Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система авторизації користувачів на основі Active Directory MS Windows Server
Назва теми

КвРКІ.170238.17.02.06 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія»*
Назва

Виконав: студент IV курсу, група КІ–17–2 _____ Я. А. Дишкантюк
Підпис — Ініціали, прізвище

Керівник _____ С. В. Мостовий
Підпис, дата — Ініціали, прізвище

Нормоконтролер _____ І. В. Муляр
Підпис, дата — Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки та
комп'ютерних систем і мереж _____ Ю. П. Кльоц
Підпис — Ініціали, прізвище

« 24 » червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Програмування та комп'ютерних і телекомунікаційних систем

Кафедра Кібербезпеки та комп'ютерних систем і мереж

Освітній рівень Бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123Комп'ютерна інженерія

Освітня програма Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри Ю. П. Кльоц

"05" 022021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Дишкантюку Ярославу Андрійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи)Система авторизації користувачів на основі Active Directory MS WindowsServer

Керівник проекту (роботи)Мостовий С.В., к.т.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 17.02.2021 р. № 44

2. Строк подання студентом проекту (роботи) на кафедру 17.06.2021 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналітична частина: опис придметної області та постановка завдання

Методологічні підходи до вирішення задачі за темою дослідження

Проектна реалізація

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Логічнамодель Active DirectoryServices (E1)

Логічна модель додатку системи авторизації (E2)

Логічна модель відносин доменів, дерев та лісів (E3)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Муляр І. В., доцент кафедри КбКСМ		
Антиплагіат	Муляр І. В., доцент кафедри КбКСМ		

7. Дата видачі завдання « 08 » 02 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	Березень – 1 декада	
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	Березень – 2 декада	
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	Квітень – 1 декада	
4	Робота над розділом 2 – вибір елеметної бази для створення модуля вимірювання радіації	Квітень – 2 декада	
5	Робота над розділом 3 – проектна реалізація та програмування компонентів системи	Квітень – 4 декада	
6	Оформлення графічного матеріалу	Травень – 2 декада	
7	Оформлення пояснювальної записки згідно вимог	Травень – 3 декада	
8	Попередній захист ВКР	Травень – 3 декада	
	Подання роботи для перевірки на плагіат	Червень – 1 декада	
9	Захист ВКР на засіданні ЕК	Червень – 2 декада	

Студент Підпис Дишкантюк Я.А
Ініціали, прізвище

Керівник проекту (роботи) Підпис Мостовий С.В.
Ініціали, прізвище

№	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
2		КвРКІ.170238.02.06 ПЗ	Пояснювальна записка	64		
			Графічні матеріали			
5		КвРКІ.170238.02.06 Е1	Логічна модель Active Directory Services	1		
7		КвРКІ.170238.02.06 Е2	Логічна модель додатку системи авторизації	1		
9		КвРКІ.170238.02.06 Е3	Логічна модель відносин доменів, дерев та лісів	1		
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						

Зм	Арк	№ докум	Підпис	Дата	КРКІ.170238.02.06 ВП		
Розробив		Дишкантюк Я.А.			Система авторизації користувачів на основі Active Directory MS Windows Server Відомість проекту	Літера	Аркуш 1 / Аркушів 1
Перевір.		Мостовий С.В.				У	
Н.контр.		Муляр І.В.				ХНУ, КІ-17-2	
Затв.		Кльоц Ю.П.					

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система авторизації користувачів на основі Active Directory MS Windows Server».

Автор роботи: Дишкантюк Ярослав Андрійович.

Керівник роботи: Мостовий Сергій Вікторович.

Пояснювальна записка: 64 с., 6 рис., 2 дод., 20 джерел.

Графічна частина: 3 плаката.

СИСТЕМА АВТОРИЗАЦІЇ КОРИСТУВАЧІВ НА ОСНОВІ ACTIVE DIRECTORY MS WINDOWS SERVER

Метою роботи є розробка системи авторизації користувачів на основі Active Directory Ms Windows Server.

У даному дипломному проекті розроблено систему авторизації користувачів на основі Active Directory Ms Windows Server, яка відповідає вимогам, поставленим у технічному завданні. У ході виконання проектування розроблено логічну модель Active Directory Services, логічну модель додатку системи авторизації.

Проект виконано в повному обсязі, здійснені розрахунки й моделювання підтверджують працездатність системи авторизації користувачів на основі Active Directory Ms Windows Server та задовольняються вимогами ТЗ. Проведені тестування підтверджують справність та правильність конструкторських рішень при проектуванні системи авторизації.

Підпис студента

10.06.2021
Дата

ВСТУП

У наш час майже всі підприємства обладнані персональними комп’ютерами, та під’єднані до комп’ютерних мереж. Для забезпечення високої якості обслуговування, та відповідного рівня надання послуг потрібно забезпечити стабільну та безперебійну роботу комп’ютерної мережі, це можливо за допомогою використання високоякісного обладнання та відповідного програмного забезпечення.

Два або більше комп’ютерів пов’язаних між собою засобами зв’язку для передач інформації є мережею. Мережі класифікуються, або за протоколом зв’язку, або за протоколом зв'язку, або за топологією. Протокол зв'язку визначає закони та формати даних для обміну інформацією в комп’ютерній мережі. Серед відомих протоколів є Ethernet, який широко використовується в локальних мережах.

Наприкінці 1960-х років Гавайський університет створив розгалужену мережу під назвою ALOHA. Метою університету було з'єднання комп'ютерів, розповсюджених по кампусу. Найважливішою особливістю цієї моделі мережі на сьогоднішній день є техніка, яка називається CSMA \ CD . Відкрите виявлення носія CSMA \ CD, багаторазовий доступ із виявленням змови.

Множинний доступ визначає, що до одного кабелю можна підключити кілька комп’ютерів. Виявлення зіткнень - це захід безпеки, який вживається для запобігання зіткненню даних на лінії. Цей старовинний дизайн мережі є основою сучасного Ethernet.

У 1972 році компанія XEROX випустила першу карту Ethernet для експериментальних цілей, а в 1975 році випустила перший продукт Ethernet. Оригінальна версія цього продукту була розроблена для підключення понад 100 комп'ютерів за допомогою кабелю протяжністю 1 км зі швидкістю 2,95 Мбіт / с. Картка XEROX Ethernet була дуже успішною. Intel, Xerox та Digital встановили новий стандарт для Ethernet 10 Мбіт / с. Цей створений стандарт демонструє велику схожість із прийнятим сьогодні стандартом IEEE 802.3.

Ethernet - це форма кабелю та сигналізації, що з'єднує системи в локальній мережі. Модель OSI діє на основі комп'ютерного зв'язку .

Ethernet, який був визначений у перших двох шарах (шар 1 -фізичний та шар-дані-посилання-) при моделюванні OSI, був вперше опублікований у `` Blue Book Standard for Ethernet Version I. " (Standard Blue Book), а випущена книга, що описує стандарти, що використовуються цією версією.

Серед стандартів, описаних тут, є методика "базової смуги", стандарт мережі CSMA / CD (Carrier Sense Multiple Access / Collision Detect) і стандарти використання коаксіального кабелю, які використовувались у перші дні Ethernet і широко застосовувались для багатьох років . Пізніше цей стандарт було переглянуто з новим стандартом під назвою Ethernet II, який був випущений в 1985 році.

Версія Ethernet II заснована на проекті 802 IEEE (Інститут інженера електротехніки та електроніки) та формуванні стандарту мережі 802.3 CSMA / CD. Як правило, ці два посилання є взаємозамінними, оскільки вони не мають різниці, крім заголовка на початку пакета Ethernet.

Наземна мікрохвильова лінія використовує діапазон низьких гігагерц . Мікрохвильові антени зазвичай розміщують поверх будівель, веж, пагорбів і гірських вершин.

Основним завданням мережевого рівня є маршрутизація. Коли передані блоки даних надходять на мережевий рівень, вони називаються пакетами. Процес маршрутизації дозволяє відправляти пакети в інші комп’ютерні мережі поза локальною мережею.

Для керування та забезпечення захищеного доступу до ресурсу необхідно розробити систему авторизації, в цьому і полягає актуальність теми нашої роботи.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз предметної області

Active Directory (AD) - це служба каталогів, розроблена корпорацією Майкрософт для доменних мереж Windows. Він включений до більшості операційних систем Windows Server як набір процесів та служб. Спочатку Active Directory відповідала лише за централізоване управління доменом. Однак Active Directory стала загальною назвою для широкого кола служб, пов'язаних з ідентифікацією на основі каталогів.

Сервер, на якому запущена роль доменної служби Active Directory (AD DS), називається контролером домену. Він здійснює автентифікацію та авторизацію всіх користувачів та комп’ютерів у мережі типу домену Windows. Призначення та застосування політик безпеки для всіх комп’ютерів та встановлення або оновлення програмного забезпечення. Наприклад, коли користувач входить на комп’ютер, який є частиною домену Windows, Active Directory перевіряє надісланий пароль і визначає, чи є користувач системним адміністратором чи звичайним користувачем. Крім того, це дозволяє керувати та зберігати інформацію, забезпечує механізми автентифікації та авторизації та встановлює структуру для розгортання інших супутніх служб: Сертифікаційні служби, Служби федерації Active Directory, Полегшені служби каталогів та Служби управління правами [1].

Active Directory використовує Lightweight Directory Access Protocol (LDAP) версії 2 і 3, версія Microsoft по Kerberos, і DNS.

По-простому можна сказати, що це послуга, створена на одному або декількох серверах, де створюються такі об'єкти, як користувачі, комп'ютери або групи, з метою управління входами на комп'ютерах, підключених до мережі, а також управління політикою в мережі.

Його ієрархічна структура дозволяє підтримувати низку об’єктів, пов’язаних із компонентами мережі, такими як користувачі, групи користувачів, дозволи та розподіл ресурсів та політики доступу.

Active Directory дозволяє адміністраторам встановлювати загальнофірмові політики, розгортати програми на багатьох комп’ютерах та застосовувати критичні оновлення для всієї організації. Active Directory зберігає інформацію про організацію в центральній, організованій та доступній базі даних. Їх можна знайти від каталогів із сотнями об’єктів для невеликої мережі до каталогів з мільйонами об’єктів.

Active Directory, як і NIS , виникла з-за необхідності мати єдиний каталог, тобто замість того, щоб користувач мав пароль для доступу до основної системи компанії, пароль для читання своїх електронних листів, пароль для входу в комп'ютер та кілька інших паролів, використовуючи AD, користувачі можуть мати лише один пароль для доступу до всіх ресурсів, доступних у мережі. Ми можемо визначити каталог як базу даних, що зберігає інформацію про користувачів.

AD вийшов разом із Windows 2000 Server. Такі об'єкти, як користувачі, групи, члени групи, паролі, облікові записи комп'ютерів, трасти, інформація про домен, організаційні підрозділи тощо зберігаються в базі даних AD. Окрім зберігання декількох об'єктів у своїй базі даних, AD надає кілька послуг, таких як: автентифікація користувачів, реплікація бази даних, пошук об'єктів, доступних у мережі, централізоване адміністрування безпеки за допомогою GPO, серед інших послуг. Ці функції значно полегшують адміністрування AD, завдяки чому можна централізовано адмініструвати всі ресурси, доступні в мережі.

Щоб користувачі мали доступ до ресурсів, доступних у мережі, вони повинні увійти в систему. Коли користувач входить в систему, AD перевіряє, що інформація, надана користувачами, є дійсною, і якщо так, то він перевіряє справжність. AD організована ієрархічно, з використанням доменів. Якщо мережа використовує AD, вона може містити кілька доменів. Домен - це не що інше, як адміністративні та захисні межі, тобто адміністратор домену має дозволи лише на домен, а не на інші домени. Політика безпеки також застосовується лише до

домену, а не до інших доменів. Коротше кажучи: різні домени можуть мати різних адміністраторів та різні політики безпеки.

У доменах, заснованих на AD, ми можемо мати два типи серверів: Контролер домену (DC - Контролер домену) та Сервер-член (Сервер-член).

Для встановлення AD необхідно, щоб послуга DNS була доступна, тобто вона є необхідною умовою (залежністю) для установки AD. AD використовує DNS для іменування серверів та ресурсів, а також для дозволу імен. Якщо служба DNS недоступна в мережі під час встановлення AD, ми можемо встановити її під час встановлення AD.

Використовуючи домени, ми можемо зробити так, щоб наша мережа відображала структуру компанії. Коли ми використовуємо кілька доменів, ми маємо концепцію довірчих відносин. Довірчі відносини дозволяють користувачам обох доменів отримувати доступ до ресурсів, розташованих у цих доменах. У Windows 2000 довіра є двонаправленою та транзитивною, тобто якщо домен X довіряє домену Y, а Y довіру W, домен X також довіряє домену W.

Щоб дозволити користувачам одного домену доступ до ресурсів іншого домену, Active Directory використовує довірчі відносини . Довірчі відносини створюються автоматично при створенні нових доменів. Межі довірчих відносин позначаються не доменом, а лісом, до якого вони належать. Існують транзитивні довіри, де довіри Active Directory можуть бути ярликом (об’єднує два домени в різних деревах, перехідний, одно- або двосторонній), лісовий (перехідний, одно- або двосторонній), сфера (перехідна чи неперехідна, одностороння або двосторонній) або зовнішній (неперехідний, односторонній або двосторонній) для підключення до інших лісів або доменів, що не належать до Active Directory. Active Directory використовує протокол Kerberos V5, хоча він також підтримує NTLM та веб-користувачів за допомогою аутентифікації SSL / TLS .

Active Directory дозволяє адміністраторам призначати загальну політику компанії , встановлювати програми на великій кількості комп’ютерів та застосовувати критичні оновлення до всієї організації. "Активний каталог" зберігає інформацію та параметри в організованій та доступній центральній базі даних .

Мережевий каталог , активний може варіюватися від невеликої установки з сотнею об'єктів, в більшу установку з мільйонами об'єктів. Попередній перегляд Active Directory відбувся в 1999 році і вперше був випущений з Windows 2000 . Пізніше його було переглянуто з метою розширення його функціональних можливостей та вдосконалення адміністрування до нової версії, відомої як "Windows Server 2003". Також присутній у Windows Server 2008.

Active Directory - це набір файлів, розташованих на сервері домену, який містить всю інформацію, що дозволяє контролювати доступ користувачів до мережі. У ньому реєструються імена та паролі користувачів, їх дозволи на доступ до файлів, принтерів та інших мережевих ресурсів, квоти дисків, комп'ютери та час, який кожен користувач може використовувати тощо.

1.2 Структура каталогу Active Directory

Active Directory (AD) складає інформацію про мережеві послуги у деревоподібній структурі даних. У простому мережевому середовищі (наприклад, у невеликій компанії) зазвичай існує лише один домен. У середній або великій мережі домен може бути багато, або пов'язані з AD інших компаній чи організацій.

