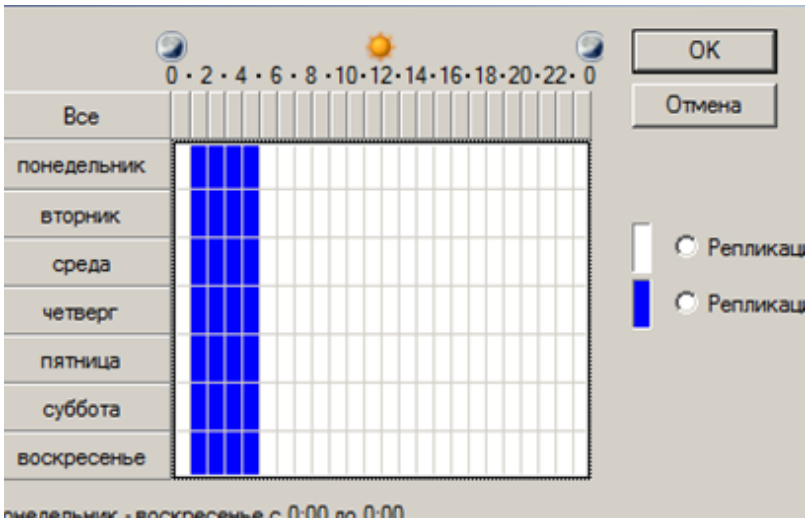


Рисунок 3.31 – Реплікації

Нижче наведені опції конфігурації для всіх зв’язків сайту:

– вартість – це призначене адміністратором значення, яке визначає відносну вартість зв’язку сайту, зазвичай відображає швидкість мережевої передачі і витрати, пов’язані з її використанням.

– графік реплікації – визначає, у який час протягом дня зв’язок сайту доступний для реплікації.

– інтервал реплікації – визначає інтервали часу, через які сервери-плацдарми перевіряють оновлення модифікацій каталогу на серверах-плацдармах інших сайтів.

У деяких випадках необхідно управляти тим, які контролери домену будуть використовуватися у якості серверів-плацдармів. Робота сервера-плацдарму може додавати істотне навантаження на контролер домену, якщо є багато змін інформації каталогу і встановлено часте проведення реплікації. Для конфігурування серверів-плацдармів потрібно отримати доступ до об’єктів в інструменті адміністрування.

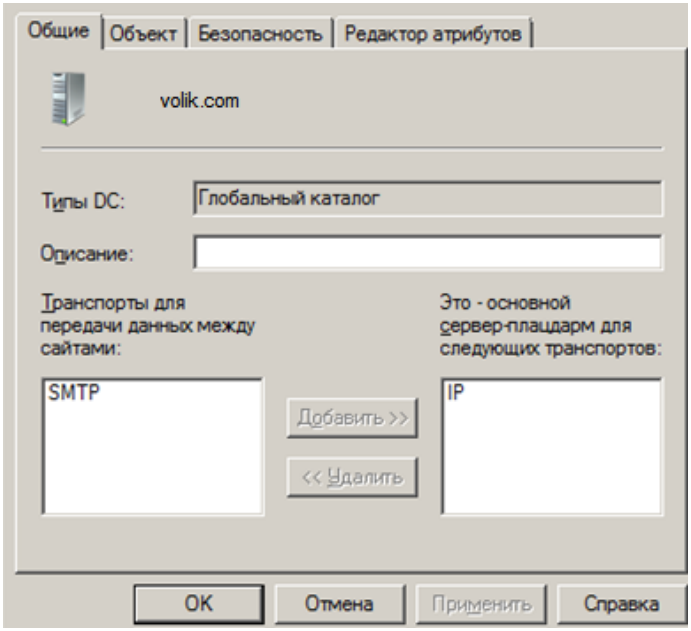


Рисунок 3.32 – Налаштування серверів-плацдармів

Перевага конфігурування привілейованих серверів-плацдармів полягає в гарантії того, що серверами-плацдармами будуть обрані контролери домену, зазначені адміністратором. Конфігурування привілейованих серверів-плацдармів обмежує можливості ISTG вибирати сервер-плацдарм, тобто завжди буде вибиратися сервер, який налаштований як привілейований. Якщо він не буде працювати то і реплікації припиняться доти, поки сервер не буде знову доступний.