Найменший одиниця зберігання Active Directory - це об'єкт. Кожен об'єкт має власний атрибут схеми і може зберігати різні дані, такі як користувачі, групи, комп'ютери, поштові скриньки чи інші основні об'єкти.

Основними об'єктами під доменом AD є наступні типи:

- Контролери домену, які зберігають контролер домену (DC, контролер домену), до якого належить домен.
- Комп'ютери, зберігає об'єкти комп'ютера, додані до домену.
- Вбудовано, зберігає вбудовану групу облікових записів.
- Користувачі, зберігає об'єкти користувачів в AD.

Якщо компанії потрібно керувати обліковим записом компанії з іншою організаційною структурою, в AD можна створити один або кілька організаційних

підрозділів (Організаційний підрозділ, що називається OU). Організаційний підрозділ - це об’єкт Active Directory з можливостями зберігання (він знаходиться в ADSI (це інтерфейс IADsContainer), ви можете зберігати об’єкти AD в OU, включаючи користувачів, групи, комп’ютери тощо, щоб організаційна структура могла бути по-справжньому відображена в AD, а також зручно для іншої функції в AD - груп Застосування та централізоване управління груповою політикою [2].

Якщо мережеве середовище організації дуже велике і складне, доменів може бути багато. У AD може бути один або кілька доменів, і велика компанія може використовувати філії або відділення для організації об’єктів домену. Таким чином, буде кілька доменів в AD. Якщо вам потрібно надати спільний доступ до даних або виконати делеговані параметри керування та конфігурації в доменах, вам потрібно встановити організаційні відносини між собою. Microsoft додасть більше до AD ієрархічні відносини між доменами називаються деревом доменів. Структура дерева доменів відрізняється ідентифікацією DNS. Наприклад, компанія може мати бізнес-відділи, інженерні підрозділи та відділи управління.

У багатодоменному середовищі може знадобитися обмін та обмін даними між різними доменами, такими як налаштування конфігурації, облікові записи користувачів, налаштування групової політики тощо. На даний момент потрібна роль, яка виконує роль обміну інформацією між різними доменами також має відповідати специфікації деревоподібної структури AD.Тому Microsoft встановила посередницьку роль між кількома доменами, що називається Forest, і організація може лише Існує Forest, під Лісом знаходяться їхні відповідні доменні ліси, а під Forest, інформація може обмінюватися між доменами або між доменами лісів.

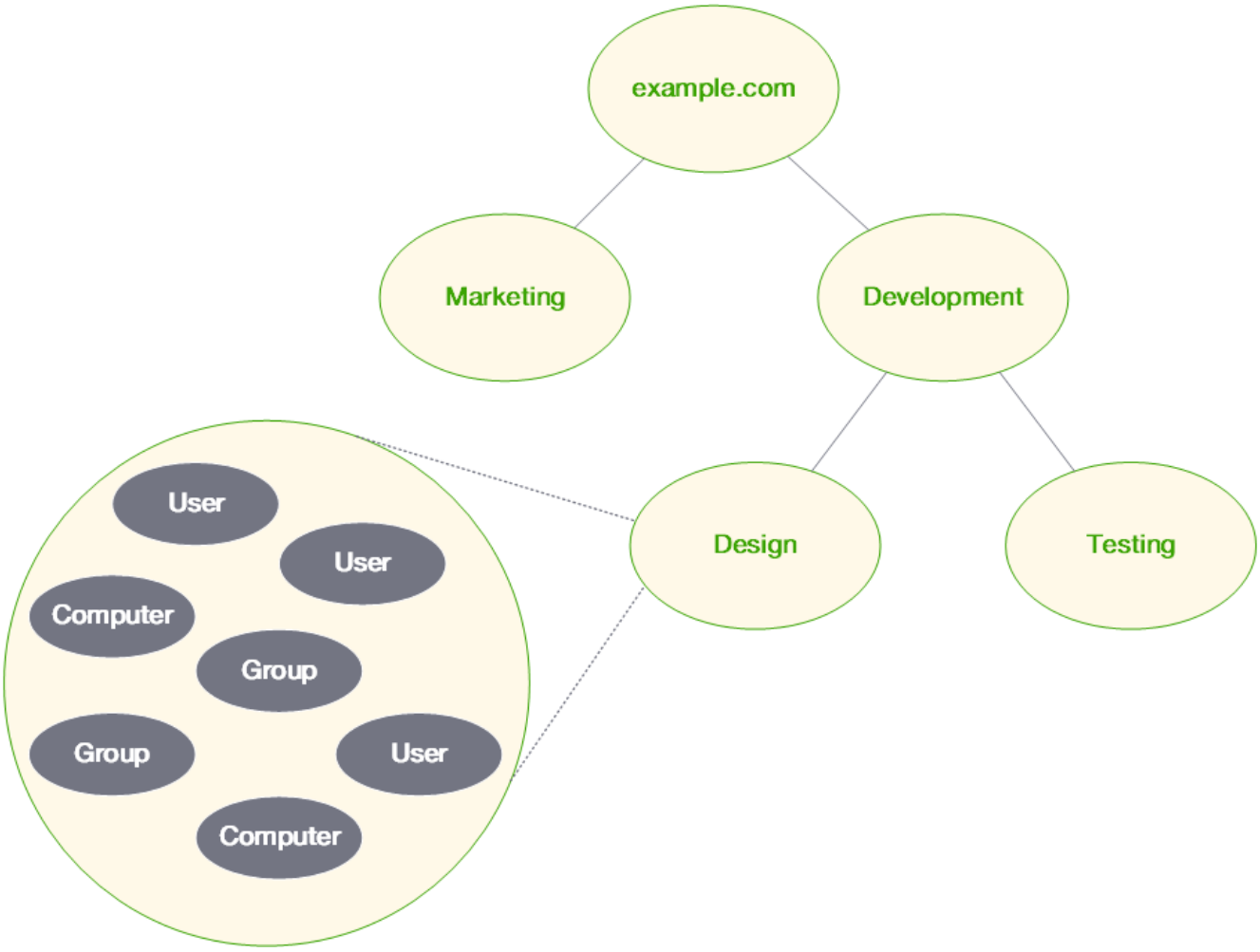


Рисунок 1.1 – Ієрархія об’єктів Active Directory

1.3 Фізична структура Active Directory

За Active Directory стоїть мережевий сервіс та метод зв'язку, заснований на мережевій інфраструктурі Windows Server (інфраструктура). Ієрахію об’єктів Active Directory зображено на Рисунку 1.1. Ці мережеві служби та методи зв'язку дозволяють Active Directory мати високий ступінь масштабованості та зворотної сумісності. Мережеві адміністратори повинні належним чином налаштувати та контролювати мережевих служб та методів зв'язку, щоб Active Directory могла працювати нормально та безперебійно.

У попередньому середовищі домену Windows NT фізична структура домену ділиться на три ролі, а саме: основний контролер домену (Primary Domain Controller, PDC), резервний контролер домену (Backup Domain Controller, BDC) та сервер-член. (Член-сервер) трьох типів, дані домену зберігаються в PDC і BDC, а

дані обмінюються між PDC і BDC, але спосіб розгортання PDC і BDC незручний (домен може мати лише один PDC). PDC може не буде налаштовано в географічному середовищі, і всі запити домену будуть спрямовані на PDC, тому легко викликати затори при вході та доступі домену. Ця проблема була покращена в Active Directory, тобто більше немає BDC (Є лише дві ролі: DC і Server Server), будь-який контролер домену в домені може відповідати за обробку запитів домену від клієнта, тому він матиме значну гнучкість у розподіленому розгортанні.

У фізичній структурі AD найважливіша роль відводиться не Глобальному каталогу (Глобальний каталог, скорочено GC). Він зберігає найповніші дані про структуру Active Directory, а також підтримує каталог. Основна тема запиту програми до нашої ери, і, як правило, в різних географічних місцях (наприклад, у Китаї, Тайвані, США та Великобританії кожен має свої філії, і кожен має домен), GC відіграє важливу роль у структурі кеш-пам'ятки. до філії Великобританії та намагається увійти до домену, Windows спочатку шукатиме найближчий сервер глобальних каталогів (надається налаштуваннями DNS). Якщо він не може його знайти, він підключиться до GC в інших регіонах. Якщо мережа філії повільно, цей вид міжгеографічного доступу до даних AD безпосередньо вплине на час входу в систему, тому ретельне розгортання GC дуже важливо для впровадження AD [3].

Операційний хост (Operations Masters, також відомий як гнучка одноопераційна операція, а саме FSMO) встановлюється як контролер домену, щоб забезпечити певну роль інформації в кожному домені Active Directory, принаймні є три основні операційні символи.

- Основний контролер емулятора контролера домену: контролер домену, встановлений як ця роль, може бути викликаний контролером домену Windows NT Backup (контролер доменного резервного копіювання), що все ще існує в домені, як основний контролер домену (основний контролер домену). Він використовується, і він також є хостом, який забезпечує синхронізацію часу служби служби часу Windows у лісі.

- RID Master: відносний ідентифікатор (пов’язаний ідентифікаційний код) об’єктів AD зберігатиметься в контролері домену, що може розпорошити трафік запитів на основі RID.
- Майстер інфраструктури: відповідає за обробку посилань на об’єкти до поточного домену та посилань на об’єкти, що відповідають іншим доменам, і може нести відповідальність за обробку змін об’єктів AD (таких як видалення та перейменування).

Є також дві ролі, які мають додаткові функції, але не є обов’язковими для розгортання в домені:

- Майстер схеми: відповідає за обробку всіх змін об’єктної структури в домені.
- Майстер імен доменів: відповідає за обробку розділів каталогів та розділення каталогів програм у домені.

Сайт Active Directory (сайт) відноситься до мережевого розташування сутності. На сайті може бути багато контролерів домену. Реплікація даних домену AD базується на сайті, а інструмент, який насправді обробляє реплікацію, називається KCC (Знання Перевірка узгодженості, перевірка узгодженості знань), він буде синхронізувати дані домену в налаштуваннях сайту в певний час, дії реплікації поділяються на внутрішню реплікацію (внутрішньосайтова реплікація) та зовнішню реплікацію (Або реплікацію між сайтами, внутрішню реплікація - це обмін інформацією між контрольними станціями в одному домені, зовнішня реплікація встановлюється адміністратором мережі за допомогою призначеного способу зв'язку (IP або SMTP), а топологія копіюється.

За замовчуванням метод зв'язку станції полягає у використанні IP (RPC через IP) для зв'язку.Цей метод є найшвидшим, і TCP / IP можна використовувати для віддалених дзвінків та обробки, але якщо це недоменні дані (Архітектура Метод зв'язку SMTP можна використовувати для реплікації, налаштувань та загальних оновлень каталогу (тобто без об'єктів AD) , але цей метод вимагає створення служби сертифікатів на рівні підприємства, перш ніж його можна буде використовувати. забезпечити підтвердження та збереження даних SMTP.

У середньому та великому мережевому середовищі важливо належним чином розподілити мережевий трафік та спроектувати топологію мережі. KCC використовуватиме встановлену вартість мережі (вартість) для вибору, яку мережу використовувати. Реплікація, наприклад, може існувати Лінія T1 та ISDN 64 Кбіт / с між компанією та офісом , а вартість T1 встановлена на 500 (оскільки буде багато трафіку), а ISDN - лише 100, KCC вибере ISDN для реплікації, що представляє мережу Адміністратор може вирішити, яку мережу використовувати для реплікації. Алгоритм реплікації KCC визначить, яка мережа найбільш підходить для копіювання даних AD. Окрім вартості, AD також підтримує структуру мосту сайту. Можливість мосту сайту дозволяє розподілити вартість реплікації, а також може розподілити трафік реплікації того самого GC. Він також підходить для реплікації інформації AD між різні географічні регіони. Робота з розповсюдженням.

Active Directory значною мірою покладається на DNS, оскільки DNS може дозволити AD показувати ієрархічну деревоподібну структуру, а також може відповідати стандартам відкритих каталогів. Тому при побудові домену служба DNS (або інший DNS-сервер) повинна бути налаштована Існуючи в мережі або контролері домену, AD використовує запис SRV для ідентифікації контролера домену для надання послуг з обробки домену. На відміну від домену Windows NT, Windows NT використовує протокол NetBIOS, але AD використовує TCP / IP, але AD все ще забезпечує формат, який може конвертувати між форматом облікового запису Windows NT (DOMAIN \ User) та форматом облікового запису AD (user@domain).

1.4 Фізичне зберігання

Active Directory використовує вдосконалений движок бази даних Microsoft Jet (на основі проекту Microsoft Jet Blue), розширюваний механізм зберігання даних (ESE98), який може зберігати 16 ТБ даних, теоретично може містити один мільярд об'єктів домену, а ім'я файлу - NTDS. Dit , він зберігається в каталозі% system_root% \ NTDS (диск, на якому знаходиться цей каталог, також повинен

бути у форматі NTFS), містить таблицю даних об'єктів і таблицю даних посилань, новий опис інформації про безпеку додано до Windows Паспорт даних сервера 2003.Записи, коли дані оновлення AD зберігаються в edb * .log, ім'я за замовчуванням - edb.log, інші файли записуються з "edb" + число + ".log", а також edb.chk також використовується як журнал контрольних точок і Res1.log та Res2.log як зарезервовані файли системи.

Компонентами, що зберігаються в сутності AD, є:

- Інтерфейс верхнього рівня (інтерфейс): як інтерфейс підключення клієнта служби каталогів або інших серверів служби каталогів, таких як LDAP, REPL, MAPI та SAM.
- Агент служби каталогів (Агент служби каталогів): реалізований у NTDSA.DLL, відповідальний за отримання та обробку запитів від клієнтів або запитів від інших серверів (наприклад, запитів KCC).
- Рівень доступу до бази даних: міститься в ntdsa.dll і відповідає за прямий доступ до бази даних.
- Розширюваний механізм зберігання: відповідає за обробку бази даних та відповідності її імен (DN).
- Файл бази даних: NTDS.dit і файл запису, відповідальний за обробку несанкціонованих транзакцій.

Контролер домену буде регулярно дефрагментувати NTDS.dit (за замовчуванням 12 годин) і очищати сміття у файлі даних, а перед реорганізацією перевірятиме, чи місце на диску в 1,5 рази більше, ніж файл бази даних. Якщо в каталозі, де знаходиться база даних, недостатньо вільного місця, перемістіть базу даних в інше місце. Однак через різницю в механізмі служби тіньового копіювання (VSS) між Windows 2000 та Windows Server 2003 процес переміщення може не вдатися. У Windows 2000 файли журналів та бази даних можуть зберігатися на різних дисках, але Windows Server 2003 повинен зберігатися на одному диску. Щоб перемістити базу даних, потрібно перезапустити сервер, увійти в режим відновлення Active Directory та скористатися інструментом ntdsutil для його переміщення [5].