Таким чином після виконання вищезазначених дій було виконано тестове розгортання розробленої моделі каталогу AD на базі серверної операційної системи «Windows Server 2016 R2» для центрального офісу компанії.

ВИСНОВКИ

У ході виконання випускної роботі після проведення аналізу теоретичних відомостей, а також аналізі існуючої інфраструктури та бізнес-процесів виробничої компанії була розроблена і запропонована до впровадження модель серверної системи на базі AD.

Для розглянутої в роботі організації була обрана модель єдиного лісу з центральним доменом і чотирма дочірніми регіональними доменами. Порядок призначення доменних імен обирався за територіальною ознакою, що дозволяє відобразити географічну структуру компанії, а також можливість реорганізації. Для поділу ресурсів між організаційними підрозділами для центрального домену була обрана модель на основі структури організації, оскільки вона дозволяє забезпечувати певний рівень автономності для кожного відділу і спрощене адміністрування. Була розроблена стратегія управління обліковими записами і групами безпеки підприємства, а також розглянуті питання конфігурації сайтів.

Також було виконано тестове розгортання розробленої моделі каталогу AD на база серверної операційної системи «Windows Server 2016» для центрального офісу компанії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. paessler.com. [Електронний ресурс] – Режим доступу до ресурсу: https://www.paessler.com/it-explained/active-directory.

2. computerhope.com. [Електронний ресурс] – Режим доступу до ресурсу: https://www.computerhope.com/jargon/s/server.htm

3. techterms.com. [Електронний ресурс] – Режим доступу до ресурсу: https://techterms.com/definition/server

4. microsoft.com/uk-ua. [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/windows/win32/adsi/so-what-is-active-directory?redirectedfrom=MSDN

5. Active Directory, 4th Edition / [B. Desmond, J. Richards, R. Allen та ін.]., 2008. – 866 с.

6. dummies.com. [Електронний ресурс] – Режим доступу до ресурсу: https://www.dummies.com/programming/networking/network-administration-structure-of-active-directory/

7. conceptdraw.com. [Електронний ресурс] – Режим доступу до ресурсу: https://www.conceptdraw.com/How-To-Guide/active-directory-diagram

8. etutorials.org. [Електронний ресурс] – Режим доступу до ресурсу: https://tinyurl.com/ksjszex

9. monitis.com. [Електронний ресурс] – Режим доступу до ресурсу: https://www.monitis.com/blog/active-directory-replication/

10. Станек У. Microsoft Windows Server 2012 R2: хранение, безопасность, сетевые компоненты. Справочник администратора / У. Станек. - СПб.: BHV, 2015. - 416 с.

11. ccbtechnology.com. [Електронний ресурс] – Режим доступу до ресурсу: https://ccbtechnology.com/what-microsoft-azure-is-and-why-it-matters/

12. Фленов, М. Web-сервер глазами хакера / М. Фленов. - М.: БХВ-Петербург 2017. - 320 с.

13. Технологія RAID» [Електронний ресурс] http://www.bytemag.ru/ - Режим доступу: URL: http://www.bytemag.ru/articles/detail.php?ID=8507

14. Минаси, Марк Windows Server 2012 R2. Полное руководство. Том 1. Установка и конфигурирование сервера, сети, DNS / Марк Минаси и др. - Москва: 2017. - 960 с.

15. Мюллер, С. Модернизация и ремонт серверов / С. Мюллер. - М.: Диалектика / Вильямс, 2017**.** - 383 с.

16. Васкевич Стратегии клиент/сервер / Васкевич, Дэвид. - М.: Киев: Диалектика, 2016. - 384 с.

17. Вивек Разработка Web-серверов для электронной коммерции. Комплексный подход / Вивек, Раджив Шарма; , Шарма. - М.: Издательский дом Вильямс, 2016. - 400 с.