У Windows Server 2008 була додана нова роль контролера домену, яка називається "Контролер домену лише для читання" (RODC). RODC може використовуватися як філія, філія, офіс організації або як тимчасовий підрозділ тощо. Він використовується, коли є є проблемами безпеки або ризиками, коли там розміщений контролер домену. Як випливає з назви, RODC не буде записувати будь-які дані в Active Directory, а реплікація з іншими доменами також обмежена, і лише облікові записи під контролем реплікації пароля Політика, визначена системним адміністратором, зможе кешувати паролі та інші функції.

Щоб додати контролер домену лише для читання до AD, функціональний рівень домену повинен бути Windows Server 2003 або вище.

1.5 Безпека

Захист Active Directory можна розділити на ідентифікацію безпеки об’єкта, ієрархічну безпеку та довірчі відносини між лісами.

AD використовує Kerberos V5 як основну архітектуру для перевірки безпеки, і кожен об’єкт AD має унікальний ідентифікатор безпеки (SID), приклад формату - S-1-5-21-7623811015-3361044348-030300820 -1013. За своїм значенням ця група ідентифікаційних кодів зберігається в атрибуті objectSid AD.

В AD різні рівні OU можуть визначати різну інформацію про безпеку та різні права користувачів, а різні рівні домену можуть також визначати різні права користувачів, а адміністратори також можуть використовувати шаблони управління безпекою (Secutiy Template) для визначення різної інформації про безпеку або використання групової політики (Групова політика) для визначення. У великій мережі використання групової політики зручніше, ніж шаблон безпеки. Поєднання двох зручніше. Можна досягти результатів множника з половиною зусиль (наприклад, інтеграція з Microsoft Base Security Analyzer).

Захист, визначений у батьківській ієрархії, може успадковуватися дочірньою ієрархією.

У широкомасштабному мережевому середовищі можуть існувати партнерські відносини між організаціями або співпраця між проектами, а коли

потрібен спільний або авторизований доступ між двома лісами, довірчі відносини можуть використовуватися для встановлення довіри між лісами. З метою санкціонування прав доступу між лісами один одного середовище AD Windows Server 2003 та пізніших версій може підтримувати чотири типи відносин довіри:

- Довіра ярликів - це метод довіри, призначений для прискорення процесу перевірки. У багаторівневому домені користувачі можуть входити в систему, якщо вони підключаються до найближчого домену, не надсилаючи повідомлення на авторизований кореневий сервер. Пристрій.
- Зовнішня довіра, яка є методом авторизації між лісами.
- Довіра до сфери (довіра до сфери) використовується як модель довіри для служб каталогів LDAP, не автентифікованих Kerberos, та доменів Windows.
- Лісовий трест. Це вдосконалений зовнішній метод довіри. Довірчі відносини можна отримати через посередницький лісовий трест. Наприклад, acme.com.tw довіряє aspvendor.com, а contoso.com.tw також довіряє aspvendor .com, а потім acme.com.tw може отримати довірчі відносини з contoso.com.tw.

Встановлення довірчих відносин можна розділити на односторонні та двосторонні. Одностороння довіра означає, що довірена сторона може отримати доступ до ресурсів довіреної сторони, тоді як двостороння довіра може отримати доступ до ресурсів довіреної сторони [6].

Ярлик Trust є по суті явним довірою, яке створює ярлики між двома доменами в доменній структурі. Цей тип відносин дозволяє збільшити зв’язок між двома доменами, зменшити кількість запитів та час очікування на автентифікацію. Передачу довірчих відносин можна розділити на два типи: перехідні та неперехідні. Перехідні означають, що домен, що встановлює довірчі відносини, також може використовуватися для встановлення довіри до інших доменів у тому самому лісі, що не підлягає передачі означає, що лише домен (незалежно від ієрархії чи ні), який встановлює довірчі відносини, може використовувати інформацію про довіру.

Стандартне іменування Active Directory базується на версії протоколу X.500 LDAP. Для служби каталогів такого масштабу, як AD, протоколи LDAP з

ієрархічними можливостями ідентифікації дуже підходить в якості протоколів доступу до служб каталогів, але AD може також підтримувати формат UNC епохи NT (надається постачальником послуг AD Каталог служб Windows NT), а перетворення між іменами UNC та LDAP здійснюється за допомогою `IADsNameTranslate` інтерфейсу ADSI.

Службові інтерфейси Active Directory (ADSI) надають програмісту об'єктно-орієнтований інтерфейс, що полегшує створення програм каталогів за допомогою деяких високорівневих мовно сумісних інструментів, таких як Visual Basic, без необхідності мати справу з різними просторами імен.

За допомогою ADSI можна створювати програми, які здійснюють єдиний доступ до декількох ресурсів у мережевому середовищі, незалежно від того, засновані вони на LDAP або іншому протоколі. Крім того, це дозволяє створювати сценарії для адміністраторів.

Ви також можете розробити інтерфейс обміну повідомленнями (MAPI), який дозволяє створювати програми MAPI.

1.6 Функціональна ієрархія

Отже, Active Directory є відкритою службою каталогів, і для того, щоб мати можливість розміщувати різні версії операційної системи Windows та її доменів, механізм контролю версій використовується особливо в AD, який називається функціональним рівнем (функціональний рівень). максимальний рівень версії, який зараз можна використовувати в середовищі домену, і ця модифікація є односторонньою модифікацією, яку не можна скасувати. Якщо в домені є контролери домену з різними версіями операційних систем, для максимальної сумісності параметр функціонального рівня повинен базуватися на найнижчій версії. Наприклад, якщо в домені є Windows Server 2003 та Windows 2000, то функціонал рівень домену має бути змішаним режимом Windows 2000. Якщо встановлено рідний режим Windows Server 2003, контролер домену Windows 2000 вийде з ладу. Однак, оскільки нова версія налаштувань AD зазвичай сильніша за

попередню версію (особливо поліпшення безпеки), якщо в домені немає попередньої версії операційної системи, рівень функції слід встановити на останню версію, щоб відкрити функції AD All.

Крім того, якщо ви хочете встановити нову версію операційної системи в домен (наприклад, встановити Windows Server 2008 у домені Windows Server 2003) як контролер домену, спочатку потрібно розгорнути інформацію про схему в Active Directory до Сумісний із новішими версіями операційних систем, тому Microsoft надасть на інсталяційному компакт-диску інструмент підготовки Active Directory (adprep.exe), що дозволяє системним адміністраторам просте оновлення структури даних в Active Directory, включаючи ліс та Структура даних домену (з використанням параметрів параметрів), щоб бути сумісною з новою версією операційної системи.

- adprep /forestprep: Оновити структуру даних лісу.
- adprep /domainprep: Оновіть структуру даних домену.
- adprep /rodcprep: Підготуйте домен, щоб забезпечити функцію RODC (контролер домену лише для читання) (підтримується лише після Windows Server 2008).

Для BDC Windows NT для підтримки сумісності підтримується не встановлення функціонального рівня, а емулятор PDC майстра операцій.

Оскільки Microsoft розробляє Active Directory для використання служби відкритих каталогів як свою політику, і однією з найосновніших характеристик служб каталогів є можливість "приймати всі річки", крім основних даних мережевих служб, її також потрібно можливість бути сумісним з іншим підключенням послуг та інтеграцією, таким чином, Microsoft впровадила пристрій для зберігання об'єкта в AD, називається «схема». структура об'єкта може розглядатися як метадані об'єктів AD. Кожен об'єкт (будь то одиниця або об'єкт-контейнер) має власну схему для зберігання різних даних, що ідентифікують об'єкт. Схема складається з класу та атрибута. Атрибут - це найменший блок зберігання, а клас містить атрибути [7].

Дані, що зберігаються в атрибуті, мають багато форматів. Microsoft визначає ці формати у 27 типів даних схеми, таких як Account-Expiresатрибути, що вказують дату закінчення терміну дії облікового запису. Ціле число, ще один приклад sAMAccountNameатрибута, що вказує ім'я SAM рахунку, його значенням є значення String (Unicode) (значення рядка, яке підтримує Unicode), а іншим прикладом Pictureатрибута, що зберігає фотографію користувача, є значення Object Repl-Link, що представляє собою байтові дані, і їх можна скопіювати в інші контролери домену).

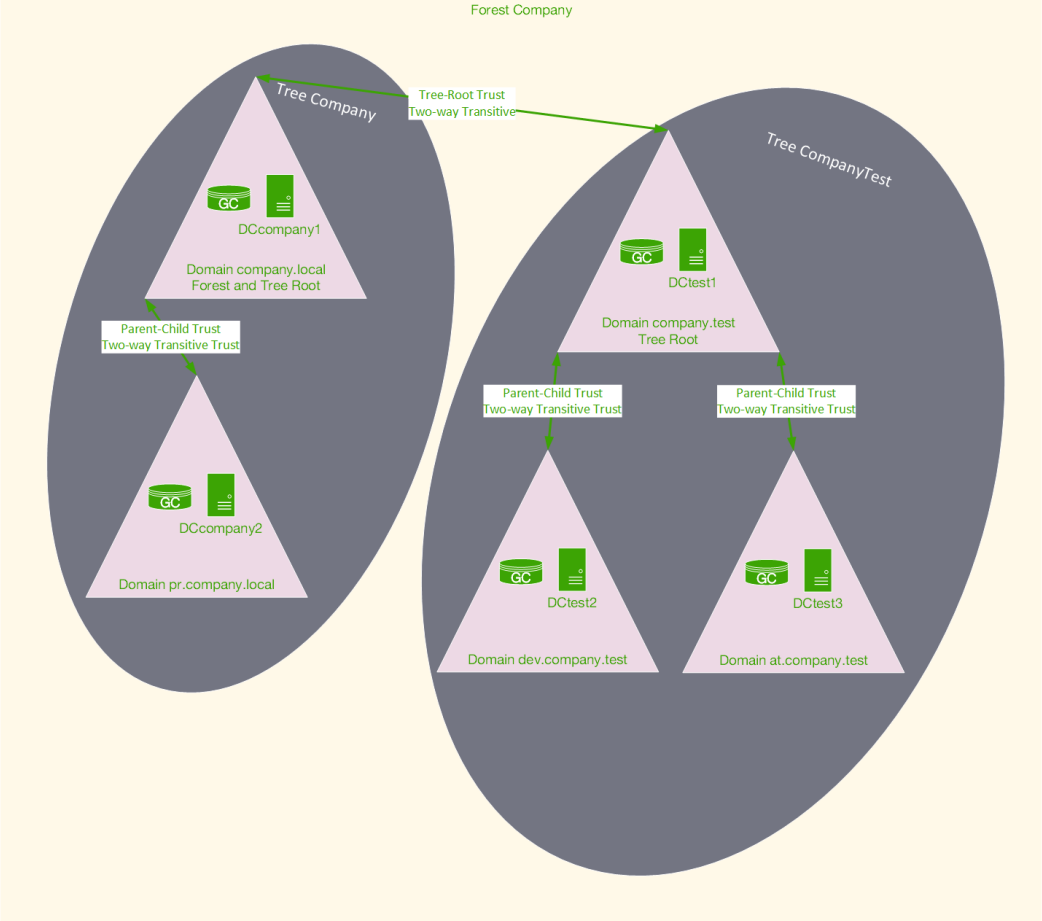


Рисунок 1.2 – Domain, tree and forest relationship

Корпорація Майкрософт також відкрила метод розширення схеми. Розробники можуть використовувати цей набір методів для розширення даних у схемі Active Directory, але після запису в AD їх неможливо видалити (оскільки

ідентифікатор об'єкта змінити не можна, але його можна відключити. Найкращим прикладом розширення схеми AD є Microsoft Exchange Server.

На додаток до базової служби мережевих каталогів самої Active Directory, Microsoft також розробила різні служби, використовуючи цю інфраструктуру, і була додана до різних версій Windows Server 2003 для розширення сфери застосування Active Directory. Відносини між доменами, деревами та лісами зображено на рисунку 1.2.

Оскільки сама AD має децентралізовані можливості автентифікації та авторизації, і в 2003 році Інтернет використовував єдиний вхід (єдиний вхід) у стилі дослідження архітектури, Microsoft також почала використовувати AD для розробки такого, який може підтримувати декілька єдиного входу Функцією веб-сайту (або програми) насправді є Служба федерації Active Directory (AD Federation Services, скорочено ADFS), яка розкриває наступні ключові компоненти:

- Служба федерації: Сервер, відповідальний за обробку автентифікації в архітектурі SSO ADFS.
- Проксі-сервер Федерації: діє як проксі-сервер Служби Федерації у зовнішніх мережах або службах WS-I та підтримує параметри автентифікації у специфікаціях WS-Федерації.
- Клієнт, який усвідомлює претензії: Веб-клієнт компонента, який інформує про претензії, відкритий ADFS, або програма ASP.NET, може безпосередньо підтримувати архітектуру єдиного входу ADFS.
- Агент на базі Windows Token: веб-програма на основі автентифікації Windows. ADFS може підтримувати моделювання та обмін правами AD та правами Windows NT.

Ця послуга вперше з’явилася у версії Windows Server 2003 R2 і була оновлена до ролі Служби федерації Active Directory у Windows Server 2008.

Легка служба каталогів в Windows Server 2003 називається Active Directory Application Mode (ADAM). Це служба каталогів, яка може працювати самостійно без інтеграції з інфраструктурою AD і підходить для продуктивності Ієрархічна концепція підприємства та управління об’єктами, а розробники можуть

використовувати лише досвід використання ADSI. Немає необхідності вивчати метод роботи ADAM. Він також може використовуватися як зовнішній постачальник перевірок для ADFS. Легкий каталог може встановлювати кілька екземплярів на одному комп’ютері, тому також дуже зручно використовувати ADAM для реалізації програм із підтримкою каталогів, особливо пов’язаних з організаційними структурами (такими, як персонал або системи людських ресурсів), а сама ADAM Схема також може Розробники можуть розглядати ADAM як інший тип бази даних або копіювати дані з AD в ADAM. Однак ADAM не копіює сайт AD. Розробники повинні писати власні програми для копіювання даних.

Легку службу було перейменовано в Службу полегшених каталогів Active Directory (AD LDS) у Windows Server 2008 та підвищено до однієї з ролей програми AD.

Його робота подібна до інших структур LDAP (Легкий протокол доступу до каталогів), оскільки цей протокол реалізований подібним чином до бази даних, яка централізовано зберігає всю інформацію, пов’язану з доменом автентифікації. Однією з його переваг є синхронізація між різними серверами автентифікації у всьому домені.