ДОДАТОК А

Файл відповідей:

Файл UNATTEND.xml для початкового етапу конфігурування установки системи «Дирекція»:

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
<settings pass="windowsPE">
<component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<SetupUILanguage>
<UILanguage>ru-RU</UILanguage>
</SetupUILanguage>
<InputLocale>0419:00000419</InputLocale>
<SystemLocale>ru-RU</SystemLocale>
<UILanguage>ru-RU</UILanguage>
<UILanguageFallback>ru-RU</UILanguageFallback>
<UserLocale>ru-RU</UserLocale>
</component>
<component name="Microsoft-Windows-Setup" processorArchitecture="x86"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<DiskConfiguration>
<Disk wcm:action="modify">
<CreatePartitions>
<CreatePartition wcm:action="modify">
```

<Order>1</Order>
<Extend>false</Extend>
<Type>Primary</Type>
<Size>20000</Size>
</CreatePartition>
</CreatePartitions>
<DiskID>0</DiskID>
<WillWipeDisk>false</WillWipeDisk>
</Disk>
<WillShowUI>Never</WillShowUI>
</DiskConfiguration>
<ImageInstall>
<OSImage>
<InstallFrom>
<Credentials>
<Domain>volik.com</Domain>
<Password>Pa$$w0rd</Password>
<Username>Администратор</Username>
</Credentials>
</InstallFrom>
<InstallTo>
<DiskID>0</DiskID>
<PartitionID>1</PartitionID>
</InstallTo>
<InstallToAvailablePartition>true</InstallToAvailablePartition>
<WillShowUI>OnError</WillShowUI>
</OSImage>
</ImageInstall>
<WindowsDeploymentServices>
<ImageSelection>

<InstallTo>
<DiskID>0</DiskID>
<PartitionID>1</PartitionID>
</InstallTo>
<InstallImage>
<Filename>Directorate.wim</Filename>
<ImageName>Directorate</ImageName>
<ImageGroup>GROUP</ImageGroup>
</InstallImage>
</ImageSelection>
<Login>
<Credentials>
<Domain>volik.com</Domain>
<Password>Pa$$w0rd</Password>
<Username>Администратор</Username>
</Credentials>
</Login>
</WindowsDeploymentServices>
<Restart>Restart</Restart>
</component>
</settings>
<cpi:offlineImage cpi:source="wim://server8/reminst/images/%D0%BE%D1%82%D0%B4%D0%B5%D0%BB%20it.wim#Windows 7 ENTERPRISE" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>

Приклад файла-відповіді IMAGE UNATTEND.xml для фінальних етапів конфігурації системи «Дирекція»:

<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">

<settings pass="oobeSystem">
<component name="Microsoft-Windows-International-Core" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<InputLocale>en-us</InputLocale>
<SystemLocale>ru-ru</SystemLocale>
<UILanguage>ru-ru</UILanguage>
<UserLocale>ru-ru</UserLocale>
</component>
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<OOBE>
<HideEULAPage>true</HideEULAPage>
<NetworkLocation>Work</NetworkLocation>
<ProtectYourPC>1</ProtectYourPC>
</OOBE>
<UserAccounts>
<LocalAccounts>
<LocalAccount wcm:action="add">
<Password>
<Value>UABhACQAJAB3ADAAcgBkAFAAYQBzAHMAdwBvAHIAZAA=</Value>
<PlainText>false</PlainText>
</Password>
<DisplayName>WinUser</DisplayName>

<Name>WinUser</Name>
<Group>Administrators</Group>
</LocalAccount>
</LocalAccounts>
</UserAccounts>
</component>
</settings>
<settings pass="specialize">
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<RegisteredOwner>Management</RegisteredOwner>
<TimeZone>FLE Standard Time</TimeZone>
<ComputerName>*</ComputerName>
</component>
<component name="Microsoft-Windows-UnattendedJoin" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Identification>
<Credentials>
<Domain>volik.com</Domain>
<Password>Pa$$w0rd</Password>
<Username>Администратор</Username>
</Credentials>
<JoinDomain>volik.com</JoinDomain>
</Identification>

</component>

</settings>

<cpi:offlineImage cpi:source="wim://server8/reminst/images/%D0%BE%D1%82%D0%B4%D0%B5%D0%BB%20it.wim#Windows 7 ENTERPRISE" xmlns:cpi="urn:schemas-microsoft-com:cpi" />

</unattend>

На початку файлу відповідей вказується (версія в нашому випадку "1.0", кодування "utf-8", а так само налаштування самого файлу)

<settings pass="windowspe">// Налаштування для образу WinPE

<component> //Початок компонентів.

//(Ім'я компонента, архітектура, ключ, мова - нейтральний, версія).

Setupuilanguage\Uilanguage (ru-ru) // Під час установки буде використовуватися російська мова.