Кожен об'єкт у мережі має відмінне ім'я (DN), тому принтер з назвою " Друк до організаційних підрозділів" (OU) " Продажі" та домен foo.org можна записати такими способами:

- в DN це буде CN = Друк, OU = Продажі, DC = foo, DC = org , де
    - CN - загальна назва
    - DC - це об’єктний клас домену.
- У канонічній формі це буде foo.org/Sales/Imprime

Інші методи адресації - це локальний спосіб пошуку ресурсу

- Відносне розрізнене ім’я (RDN), яке шукає ресурс лише із загальним іменем (CN).

- Глобальний унікальний ідентифікатор (GUID), який генерує 128-розрядний рядок, який використовується Active Directory для пошуку та реплікації інформації

Певні типи об’єктів мають ім’я основного користувача (UPN), що дозволяє скорочений доступ до ресурсу або каталогу в мережі.

Сервіс сертифікатів - це перша послуга, включена в систему Active Directory в Windows Server 2008. Спочатку вона була сервером сертифікатів (Сертифікат Сервера) в Windows 2000 та Windows Server 2003 для створення державних фондів на підприємствах. Ключова інфраструктура . У Windows Server У 2008 році сертифікати та об’єкти AD мають більш сильну та тісну інтеграцію, тому, маючи роль Служби сертифікатів Active Directory (AD CS), ця роль також може поєднуватися із Службою керування правами (RMS), інтегрованою разом для забезпечення управління правами в рівень документа чи заявки.

Служба управління правами - це також послуга, яка була вперше включена в систему Active Directory у Windows Server 2008. Найперше функція управління інформаційними правами (Information Right Management) була запропонований у Microsoft Office 2003. Він може використовуватися. Він контролює розповсюдження документів Office, таких як друк та зберігання файлів. Тоді Microsoft випустила Right Management Server та RMS SDK для платформи Windows Server 2003. У Windows Server 2008 це буде інтегрований в Active Directory.

1.7 Інтеграція Unix в Active Directory

Рівень різноманітності взаємодії Active Directory можна зафіксувати в більшості Unix-подібних операційних систем за допомогою стандартних клієнтів LDAP , але в цих системах зазвичай бракує автоматичного буквального перекладу багатьох атрибутів, пов’язаних із компонентами Windows, таких як групові принципи та одностороння довіра. В даний час багато сторонні постачальники програмного забезпечення пропонують методи інтеграції Active Directory на платформах Unix

(включаючи UNIX , Linux , Mac OS X та декілька програм на базі Java та Unix). Частина цих постачальників включає програмне забезпечення четвертого програмного забезпечення (ADmitMac), Quest Програмне забезпечення (Vintela Authentication Services), Centrify (DirectControl) та аналогічне програмне забезпечення (Аналогічно відкрите та Аналогічне підприємство). Microsoft також має безкоштовну послугу Microsoft Windows (тобто Службу Windows для Unix), розроблену для продуктів UNIX на цьому ринку.

Ці додаткові структури об'єктів були випущені у версії Windows Server 2003 R2 і містять загальні атрибути, які точно відповідають RFC 2307. Усі ці довідкові реалізації RFC 2307, nss_ldap та pam_ldap надаються з PADL.com, включаючи підтримку безпосереднього використання цього атрибута та заповнення інформації. Схема Active Directory для членства в групі за замовчуванням складається зі запропонованим розширенням RFC 2307bis. RFC 2307bis використовує атрибути членів LDAP для зберігання даних членів групи Unix, що відрізняється від базового RFC 2307, який зберігає членів групи як розділений комами список ідентифікаторів користувачів. Windows Server 2003 R2 включає оснащення MMC для створення та редагування цих атрибутів.

Альтернативним варіантом є використання інших служб каталогів, таких як Fedora Directory Server (раніше Netscape Directory Server) або Sun System Java Server Directory Server, які можуть виконувати двосторонню синхронізацію з Active Directory. Платформи між клієнтами Linux і Windows повинні використовувати Аутентифікація Windows та Active Directory, що надаються між інтегрованою керуванням (відхиленою). Інший варіант - використовувати OpenLDAP та його напівпрозору функцію накладання, щоб розширити проект на будь-який віддалений сервер LDAP, який використовує додаткові атрибути, що зберігаються в локальній базі даних. Клієнт, зазначений у локальній базі даних, побачить атрибути, що містяться в віддаленому та наземному базі даних, коли віддалена база даних залишається цілою [8].

Samba 4 випущена 11 грудня 2012 року, включає сервер, сумісний з Active Directory. Samba - це безкоштовна програма , яка має контролер домену, сумісний з Windows NT 4, Windows 2003 та Windows 2008 .

Програма Mandriva Directory Server із відкритим кодом забезпечує веб-інтерфейс для управління контролером домену Samba та службою каталогів LDAP.

Іншою альтернативою є NetIQ eDirectory, 5, яка є мультиплатформою: її можна запускати в будь-якій операційній системі : Linux, AIX, Solaris, Novell Netware , UNIX та інтегрує Native LDAP v.3. Це попередник з точки зору структур каталогів, оскільки він був представлений в 1990 році з версією Novell Netware 4.0. Незважаючи на те, що AD Microsoft зросла популярністю, вона все ще не може відповідати надійності та якості eDirectory та його крос-платформним можливостям.

Sun Java ES Directory Server 6 і OpenDS 7 - це інші альтернативи, перша на основі Java, а друга на базі і розроблена в C. Перша є продуктом Sun Microsystems, а друга - альтернативою з відкритим кодом.

Альтернативою, яка інтегрує OpenLDAP, Heimdal kerberos, Samba, а також цифрову сертифікацію та Bind9 (модифікований для використання LDAP як бекенда), є WBSAgnitio .

1.8 Висновки

На відміну від попередньої системи управління доменом Windows NT Server, яка надавала лише домен управління, Active Directory також дозволяє створювати ієрархічні структури доменів та субдоменів, полегшуючи структурування ресурсів відповідно до їх розташування або функцій в організації. Іншою важливою відмінністю є використання таких стандартів, як X.500 та LDAP, для доступу до інформації.

У свою чергу, кожен із цих об’єктів матиме атрибути, які дозволять їх однозначно ідентифікувати (наприклад, користувачі матимуть поле «ім’я», поле «електронна пошта» тощо), мережеві принтери матимуть поле «ім’я», поле "виробник", поле "модель", поле "користувачі, які можуть отримати доступ" тощо). Вся ця інформація зберігається в Active Directory і автоматично копіюється на всі сервери, які контролюють доступ до домену.

Таким чином, можна створювати ресурси (такі як спільні папки, мережеві принтери тощо) і надавати доступ до цих ресурсів користувачам, з тією перевагою, що всі ці об'єкти зберігаються в Active Directory, і цей список об'єктів реплікація на весь домен адміністрування, можливі зміни будуть видно у всьому обсязі. Іншими словами, Active Directory - це централізована реалізація служби каталогів у розподіленій мережі, яка спрощує управління, управління та запити всіх логічних елементів мережі (таких як користувачі, комп’ютери та ресурси).
Адреси ресурсів Active Directory є стандартними для Загальної конвенції про імена (UNC), уніфікованого локатора ресурсів (URL) та LDAP Naming.

2 МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ВИРІШЕННЯ ЗАДАЧІ ЗА ТЕМОЮ ДОСЛІДЖЕННЯ

2.1 Авторизація

Авторизація - це функція визначення прав / привілеїв доступу до ресурсів, яка пов’язана із загальною інформаційною безпекою та комп’ютерною безпекою , і зокрема, з контролем доступу. Більш формально "авторизація" означає визначення політики доступу. Наприклад, кадровий персонал, як правило, уповноважений отримувати доступ до записів працівників, і ця політика часто оформляється як правила контролю доступу в комп'ютерній системі. Під час роботи система використовує правила контролю доступу, щоб вирішити, чи будуть запити на доступ від (аутентифікованих) споживачів схвалені (надані) чи відхилені. Ресурси включають окремі файли або дані елемента , комп'ютерні програми , комп'ютерні пристрої та функціональні можливості, що надаються комп'ютерними програмами . Прикладами споживачів є користувачі комп'ютерів, комп'ютерне програмне забезпечення та інше обладнання на комп'ютері.

Контроль доступу в комп’ютерних системах та мережах покладається на політику доступу . Процес контролю доступу можна розділити на наступні фази: фаза визначення політики, де доступ санкціонований, і фаза забезпечення політики, коли запити на доступ затверджуються або відхиляються. Авторизація - це функція фази визначення політики, яка передує фазі застосування політики, коли запити на доступ затверджуються або відхиляються на основі раніше визначених дозволів.

Більшість сучасних багатокористувацьких операційних систем включають керування доступом на основі ролей (RBAC) і, отже, покладаються на авторизацію. Контроль доступу також використовує автентифікацію для перевірки особи споживачів. Коли споживач намагається отримати доступ до ресурсу, процес контролю доступу перевіряє, чи був споживач уповноважений використовувати цей ресурс. Авторизація є відповідальністю органу влади, такого

як керівник підрозділу, в межах домену програми, але часто делегується зберігачу, такому як системний адміністратор. Авторизації виражаються як політики доступу в деяких типах "додатка для визначення політики", наприклад, у вигляді списку контролю доступу або можливості , або пункту адміністрування політики, наприкладXACML . Виходячи з " принципу найменших привілеїв ": споживачі повинні мати дозвіл лише на доступ до того, що їм потрібно, щоб робити свою роботу. У операційних системах старих та однокористувацьких систем часто були слабкі або відсутні системи аутентифікації та контролю доступу [9].

"Анонімні споживачі" або "гості" - це споживачі, від яких не вимагали автентифікації. Вони часто мають обмежені дозволи. У розподіленій системі часто бажано надати доступ, не вимагаючи унікальної ідентифікації. Відомі приклади маркерів доступу включають ключі, сертифікати та квитки: вони надають доступ, не підтверджуючи особу.

Довірені споживачі часто мають дозвіл на необмежений доступ до ресурсів у системі, але вони повинні бути перевірені, щоб система контролю доступу могла приймати рішення про затвердження доступу. "Частково довіряють", і гості часто мають обмежені дозволи, щоб захистити ресурси від неналежного доступу та використання. Політика доступу в деяких операційних системах за замовчуванням надає всім споживачам повний доступ до всіх ресурсів. Інші роблять протилежне, наполягаючи на тому, що адміністратор чітко уповноважує споживача використовувати кожен ресурс.

Навіть коли доступ контролюється за допомогою комбінації списків автентифікації та контролю доступу , проблеми збереження даних авторизації не є тривіальними та часто становлять стільки ж адміністративного тягаря, скільки керування автентифікаційними даними. Часто доводиться змінювати або видаляти авторизацію користувача: це робиться шляхом зміни або видалення відповідних правил доступу в системі. Використання атомної авторизації є альтернативою управлінню авторизацією для кожної системи, коли довірена третя сторона надійно розподіляє інформацію про авторизацію.

Авторизація та автентифікація - це тісно пов’язані функції, але є важливі відмінності. Системи авторизації визначають, що користувачеві дозволено робити, виходячи з його ідентифікаційного профілю. Аутентифікація, навпаки, підтверджує, що користувач насправді є користувачем або ідентичністю, якою вони заявляють.

Найкращий спосіб зрозуміти взаємозв'язок автентифікації та авторизації - це порядок операцій. Системи, що базуються на ідентичності, спочатку повинні пройти процес автентифікації для користувача чи ідентифікатора, а потім визначити, що дозволено аутентифікованому користувачеві. Консолідовані апартаменти часто проводять цей процес у фоновому режимі. Проте обидва фрагменти повинні бути присутніми та функціональними для забезпечення безпечного доступу до певної системи чи фрагмента даних.

Порівнюючи різні системи авторизації, враховуйте такі фактори:

- Рішення Point проти Suite: Існує цілий ряд точкових рішень для авторизації. Однак найпопулярнішими та найпоширенішими рішеннями є ширші набори, які централізують всі етапи процесу ідентифікації та доступу в єдину систему. Поміркуйте, чи потрібне бізнесу точкове рішення, щоб вписатися в існуючі структури, чи повний комплекс і централізація були б більш ефективними.
- Інтеграція: Будь-яка система з можливостями автентифікації повинна мати можливість плавної інтеграції з іншими системами безпеки та ідентифікацією. Розгляньте готові або власні інтеграції між кожним потенційним продуктом авторизації та існуючим технологічним стеком бізнесу.

Більшість сучасних багатокористувацьких операційних систем включають процес авторизації. Він використовує процес автентифікації для ідентифікації споживачів. Коли споживач намагається використовувати ресурс, процес авторизації перевіряє, що споживач отримав дозвіл на використання цього ресурсу. Дозволи, як правило, визначаються системою адміністратора в якомусь "застосуванні політики безпеки", такому як ACL або можливість, заснована на "

принципі найменших привілеїв"»- Споживачі повинні отримувати лише дозволи, необхідні для виконання своєї роботи. Раніше однокористувацькі операційні системи раніше мали слабкі системи або системи аутентифікації, які повністю відсутні.

Споживачів, від яких не вимагали автентифікації, називають "анонімними споживачами" або "гостями". Вони часто мають дуже мало дозволів. У розподіленій системі часто бажано надати доступ, не вимагаючи унікальної ідентифікації. Відомі приклади авторизаційних маркерів включають ключі та квитки, які дозволяють надати доступ без надання ідентифікаційних даних.

Існує також поняття споживачів "надійних" (довірених). Споживачам, які пройшли автентифікацію та яких позначено як довірених, надається необмежений доступ до ресурсів. Гість та "частково довірені" споживачі підлягають дозволу на використання захищених ресурсів. Програми політики безпеки деяких операційних систем за замовчуванням надають всім споживачам повний доступ до всіх ресурсів. Інші роблять протилежне, наполягаючи на тому, щоб адміністратор вжив навмисних дій, щоб дозволити кожному споживачеві використовувати кожен ресурс.

Навіть коли авторизація здійснюється за допомогою комбінації автентифікації та ACL, питання збереження даних політики безпеки не є тривіальними, часто представляючи стільки адміністративних витрат, скільки підтвердження необхідних ідентифікацій користувачів. Часто бажано видалити авторизацію користувача: для цього, із застосуванням політик безпеки, необхідно, щоб дані могли оновлюватися.