Inputlocale (0419:00000419) //Під час установки Windows використовувати російську мову.

Systemlocale (ru-ru) //Використовувати російські шрифти й кодові сторінки для програм, що не використовують Unicode.

Uilanguage і Uilanguagefallback (ru-ru) // Використовувати російську мову в інтерфейсі операційної системи.

Userlocale (ru-ru) // Використовувати російський формат для відображення дати й часу, грошових одиниць і чисел.

</component> //Кінець компонентів.

<component> //Початок компонентів.

//(Ім'я компонента, архітектура, ключ, мова - нейтральний, версія).

Diskconfiguration // Конфігурація жорсткого диска.

Disk (wcm:action="modify") // Дія, яку потрібно виконати з диском "Модифікувати"

Createpartitions //Створення розділу.

Createpartition (wcm:action="modify") // Дія яку потрібно виконати з

розділом диска "Модифікувати"

Order (1)// Значення 1 означає, що розділ буде першим у черзі на створення

Extend (false) //Створюваний розділ займе все вільне місце.

Type (Primary)//Створюваний розділ буде основним.

Size (20000) //Розмір дискового простору.

</Createpartition> // Закриття тегу відповідальних за розділ диска.

</Createpartitions> //Закриття тегу відповідальних за розділи диска.

Diskid (0)//Вибір диска (нумерація починається з "0")

Willwipedisk (false) //Не робимо повне очищення диска "тому що він новий і Windows сам його відформатує"

</Disk> //Закріття тегу вибору диска.

Willshowui (Never)// Не відображати меню вибору жорсткого диска.

</Diskconfiguration> //Закріття тегу конфігурації диска.

<Imageinstall> //Тег відповідальний за установку образа.

<Osimage> - Тег відповідальний за вибір образа операційної системи.

<Installfrom> //Тег відповідає за те, від кого установлюється образ.

<Credentials> // Вказуються повноваження.

<Domain> (volik.com) // Вказується домен у якому розташовується користувач від імені якого буди здійснюється Встановлення.

<Password > (********) // Пароль користувача.

<Username>// (Адміністратор). Ім'я користувача від імені якого будевиконаються Встановлення образа.

</Credentials> //Закріття тегу відповідального за повноваження.