2.2 Windows Server

Windows Server - це серія серверних операційних систем, розроблена корпорацією Microsoft. Сервери Windows - це потужніші версії настільних операційних систем, призначені для більш ефективного управління корпоративним рівнем, корпоративних мереж, хостингу в Інтернеті чи

інтрамережі, зберігання даних, обміну повідомленнями в масштабі підприємства та подібних функцій. Першою серверною версією операційної системи була Windows NT 3.1, але першою операційною системою від бренду Windows Server, яка вийшла, була Windows Server 2003. Windows 2000 Server була першою версією сервера, яка включала такі речі, як Active Directory, DNS-сервер, DHCP-сервер, Групова політика та багато інших функцій, які широко використовуються сьогодні. Починаючи з Windows Server 2003, за ці роки було випущено більше версій, включаючи Windows Server 2003 R2, 2008, 2008 R2, 2012 та 2012 R2, де з кожним випуском додавалися нові функції, а функціонал розширювався (докладнішу інформацію можна знайти на MSDN веб-сторінка1). Остання версія серверної операційної системи - Windows Server 2012 R2 і зосереджена на хмарних обчисленнях [11]. Усі версії Windows Server підтримують Active Directory як набір служб. Кожна служба Active Directory використовується для роботи з різними об'єктами та управління різними аспектами Active Directory:

- AD Domain Services (AD DS): Керує користувачами, комп’ютерами та політикою. Це як джерело інформації каталогу, так і служба, що робить інформацію доступною та корисною. Сюди входить інформація про сервери, користувачів, клієнтів, мережеві пристрої, програми та сервери електронної пошти. AD DS забезпечує керованість, безпеку та взаємодію в централізованому, набагато простішому способі управління. Він зберігає та управляє інформацією про мережеві ресурси та дозволяє централізоване управління та делегування цього централізованого управління. Він також забезпечує підтримку програм, що підтримують каталоги, таких як Microsoft Exchange Server.
- AD Certificate Services (AD CS): Handles Service, Client, Server та User identification. AD CS - це реалізація Microsoft інфраструктури відкритих ключів (PKI). PKI - це набір апаратного забезпечення, програмного забезпечення, людей, політик та процедур, необхідних для створення, управління, розповсюдження, використання, зберігання та скасування цифрових сертифікатів. Він надає настроювані послуги з випуску та

керування цифровими сертифікатами за допомогою ряду інструментів, включаючи органи сертифікації, веб-реєстрацію CA або веб-службу реєстрації сертифікатів.

- AD Federation Services (AD FS): Керує доступом до ресурсів через традиційні межі. AD FS - це програмний компонент, що полегшує міжорганізаційний доступ до систем та додатків. Ця послуга дозволяє IT-адміністраторам або ділитися ресурсами з усім світом, або дозволяти користувачам отримувати доступ до ресурсів іншої організації. Роль сервера AD FS забезпечує спрощену, захищену федерацію ідентифікаційних даних та можливості єдиного входу в Інтернет (SSO). Це дозволяє створювати відносини довіри між двома організаціями, забезпечує доступ до додатків між організаціями та забезпечує єдиний ввід між двома різними каталогами веб-програм.
- AD Rights Management Services (AD RMS): Підтримує безпеку даних. AD RMS - це технологія захисту інформації, яка працює з програмами для захисту цифрової інформації. Це дозволяє автору створювати вміст, такий як текстовий документ або електронне повідомлення, і дозволяє захищати цей вміст за допомогою програм, що знають про AD RMS. Це дозволяє автору встановити дозволи для завдань, які можна виконати з документом, таких як читання, друк, копіювання та пересилання. Це також дозволяє окремим особам та адміністраторам визначати дозволи на доступ до документів, робочих книг та презентацій, а також запобігає друку, пересиланню та копіюванню конфіденційної інформації неавторизованим персоналом. Це гарантує, що обмеження доступу та використання застосовуються незалежно від того, де знаходиться інформація.
- AD Lightweight Directory Services (AD LDS): Він копіює структуру AD DS. AD LDS - це ієрархічний сховище каталогів на основі файлів. Це як джерело інформації каталогу, так і служба, що робить інформацію доступною та придатною для використання. Сюди входить інформація про користувачів, мережеві пристрої, програми, сервери, сервери електронної пошти. AD LDS

забезпечує керованість, безпеку та сумісність у централізованому, набагато простішому способі управління. Він використовує полегшений протокол доступу до каталогу (LDAP), який забезпечує гнучку підтримку програм із підтримкою каталогів, без залежностей та обмежень домену AD DS, пов'язаних з доменом. Він пропонує служби каталогів для програм із підтримкою каталогів, не завдаючи додаткових витрат на домени та ліси. Також немає вимоги до єдиної схеми у всьому лісі, що означає, що AD LDS можна налаштувати.

2.3 Zentyal server

Zentyal розпочав свою діяльність як проект з відкритим кодом, надаючи компаніям та організаціям повний повнофункціональний сервер на базі Linux. Зараз Zentyal - компанія, що базується в Сарагосі, Іспанія, і пропонує два основні продукти - Zentyal Cloud і Zentyal Server. Zentyal Server зосереджений на впровадженні протоколів Microsoft Exchange та Active Directory на Linux і став одним з найпопулярніших проектів з відкритим кодом у світі, випущених під загальною публічною ліцензією GNU. Zentyal пропонує два типи серверів Zentyal - громадські та комерційні. Комерційні версії Zentyal працюють поверх серверної версії Ubuntu, завжди на LTS (довгострокова підтримка), тоді як версія спільноти може базуватися на стандартних серверних версіях Ubuntu. Сервер Zentyal з'єднує дві основні функції - пошту та сервер каталогів. Він також включає DNS-сервер, DHCP-сервер, NTP-сервер, Центр сертифікації та VPN-сервер і клієнт. На додаток до цих послуг, він пропонує деякі основні мережеві управління, такі як конфігурація статичного та DHCP-інтерфейсів, служби об'єктів, фільтрація пакетів та переадресація портів. Основними функціями є послуги пошти та каталогів:

- Mail service: Zentyal пропонує власну сумісність з протоколами Microsoft Exchange Server і підтримку Microsoft Outlook 2007 і 2010. Він також забезпечує рідну сумісність з Microsoft Active Directory і використовує кілька доменів віртуальної пошти. Поштова служба надає основні операції з

електронною поштою, календарями, контактами, пропонує функціональність веб-пошти та синхронізацію з мобільними пристроями (підтримка ActiveSync). На додаток до цієї функціональності електронної пошти, він також вводить антивірус, антиспам та підтримує фільтри типів Extention та MIME.

- Domain & Directory service: Zentyal пропонує управління центральним доменним каталогу, включаючи операції з такими об'єктами, як підрозділи, користувачі, групи безпеки, списки розсилки та контакти. Він підтримує операційні системи Windows XP, Windows Vista, Windows 7 і Windows 8. Інші запропоновані функції - це спільний доступ до файлів у середовищах Windows (CIFS), списки контролю доступу та антивірус із вбудованим карантином для файлового сервера.

Zentyal інтегрує Samba4 як Службу каталогів, реалізуючи функціональність контролера домену Windows та спільний доступ до принтерів / файлів. Концепція домену в Zentyal заснована на реалізації Microsoft Active Directory і повністю залежить від можливостей Samba4. Він також надає можливості спільного використання файлів за допомогою протоколу SMB / CIFS для підтримки сумісності з клієнтами Microsoft [12]. Інтегруючи технології Samba4, Zentyal може виступати як автономний сервер доменів або стати додатковим контролером існуючого домену, приєднуючись до Windows Server або будь-якого контролера на базі Samba4. Zentyal Server також може приймати будь-яку з ролей FSMO. Однак інтеграція Samba4 має деякі відомі обмеження:

- Samba не підтримує кілька доменів, тому підтримується лише один домен у лісі.
- Ім'я хосту не може збігатися з ім'ям NETBIOS.
- Довірчі відносини між доменами та лісами не підтримуються.
- Об’єкти групової політики не можна синхронізувати із Zentyal на сервери Windows (лише Zentyl на Zentyal та Windows на Zentyal).

2.4 Засоби адміністрування віддаленого сервера Windows

Незалежно від розміру організації, управління Active Directory є необхідністю. Досить багато програм було розроблено, щоб допомогти адміністраторам AD у роботі, деякі з яких прості та зручні у використанні, інші складні та пропонують багато функціональних можливостей. У цьому розділі ми розглянемо основні інструменти, надані Microsoft, а також декілька найкращих комерційних програм на ринку [13].

Засоби віддаленого адміністрування серверів (RSAT) дозволяють IT-адміністраторам керувати Windows Server з віддаленого комп’ютера, на якому запущена операційна система Windows. RSAT доступний майже для будь-якої версії Windows і забезпечує базовий набір програм, які можуть використовуватися адміністраторами для управління Active Directory.

2.4.1 Active Directory Users та Computers

Active Directory Users та Computers - це оснастка консолі керування Microsoft (MMC), що входить до складу RSAT. Він використовується для адміністрування та публікації інформації в каталозі і служить основним додатком, що використовується для управління об'єктами користувачів, комп'ютера та групи. Він забезпечує основні CRUD-операції з об'єктами в Active Directory і дозволяє адміністраторам виконувати деякі основні завдання управління, такі як:

- User account – додавання нових користувачів, зміна паролів, надання прав, і так далі.
- Group – створення груп безпеки, зміна прав, встановлення членства, тощо.
- Computer account – створення комп’ютера, зміна властивостей, і так далі.
- Domain – підключення до певного домену, управління властивостями домену, тощо.
- Organizational Units – створення нового контейнера або підрозділу, управління властивостями, тощо.

2.4.1 Active Directory Domains and Trusts

Active Directory Domains and Trusts - це оснастка консолі керування Microsoft (MMC), що входить до складу RSAT. Цей інструмент не пропонує такого ж рівня функціональності, як користувачі та комп'ютери Active Directory, а орієнтований на завдання, які можна виконати глобально на доменах. Він використовується для адміністрування довірчих відносин домену, функціональних рівнів домену та лісу та суфіксів основного імені користувача (UPN). Це дозволяє адміністраторам виконувати деякі основні завдання управління, такі як:

- Domain trust – створити довіру, перевірити довіру, створити ярлик, сферу або зовнішню довіру, тощо.
- Forest trust – створити лісовий трест, керувати маршрутом для певних суфіксів імен, тощо.
- Domain functional level – вибрати режим, тощо.
- Forest functional level – вибрати режим, тощо.
- UPN – створити суфікс UPN, тощо.

Цей інструмент можна запустити лише в операційній системі Windows і є безкоштовним, але його можна використовувати для управління будь-яким сервером Active Directory, сумісним з Microsoft і Samba4. Хоча цей інструмент може бути дуже зручним, він непридатний для управління великим середовищем. Це дозволяє керувати лише кількома частинами Active Directory, а робота з каталогом, що містить велику кількість користувачів, доменів, лісів, може зайняти багато часу і може бути незручним і складним.

Active Directory Sites and Services - це оснастка консолі керування Microsoft (MMC), що входить до складу RSAT. Він використовується для адміністрування реплікації даних каталогів між усіма сайтами в лісі доменних служб Active Directory (AD DS). Ця оснастка також забезпечує перегляд об'єктів, що

стосуються служби, опублікованих у AD DS. Це дозволяє виконувати деякі основні управлінські завдання, такі як:

- Server tasks – увімкнути глобальний каталог, вибрати політику запитів, перевірити топологію реплікації, тощо.
- Site tasks – кешувати універсальне членство в групі, створити сайт або підмережу, створити об’єкт групової політики, тощо.
- Site replication tasks – створення посилання на сайт або мосту посилання на сайт, додавання з'єднання, тощо.

Ці інструменти здебільшого використовуються лише організаціями з відносно складною ієрархією Active Directory. Регулярно цей інструмент зазвичай використовується організаціями, які потребують декількох сайтів, доменів, лісів, розділів тощо.

Цей інструмент можна запустити лише в операційній системі Windows і є безкоштовним, але його можна використовувати для управління будь-яким сервером Active Directory, сумісним з Microsoft і Samba4. Незважаючи на те, що цей інструмент може бути дуже зручним, через деякий час і з більшою складністю він непридатний для управління більшим середовищем. Це дозволяє керувати лише декількома частинами Active Directory, а робота з каталогом, що містить велику кількість доменів, сайтів, лісів, може зайняти багато часу, і це може бути незручно і складно [15].

Active Directory Administrative Center (ADAC) є більш досконалим інструментом, що використовується в управлінні Active Directory, а також є частиною RSAT. Він забезпечує вдосконалення для управління великими та складними середовищами. Він пропонує всі функціональні можливості згаданих програм RSAT, об'єднаних в один інструмент:

- AD Users та Computers функіональність.
- AD Domains та Trusts функціональність.
- AD Sites та Services функціональність.
- Складні LDAP запити.

- Мультидоменне управління.
- Багатолісне управління.

Додаток також дуже гнучкий і забезпечує швидкі панелі з останніми використовуваними завданнями та настроювані панелі для адміністратора для визначення важливих для нього завдань. Незважаючи на те, що це дуже складна програма, яку можна дуже добре використовувати в доменах Windows Server, вона не підтримує управління Samba4. ADAC вимагає принаймні одного контролера домену для запуску веб-служб Active Directory, які не входять до Samba4. Він заснований на Windows PowerShell, тому ним можна керувати лише в операційних системах Windows. У системах Linux для роботи програми потрібен інтерпретатор PowerShell для Linux, але, на жаль, він ще не розроблений, щоб повністю його підтримувати.

Samba-tool є основним інструментом адміністрування Samba, розробленим компанією Samba та для Samba. Він може працювати лише в операційній системі на базі Linux і надає лише основні можливості адміністрування. В основному він призначений для використання адміністраторами для простих та основних завдань адміністрування Samba та Samba Active Directory:

- Users – створити нового користувача, вимкнути або ввімкнути користувача, скинути пароль, тощо.
- Groups – створити нову групу, додати учасників, тощо.
- Domains – показати основну інформацію, підвищити рівень функції, встановити пароль, тощо.
- Sites – створити та видалити сайт.

Samba-tool не підтримує всіх завдань, доступних від RSAT, і тому непридатний для виконання навіть самих основних завдань, таких як створення нового користувача. Крім того, ним можна керувати лише в операційній системі на базі Linux.

Softerra Adaxes - це комплексне рішення для управління, адміністрування та моніторингу Active Directory. Це дозволяє адміністратору автоматизувати та

захистити надання користувачів у середовищі Active Directory. Adaxes забезпечує захист на основі ролей, автоматизацію на основі правил, робочий процес на основі схвалення та звіти AD. Adaxes пропонує функціональність усіх раніше згаданих програм та багато іншого. Він може використовуватися в малому, середньому та великому бізнесі і може бути налаштований на різні ролі управління. Він також надає додаткові функції, такі як веб-інтерфейс, самообслуговування користувачів та самостійне скидання пароля. Вони також пропонують щорічне технічне обслуговування та підтримку. Adaxes можна використовувати для управління як Microsoft Server, так і Samba4, і їх можна побачити в кожній операційній системі завдяки наявності веб-інтерфейсу. Додаток також використовує PowerShell для конкретних завдань автоматизації. Але ця програма не є абсолютно безкоштовною. Він пропонує лише безкоштовну пробну версію, і на той час мінімальна ціна повного додатка для управління до 100 користувачами становить 1600 доларів плюс мінімальні витрати на обслуговування та підтримку 480 доларів.

ADManager Plus - це просте, просте у використанні рішення для управління Active Directory та звітування. Це допомагає адміністраторам Active Directory та технічним спеціалістам у повсякденних завданнях. Він представлений як централізований та інтуїтивно зрозумілий інструмент управління інтерфейсом на основі Інтернету, але також пропонує мобільні програми для виконання важливих завдань управління користувачами прямо на мобільному пристрої. ADManager Plus пропонує функціональність усіх інструментів RSAT, об'єднаних в один інструмент, і може використовуватися в малому, середньому та великому бізнесі. За винятком тривіальних завдань управління, він також обробляє різноманітні складні смаки, такі як масове управління обліковими записами користувачів та іншими об'єктами AD, делегування рольового доступу до технічних служб та створення вичерпного списку звітів AD. Це може зменшити повторювані та складні завдання, автоматизувати рутинні дії для адміністраторів та підтримувати групове управління об'єктами. ADManager Plus можна використовувати для управління як Microsoft Server, так і Samba4. Але ця програма не є безкоштовною. Він постачається у двох виданнях. Стандартне видання для 1 домену і обмежене

до 100 об’єктів домену є безкоштовним. Інші видання є платними і ціна починається від 495 доларів.

Управління Active Directory іноді поєднується з досить складними процедурами, а програми для управління AD досить складні та різноманітні. Доступно багато інструментів, деякі досить потужні, але не всі інструменти пропонують повне управління всіма аспектами Active Directory. Такі рішення важко адмініструвати, оскільки для виконання багатьох завдань адміністраторам доводиться використовувати кілька інструментів, щоб виконати одне завдання управління. Було б корисно мати інструмент, який спрощує управління Active Directory і може використовуватися адміністраторами щодня. Зазвичай компанії використовують комбінацію службових інструментів MS, що входять до складу адміністративних інструментів MS, зокрема користувачів та комп’ютерів Active Directory, доменів і трастів Active Directory та сайтів та служб Active Directory. Це лише три основні програми, що використовуються в управлінні AD, але їх функціональність не завжди є достатньою. Тому багато адміністраторів шукають рішення інших компаній, таких як Cjwdev Limited1, за допомогою своїх інструментів AD Photo Edit та AD Permissions Reporter. Тільки раніше згадані програми - це п’ять різних інструментів, якими можуть користуватися адміністратори. Ці труднощі з управлінням Active Directory послужили натхненням для створення переліку можливостей, якими повинна володіти ідеальна програма для управління AD:

- Users and Groups management: Додаток повинен надавати простий спосіб керувати об'єктами користувача та групи в Active Directory. Він повинен мати можливість охоплювати необхідну функціональність користувачів та комп’ютерів Active Directory.
- Profile photo management: Багато служб у компанії використовують профіль фото для своїх користувачів як простий і швидкий спосіб розпізнати людину. Оскільки AD часто використовується як постачальник інформації про користувача цих служб, цілком логічно зберегти їхні фотографії профілю в AD. Додаток повинен пропонувати спосіб редагування цих

фотографій та виконання простих операцій над ними, перш ніж зберігати їх в AD.

- Індивідуальний процес створення:Створення нових користувачів (або інших об’єктів) у домені компанії може мати певні потреби в налаштуваннях. Як приклад, багатьом адміністраторам компанії потрібно створити нового користувача, змінити ряд атрибутів, характерних для середовища компанії, та додати фотографію профілю. Все це, як правило, робиться за допомогою різних інструментів, і оскільки внесення всіх цих змін може зайняти досить багато часу, новий інструмент повинен бути готовим зробити все це більш простим, приємним і прямим способом для адміністраторів.
- Attribute Editor: Інструмент редактора для кожного окремого атрибута будь-якого об'єкта доступний у всіх інструментах керування Microsoft AD, тому його також слід включити до нової програми. Він надає спосіб вибрати будь-який об'єкт в AD та вручну додати або видалити значення будь-якого атрибута цього об'єкта.
- Модульність: Нова програма повинна бути підготовлена для обслуговування адміністраторів та допомогти їм перестати використовувати багато різних дрібних інструментів, які використовуються сьогодні. Тому він повинен поєднувати функціональність багатьох різних дрібних інструментів і забезпечувати спосіб включення будь-якої нової функціональності, яку потрібно додати в майбутньому.
- Підтримка будь-якого рішення AD: Незважаючи на те, що багато компаній використовують Windows Server як контролер домену AD, все ще існує багато інших компаній, які шукають контролери домену на основі Linux, і зазвичай вони використовують сервер Samba4. Існує також комерційний продукт, заснований на реалізації Samba4, який називається Zentyal Server, який внутрішньо використовує Samba4. Метою цієї програми також повинно бути забезпечення способу підтримки будь-якої реалізації Active Directory.

- Будьте вільними та з відкритим кодом: Розширені програми для управління AD зазвичай не пропонують безкоштовну версію. Навіть якщо вони це роблять, вони скорочують можливості функціоналу до мінімуму. Цей новий додаток повинен бути безкоштовним у користуванні, а вихідний код повинен бути доступним кожному для включення нових функціональних можливостей та налаштування цієї програми.

2.5 Висновки

Нова концепція програми виникла через труднощі з управлінням користувачами, їх правами та загальними проблемами Active Directory. Згадані вище можливості показують кілька моментів, які мають вирішальне значення для задоволення програми управління AD, і ці потреби слугують мотивацією для створення цієї нової програми управління.

Цей інструмент можна запустити лише в операційній системі Windows і є безкоштовним, але його можна використовувати для управління будь-яким сервером Active Directory, сумісним з Microsoft і Samba4. Хоча цей інструмент може бути дуже зручним, він непридатний для управління великим середовищем. Це дозволяє керувати лише кількома частинами Active Directory, а робота з каталогом, що містить більшу кількість об’єктів, таких як користувачі чи групи, може зайняти багато часу і може бути незручною [14].

3 ПРОЕКТНА РЕАЛІЗАЦІЯ

3.1 Постановка задачі

База даних Active Directory в ОС Windows 2000 використовує Jet Blue на основі Extensible Storage Engine (ESE98) як ядро бази даних, з лімітом 16 терабайт і 1 мільярд об'єктів на контролер домену. Бази даних NTDS вже експериментально створені з понад 2 мільярдами об’єктів - порівняно з до 40 000 об’єктів у NT4 Security Account Manager, базі даних менеджера облікових записів безпеки. База даних з іменем файлу NTDS.DIT має дві основні таблиці: таблицю даних, що зберігає об’єкти (рядки представляють екземпляр об’єкта, наприклад, користувача, а стовпці - його атрибути) та набагато меншу таблицю посилань, яка зберігає атрибути, що посилаються на інші об’єкти (наприклад, членство в групі - MemberOf - атрибут). Крім того, існує таблиця схем, що описує об'єкти, яка менша за розміром і по суті статична. У Windows 2003 база даних використовує єдиний примірник для кращого використання простору.

Доменні служби Active Directory (AD DS) є основою кожної доменної мережі Windows. Він зберігає інформацію про членів домену, включаючи пристрої та користувачів, перевіряє їх облікові дані та визначає права доступу. Сервер, на якому запущена ця послуга, називається контролером домену [16]. З контролером домену зв’язується, коли користувач входить у пристрій, отримує доступ до іншого пристрою через мережу або запускає додаток у стилі Metro, що завантажується на пристрій.

3.2 Рекомендовані вимоги для встановлення

Для створення домену повинні виконуватися принаймні такі рекомендовані вимоги:

- Будь-якя версія сервера Windows 2000, 2003 (Server, Advanced Server або Datacenter Server) або Windows 2008. У випадку з сервером 2003, встановіть SP1 на машині з оперативною пам'яттю 256 МБ.

- Протокол TCP / IP встановлюється та налаштовується вручну, тобто без адреси, призначеної DHCP.
- Сервер імен DNS, щоб визначити адресу різних фізичних ресурсів, присутніх у мережі
- Більше 250 МБ на дисководі, відформатованому в NTFS [17].

3.3 Оцінка необхідної функціональності

У цьому підрозділі подано високий рівень основних функціональних можливостей інструменту. Інструмент спроектований таким чином, щоб його можна було легко розширити, щоб нові функції можна було просто інтегрувати.

Функціональність поділена на чотири основні області: Logical Infrastructure Management, Object Management, Physical Infrastructure Management and Extensions. Перші три названі області показують переважно функціонал, який буде частиною цієї роботи. Останній пропонує набір під-сфер, які можуть послужити натхненням для майбутньої роботи. Пояснення кожної підрозділу наведено в наступних частинах.

Users & Profiles. Правильні налаштування користувача та профілю відіграють одну з найважливіших ролей в управлінні ресурсами компанії. Керування потоком працівників має здійснюватися на професійному рівні, і цей інструмент повинен пропонувати адміністраторам можливість робити це. Адміністратор повинен мати повноваження виконувати CRUD (create / read / update / delete) завдання на всіх облікових записах користувачів. Частина цих завдань - увімкнути, вимкнути, заблокувати, розблокувати або скинути обліковий запис користувача. Слід додавати можливість керувати зображеннями профілю користувача разом із правильними завданнями перетворення зображення, такими як обертання, стиснення, зміна розміру або обрізання.

Groups & Membership. Традиційно користувачі поділяються на групи, де група має спеціальні дозволи на доступ до спеціальних ресурсів компанії. Адміністратор повинен мати можливість легко виконувати CRUD-завдання в групах безпеки та визначати членство користувача в групі. Потім групи

пропонують дозволи, які застосовуються до користувачів або інших об’єктів, що входять до групи, таких як можливість підключення до мережі VPN, максимальна кількість входів або права на файлові сервери та документи [18]. Ці дозволи призначаються відповідно до політики безпеки компанії.

Containers & Organizational Units. Усі об'єкти в Active Directory структуровані з використанням об'єктів-контейнерів та організаційних підрозділів. Відповідальність адміністратора полягає в тому, щоб структурувати об’єкти простим, але в той же час ефективним способом. Ці завдання слід легко виконувати у спеціально розробленому вигляді.

Properties, Permissions, Attributes. Властивості, дозволи та атрибути будь-якого об'єкта забезпечують найбільш детальний вигляд одного об'єкта Active Directory. Адміністратор повинен призначити всі атрибути для об'єкта в найбільш детальному поданні, і всі атрибути повинні бути знайдені в одному місці.

Domains. Аутентифікація користувача в домені є головною передумовою будь-якої іншої функціональності цього інструменту. Користувач програми повинен мати можливість використовувати будь-яке вибране ім'я користувача та пароль для підключення до AD DC та автентифікуватись проти них. Користувач також повинен мати можливість змінювати підключення до різних доменів під час запуску програми.

Domain Controllers. Робота з контролерами доменів є важливою функцією управління. Користувач з належними правами повинен мати можливість змінювати поточні налаштування контролера домену на конкретному вибраному контролері домену. Користувач повинен мати можливість виконувати загальні завдання DC, такі як встановлення майстра операцій іменування доменів та ввімкнення або вимкнення сервера глобального каталогу.

Додаткова функціональність (майбутня робота): Функціонал, описаний нижче, може бути корисним для деяких користувачів, однак, оскільки більшості користувачів він майже не потрібен, він виходить за рамки цієї роботи.

Sites & Servers: Перегляд додатків має бути розроблено таким чином, щоб забезпечити легкий обмін ресурсами та переміщення. Підвищення

функціонального рівня, зміна лісу, вибір майстра операцій або додавання суфіксів UPN, сайтів, підсайтів та служб має бути простим завданням.

Query Info: Query info service - це призначена служба для спеціально призначених, заздалегідь визначених подань об’єкта Active Directory. Додаток повинен дозволяти визначати спеціальні запити та виконувати пошук за будь-якою комбінацією заданих параметрів.

Permissions Report: Часто при переході з однієї системи в іншу або при розширенні бізнесу необхідна детальна перевірка дозволів. Додаток повинен мати можливість виконувати перевірку дозволів для домену та показувати можливі діри в безпеці та проблеми з дозволами.

Перевірка узгодженості: Користувач повинен мати можливість перевірити узгодженість домену та визначити відсутні параметри, які не встановлені відповідно до політики безпеки компанії.

Real-time Statistics: Додаток надаватиме статистику в реальному часі про використання домену компанії та надаватиме інформацію про діяльність користувачів. Це повинно включати кількість користувачів, які наразі увійшли в систему, або використання пропускної здатності мережі в режимі реального часу.

Suspicious Activity Detection: Додаток також може включати модуль, призначений для аудиту. Він може відстежувати активність користувачів та повідомляти адміністратора про будь-яку підозрілу активність, яка відбувається в даний час. Він також може повідомляти про широке використання ресурсів компанії.

3.4 Стадії розробки

В результаті базового огляду функціональності програми було створено досить вичерпний перелік можливих завдань програми, щоб більш детально вказати функціональність. Цей список служить основним інформаційним ресурсом для проектування програми.

Розробка програми буде розділена на чотири основні фази відповідно до важливості окремих завдань, де для завершення завдань, що реалізуються на наступній фазі, зазвичай потрібно закінчення функціональних завдань з однієї фази.

На першому етапі будуть реалізовані завдання, необхідні для управління додатком та виконання основних операцій. Діаграма першої стадії розробки зображена на Рисунку 3.1. Найважливішим є загальний пакет, що містить завдання для зміни налаштувань програми. Оскільки додаток базується на модулях для підтримки майбутньої розширюваності, необхідно створити систему для модулів. Користувач зможе змінювати різні уявлення. Також можна встановити параметри програми, такі як облікові дані з'єднання.