<Installfrom> // Закріття тегу відповідального за те, від кого буде установлюється образ.

<Installto> // Куди буде виконуватися Встановлення.

<Diskid> (0) // ідентифікатор диска, 0- Встановлення на 1- й диск.

<Partitionid> (1)// розділ на який буде виконуватися Встановлення 1- й розділ.

</Installto> // Закриття тегу відповідального за те, куди буде виконуватися Встановлення.

<Installtoavailablepartition> (true)

</Installtoavailablepartition>

<Willshowui> (Onerror) // Відображати меню вибору жорсткого диска у випадку помилки.

</Willshowui>.

</Osimage> -

</Imageinstall> -.

<Windowsdeploymentservices> //Конфігурація вибору образа.

<Imageselection>

<Installto>

<Diskid>0</Diskid> // Установити на перший диск тому що диски нумеруються з "0".

<Partitionid>1</Partitionid> // На який розділ диска встановлювати ОС

</Installto>.

<Installimage> // Відповідає за те який образ установлювати.

<Filename>Directorate.wim</Filename> // Тут вказується ім'я файлу образа.

<Imagename>Directorate</Imagename> // Тут вказується ім'я образа.

<Imagegroup>GROUP</Imagegroup> // Тут вказується група в якій перебуває образ.

</Installimage>

</Imageselection>

<Login>

<Credentials> // Вказуються повноваження.

<Domain>volik.com</Domain> //Назва домену.

<Password>Pa$$w0rd</Password> // Пароль користувача.

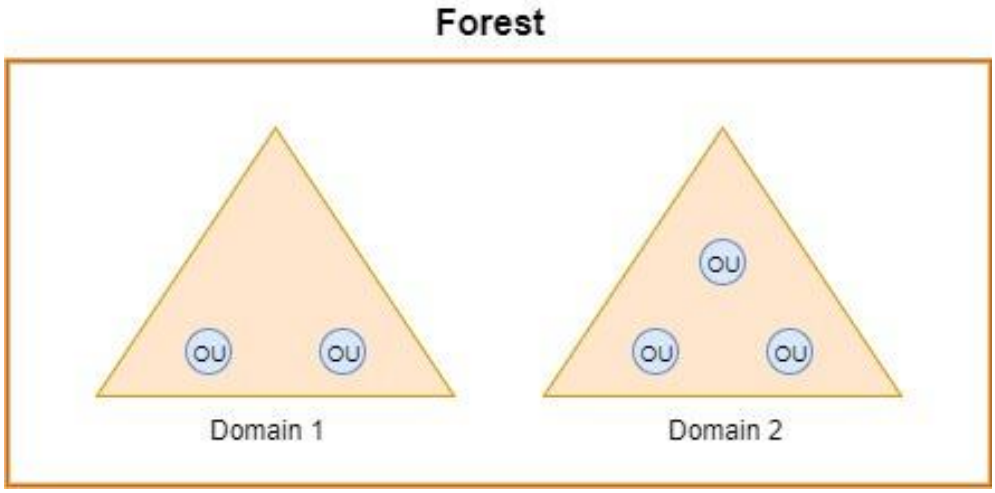
<Username>Адміністратор</Username> // Ім'я користувача.

</Credentials> Закриття тегу повноважень.

</Login>

Домени які було використано:

Домени й ліси



DNS:

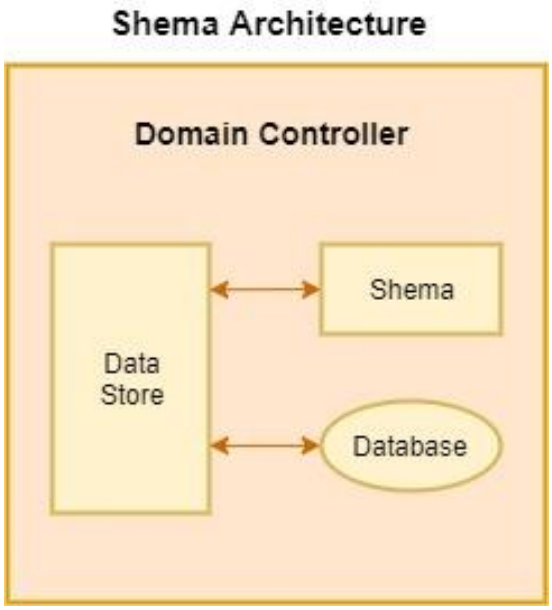
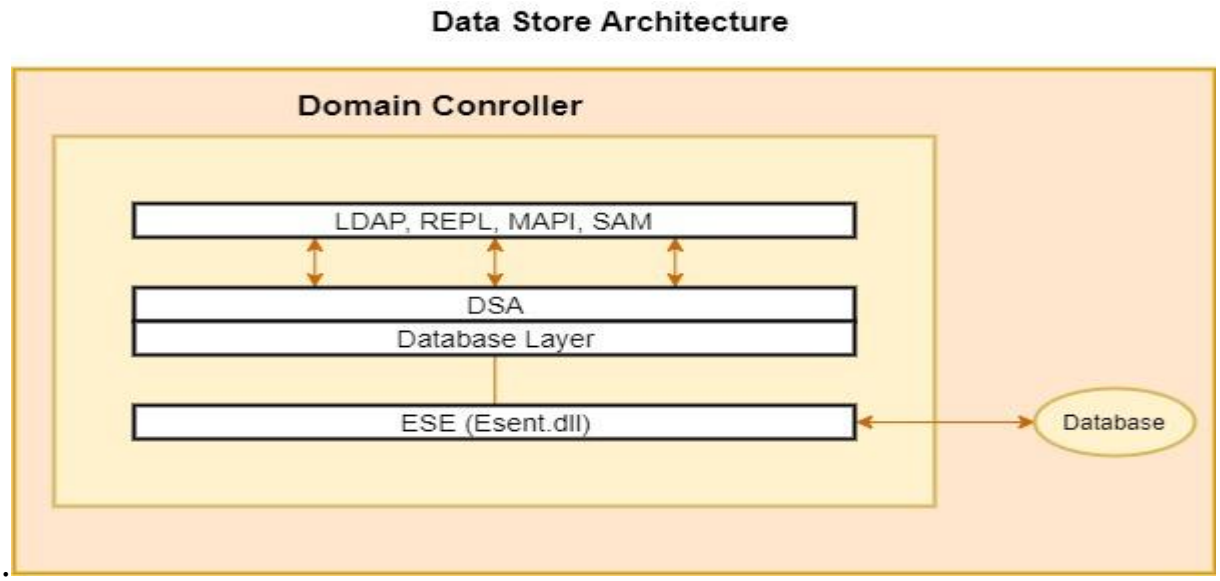
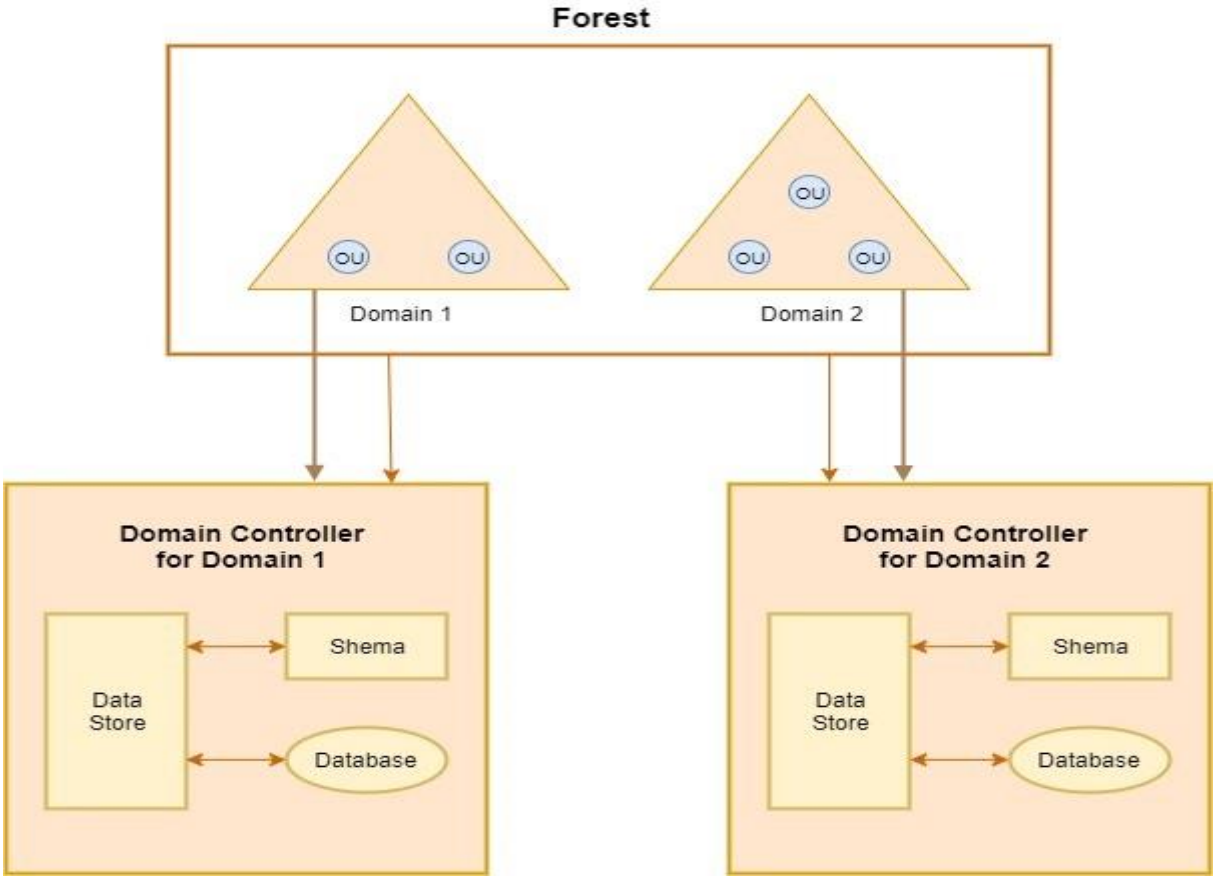


Схема містить визначення об’єктів, які було використано для створення об’єктів, які зберігаються у каталозі:


Data Store Architecture
Domain Conroller
LDAP, REPL, MAPI, SAM
DSA
Database Layer
ESE (Esent.dll)
Database

.

Data Store:


Forest
OU
OU
OU
OU
OU
Domain 1
Domain 2
Domain Controller for Domain 1
Data Store
Shema
Database
Domain Controller for Domain 2
Data Store
Shema
Database