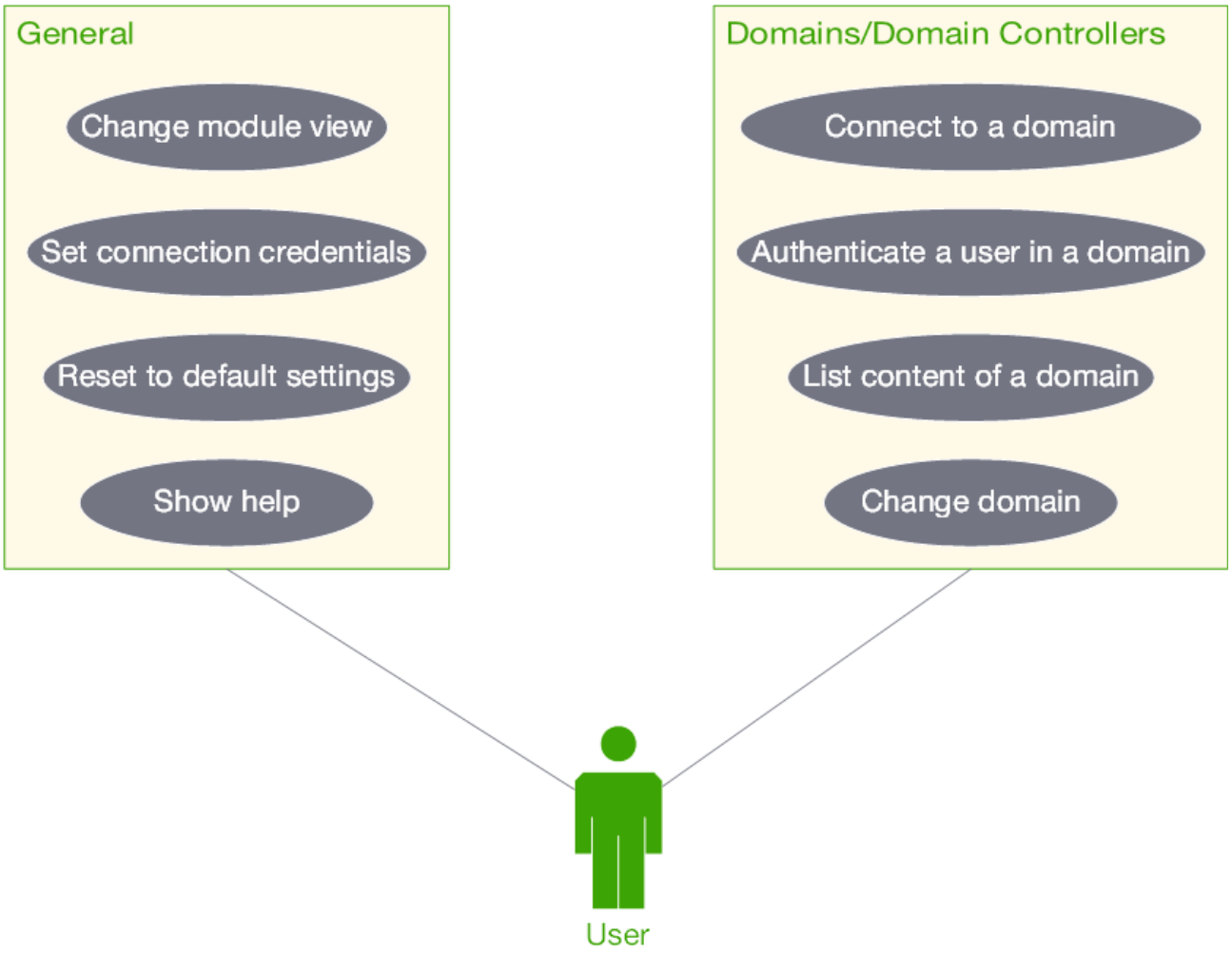


Рисунок 3.1 – Діаграма першої стадій розробки

На цьому етапі також будуть реалізовані завдання, необхідні для управління Active Directory. Діаграма другої стадії розробки зображена на Рисунку 3.2. Ці завдання відображаються в пакеті Domain/Domain Controllers та включають завдання для встановлення підключення до DC, автентифікації користувача та завантаження вмісту каталогу. Це є передумовою для майже всіх інших завдань, і тому їх потрібно виконувати спочатку.

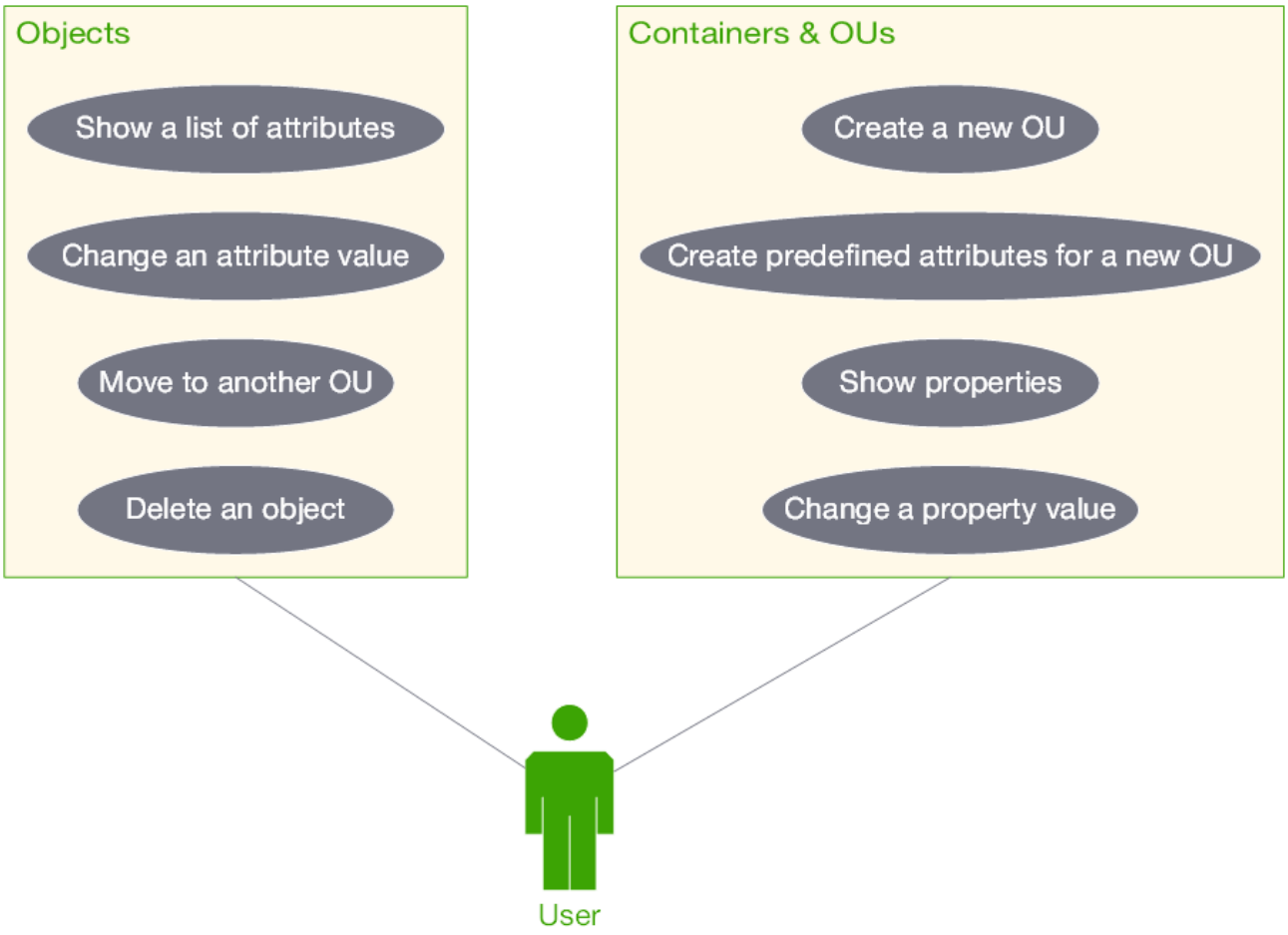


Рисунок 3.2 – Діаграма другої стадій розробки

Після успішного підтвердження придатності завдань з першої фази функціонал потрібно розширити. Наступним логічним кроком є показ усіх атрибутів, які має вибраний об'єкт, з можливістю легко змінити значення атрибутів. Також включено ще два основні випадки - переміщення об’єкта до іншого організаційного підрозділу та видалення вибраного об’єкта. Наступним кроком є можливість контролю та управління організаціями. Можна встановити

налаштування програми для створення атрибутів створення за замовчуванням та їх відповідні значення. Це встановлено для нового організаційного підрозділу, а також використовується в процесі створення нового організаційного обєднання. Діаграма третьої стадії розробки зображена на Рисунку 3.3.

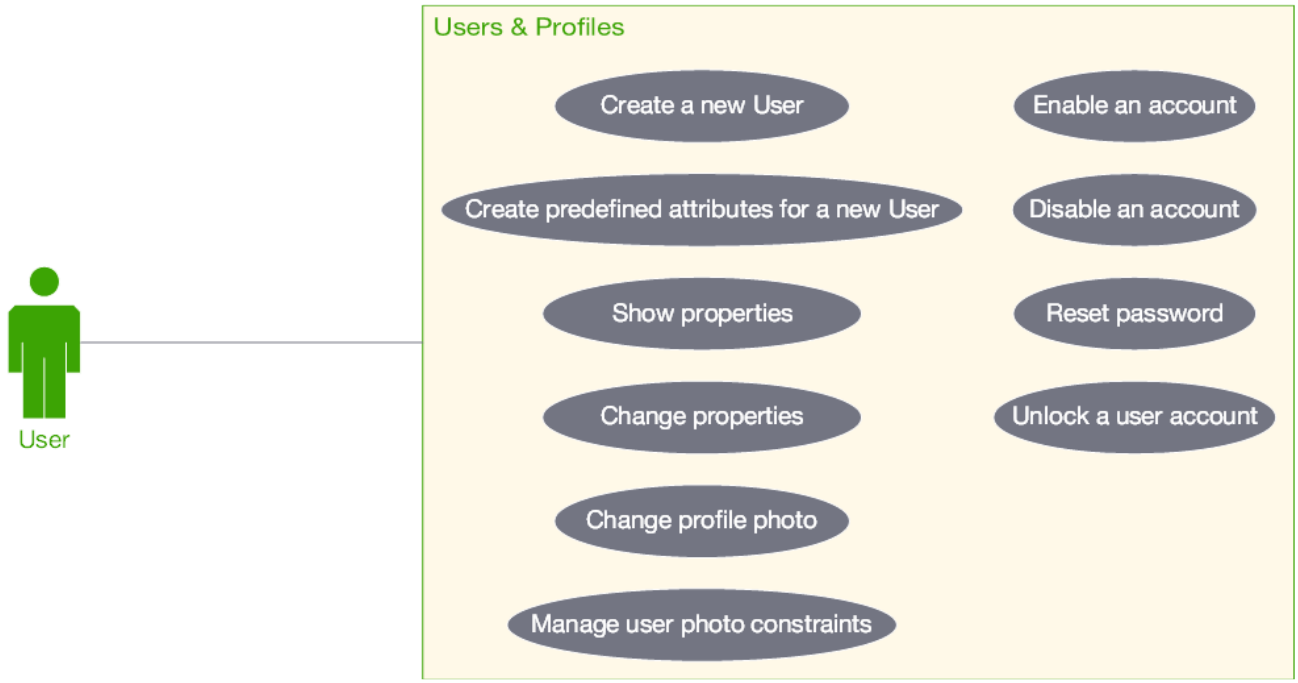


Рисунок 3.3 – Діаграма третьої стадій розробки

Користувач може створити нового організаційного обєднання з можливістю редагування заздалегідь визначених атрибутів у налаштуваннях разом зі стандартними атрибутами створення. Властивості організаційного обєднання можна показувати, а їх значення можна змінювати.

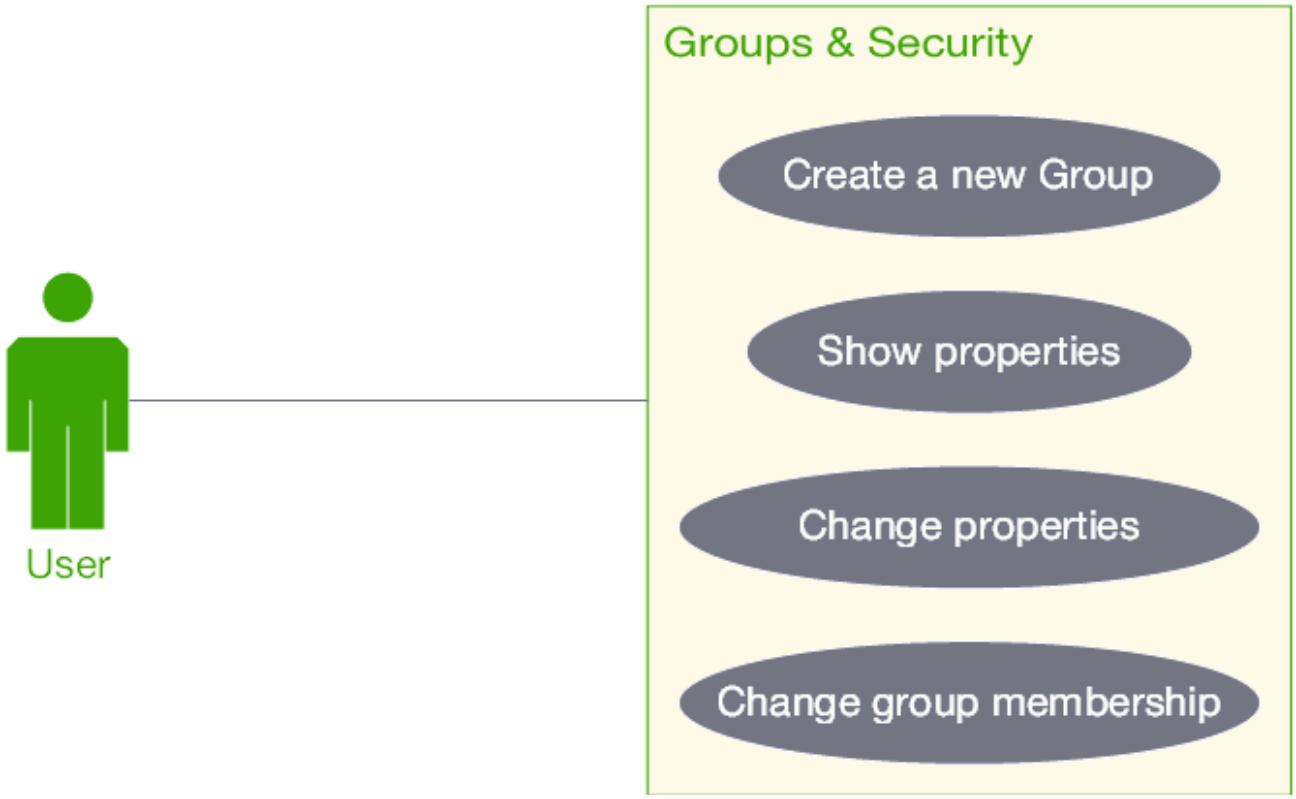


Рисунок 3.4 – Діаграма четвертої стадій розробки

На останньому етапі додано управління об’єктами групи. Діаграма четвертої стадії розробки зображена на Рисунку 3.4. Варіанти використання можна включає створення нової групи, що показує властивості вибраного об'єкта групи та можливість зміни значення властивості. Також членство в цій групі можна змінити у вікні властивостей цього об'єкта.

3.5 Реалізація

Реалізація є найважливішою частиною цієї дипломної роботи, тому було відведено багато часу щоби розділити очікувану функціональність на різні логічні компоненти та створити чітку схема зв'язку між цими компонентами.

Дизайн складається з декількох основних логічних компонентів, які містять класи та простори імен. Найважливіші частини програми, з яких подаються три як основа: графічний інтерфейс, бізнес-модель та служба даних. Ці компоненти також є відображенням моделі Model-View-ViewModel (MVVM). MVVM - це архітектурний шаблон, який відокремлює розвиток графічного інтерфейсу від

розвитку бізнес-логіки. ViewModel відповідає за перетворення даних із Моделі у подання, яке підходить і для управління та презентація у поданні. Логікою відображення View переважно займається ViewModel і використовує прив'язку даних як спосіб перенесення даних з коду до подання [19]. В прив'язці даних, коли дані в ViewModel оновлюються, View автоматично повідомляєтьсяі відповідним чином зміненюється.

Цей шаблон виявився корисним при створенні програми. Це спрощує складність тестування та допомагає зробити програму більш керованою, знизивши зчеплення між компонентами. Додаток використовує MVVM Light Framework, який має все необхідні базові класи для реалізації MVVM. Наступним важливим компонентом є компонент Служб Active Directory, який охоплює фактичну Службу Active Directory. Це трактується як чорний ящик для спілкування із заявкою і, отже, не залежить від фактичного впровадження служби Active Directory.

Цим додатком користуватимуться два типи користувачів:

- Користувач з правами адміністратора буде основним типом користувача, для якого розроблена ця програма. Цей користувач матиме повні права керувати всіма об’єктами та їх атрибутами в домені.
- Користувач без прав адміністратора буде додатковим типом користувача. Він матиме обмежені права на об'єкти та атрибути. Він може отримати доступ до об’єктів і вносити зміни, які йому дозволено робити.

Різниця між цими типами користувачів та їх правами на управління об’єктами буде збережена в Active Directory як дозвіл, і програма автоматично відображатиме ці налаштування в програмі.

Конкретна інформація, необхідна користувачеві для того, щоб додаток відповідав своїй меті, є:

- Профіль користувача, створений у домені Active Directory з усіма правами, встановленими належним чином,
- Ім'я користувача та пароль для підключення користувача до домену.

Дуже важливою для програми є наявність та співпраця з контролером домену Active Directory, тому існує необхідність запуску AD DC і виконуються всі необхідні умови для спілкування з ним. Ця програма повинна також мати можливість спілкуватися з будь-яким типом сервера AD, а саме з сервером Microsoft Server AD та Zentyal Samba4 AD.

3.5.1 Базові компоненти

Нижче описані основні компоненти, необхідні для функціонування інших компонентів належним чином. Вони виконують різні допоміжні ролі.

- Resources клас використовується для групування всіх використаних ресурсів у програмі. Це глобально доступний клас. Він використовується для легкого включення інші мови, більш ніж одна за замовчуванням, створивши копію файлу ресурсу та правильне іменування файлу ресурсу.
- Settings клас подібний до класу Resources. Він підтримує налаштування програми за замовчуванням та підтримує їх стан, навіть коли програму закрито та відкрито знову.
- Messenger клас, що використовується для підтримки обміну повідомленнями між різними компонентами. Це головним чином використовується для повідомлень між різними ViewModels, повідомлень повідомлень для DialogCoordinator та IDataService. Він базується на шаблоні дизайну Views, де будь-який клас може підписатися на прослуховування будь-якого повідомлення.
- DialogCoordinator клас, що використовується як єдиний пункт управління поданнями. Про це повідомляється через клас Messenger і залежно від типу повідомлення та типу вікна поточно відкритий, він відкриває або закриває як модальні, так і немодальні вікна та діалоги.

3.5.2 Active Directory Service

Active Directory Servic представляє сервер, на якому працює Active Directory Domain Services. Він представляє чорний ящик з точки зору програми, причому інтерфейс, який він надає, чітко визначений. Не важливо, якою реалізацією він працює, якщо він підтримує протокол, який використовується доменними службами Active Directory Domain Services. Цей компонент функціонує як джерело всіх даних. Додаток підключається до цієї послуги і автентифікує користувача. Якщо надані облікові дані приймаються, це дозволяє користувачеві з достатніми дозволами для отримання будь-яких запитуваних ним даних. Цей компонент взаємодіє лише з компонентом Data Service [20]. Отже, Data Service відповідає за всі зв'язки та належне маніпулювання отриманими даними від AD.

3.5.3 Data Service (Model)

Цей компонент виконує роль посередника між службою Active Directory та службою Business model. Він переводить об'єкти зі служби Active Directory у внутрішнє представлення, що використовується додатком, і обробляє зв'язок із Active DirectoryService. Він складається з двох логічних частин - Entities та Operations. Компонент Data Service забезпечує інтерфейс IDataService, який використовується Business model, пропонуючи ряд різних операцій для управління AD. Він також містить сутності, з яких отримано базовий компонент служби AD, перетворює їх та передає для прив'язки цілі.

Служба даних використовує .NET framework - особливо клас DirectoryEntry. Це клас використовується для створення з'єднання (коли надаються URI об'єкта AD та облікові дані користувача) та для отримання атрибутів об’єкта.

Entities - це внутрішні об'єкти, що представляють об'єкт, отриманий із AD Service. Ці сутності пропонуються та використовуються компонентом Business model для надання інформації про властивості та атрибути об’єктів AD. Кожен клас сутності успадковується від класу ADObject. Це загальний клас, який містить

інформацію про підключення до вихідного об'єкта AD та містить перелік усіх можливих властивостей, визначених у схемі AD, разом із їхніми фактичними значеннями. Він служить базовим класом, а всі інші класи успадковують від нього. Додаток підтримує розпізнавання ряду типових об’єктів AD: домену, користувача, контейнера, організаційного підрозділу, комп’ютера та групи. Усі вони успадковуються від класу ADObject і розширюють список доступних користувацьких властивостей, які використовуються для прив'язки на стороні бізнес-моделі.

IDataService - це інтерфейс, який містить усі реалізовані операції в AD Service. Типовий метод вимагає властивості ADProject або ADObject, в якому має відбутися зміна, нового значення та дії зворотного виклику, що сигналізує про помилку, яка може трапляється під час виклику служби Active Directory.

3.5.4 Business model (ViewModel)

Business model - це основна частина програми, яка пов’язує функціональність усіх компонентів. Він складається з ViewModels, які визначають дані, що використовуються Views для прив'язки цілі. ViewModels обробляє команди з подання та застосовує бізнес-логіку залежно від команди, що викликається. ViewModel містить властивості, які використовуються для прив'язки у Views. Вони також підключені до Messenger, з якого вони можуть отримувати сповіщення або надсилати сповіщення у Messenger.

MainWindowViewModel- ця ViewModel є найважливішою, оскільки вона використовується для цілей прив'язки в компонент MainWindowView. Вона підтримує загальну логіку для всього додатка, а також містить контекст для різних ViewModels конкретних модулів, таких як Users та Groups. Вона реалізує бізнес-логіку для розширення програми новими модулями та керує видимістю обраного на даний момент модуля. Наступне, що є важливим, це те функціональність MainWindowViewModel полягає в тому, що вона містить логіку для підключення до Active Directory. Вона завантажує параметри з'єднання за замовчуванням і вмикає поточного користувача для визначення інформації для

входу для підключення до Active Directory. Коли користувач хоче підключитися до нового домену або оновити завантажений вміст файлу домену, він викликає операції з компонентом DataService. Цей компонент тоді оновлює його вміст і завантажує поточний стан усіх сутностей у домені.

Modules представляють групу ViewModels, яка використовується для прив'язки даних до елементів керування включено до View. Вони групують функціональність та бізнес-логіку одного конкретного модуля. Він використовується як простий спосіб додати нову функціональність до програми. Додавання нового модуля програми виконується на рівні вихідного коду, тому для додавання нового модуля повинні бути створені View та ViewModel та посилатись на цей модуль, повинен бути доданий до MainWindowView та MainWindowViewModel. Модулі завжди підключені до MainWindowViewModel, і це єдине з'єднання, яке вони мають до програми. Крім цього, він використовує Messenger що дозволяє цьому модулю підписатися на певні повідомлення або надсилати сповіщення у вигляді повідомлення. Для кожного ViewModel є також View, яке використовується як елемент керування, доданий до основної частини MainWindow. Він також містить список інших ViewModels, які представлені як кнопки меню дій. Кнопки меню в меню дій повністю контролюються цим ViewModel, а MainWindow зберігає лише вигляд представлення цих кнопок. ViewModel отримує список початкових кореневих об'єктів AD для відображення. Потім ці об’єкти містять методи отримання своїх дітей. Це представлення добре підходить для подання для відображення цих елементів у TreeView пізніше.

Кілька ViewModels, які служать модулем, вже реалізовані, найбільше важливі з яких описані більш докладно:

- HomeViewModel - це ViewModel, який служить одним із модулів. Він містить усі об’єкти AD, отримані з домену. Він виставляє ці об’єкти для подальшого відображення у відповідному поданні. Він також містить список об'єктів меню. HomeViewModel пропонує лише вибрану кількість операцій, які можливі з меню. Ці операції включають створення нового OU, видалення вибраного об'єкта, переміщення вибраного об'єкта в інше місце в

AD. Це основні операції, доступні для всіх об’єктів в AD, а також загальний редактор атрибутів, за допомогою якого можна редагувати будь-який атрибут будь-якого об’єкта

- UsersViewModel - це модуль, що працює з об’єктами User. Він надає можливості маніпулювати об'єктами користувача в AD. Він містить список об'єктів користувача та контейнерів, що містять ці об'єкти, а також кореневий об'єкт домену. Таким чином, View може відображати фактичні об'єкти або шляхи користувача лише з кореня. Він також містить список об'єктів меню, які дозволяють маніпулювати вибраним користувачем. Вони містять визначення таких операцій, як створення нового Користувача, видалення вибраного об'єкта, переміщення вибраного об'єкта в інше місце в AD. Він також містить операції, характерні для User objects - увімкнути обліковий запис, вимкнути обліковий запис, розблокувати обліковий запис або скинути пароль.
- GroupsViewModel дуже схожий на UsersViewModel і містить список об'єктів Groups, контейнери, що містять ці об'єкти, і кореневий Domain object AD. Він також містить поточно вибраний об'єкт AD та список об'єктів меню, що пропонують операції з вибраним об'єктом AD.

Dialogs - ця група ViewModels використовується як бізнес-логіка для декількох діалогових вікон Views, до яких вони також підключені з метою прив'язки даних. Вони отримують усі важливі дані у своєму конструкторі, а потім працюють лише з цими даними. Їм також заборонено змінювати дані, і тому після успішного підтвердження вікна або після закриття вікна ViewModel викликає метод зворотного виклику, що містить результат. Дані результатів містять дані, змінені у ViewModel. Тоді відповідальність одного з модулів або MainWindow здійснює дії з іншими компонентами, такими як Data Service.

Додаток містить кілька діалогових вікон, і найбільш важливі з них описані більш детально:

- EditPhotoWindowModel використовується для редагування одного із властивостей фотографії об’єкта AD, що містить дані фотографії. В якості параметрів береться властивість фотографії, яка в даний час встановлена для об’єкта AD, і функція зворотного виклику. Функція зворотного дзвінка використовується для сигналізації про помилку або про успіх.
- EditPhotoWindowModel також повертає нещодавно створену властивість із відредагованою фотографією, і батьківський компонент несе відповідальність за зміну даних.. Він використовує компонент Налаштування для завантаження заздалегідь визначених рекомендацій на фотографії. Основні рекомендації включають формат фотографії з її розміром, шириною та обмеженням висоти. Є два можливі формати фотографії - Jpeg та Png. Усі інші атрибути можна налаштувати за допомогою SettingsView. Логіка пропонує ряд операцій, які можливі на фото. Він завантажує фотографію зі сховища та дозволяє змінювати ширину та висоту, обертаючи зображення та встановлюючи зображення до рекомендованих розмірів.
- EditPropertyWindowModel використовується як загальний ViewModel для зміни значення будь-якого атрибута об'єкта AD. Він може бути використаний для редагування будь-якого атрибута ADObject, якщо програма підтримує редагування такого атрибута. ViewModel вимагає властивості об’єкта AD, який встановлений на даний момент, та функції зворотного виклику як параметрів. Функція зворотного виклику сигналізує про помилку або успішне закінчення редагування властивості. Він надає загальнодоступну власність, яка повертає копію ADProperty із виконаними змінами. Інші компоненти, які викликали цей ViewModel може потім виконувати інші дії з цим ADProperty, наприклад виклик служби даних для внесення змін до фактичної служби Active DirectoryService.

3.5.5 Views

Views представляє частину програми, яка є найбільш видимою для кінцевих користувачів. Вони відображають розроблений графічний інтерфейс і повинні пропонувати зручний, модний і в той же час ефективний спосіб взаємодії з додатком. Представлення використовують структуру дизайну MahApps.Metro3 з відкритим кодом. Він надає великий перелік додаткових елементів керування та редизайн майже всіх оригінальних елементів керування WPF. Цей фреймворк був обраний на основі наявності ліцензії з відкритим кодом та простоти включення фреймворку в додаток. Він підтримує різні кольорові теми, і, постійно розвиваючись як безкоштовний проект з відкритим кодом, він добре підходить для потреб цього додатка. Він забезпечує метроподібний дизайн усіх вікон, елементів управління та використовує параметр лише для одного вікна для показу додаткових діалогових вікон.

MainWindow – єдиний віконний екземпляр програми. Це завжди єдине вікно, яке відкривається постійно, а всі інші діалогові вікна включаються в основне та відображаються як накладення. MainWindow має типовий рядок меню у верхній частині вікна, де можна знайти дії програми, такі як налаштування або довідка. Зліва знаходиться меню модулів. Він містить кнопки для кожного модуля, який може запропонувати додаток, і служить способом перемикання між модулями. Він також пропонує спосіб додавання нових модулів. Коли до програми додається новий модуль, додається також нова кнопка меню, і всі функції нового модуля є легко доступними для користувача. У верхній частині вікна також міститься рядок меню дій, який розділений на рядок меню дій модуля (ліва частина) та меню дій програми (права частина). Меню дій програми містить лише одну кнопку та кілька міток. Він використовується для підключення до AD і показує корисну інформацію про те, яке ім’я користувача використовується у з’єднанні та до якого домену воно наразі підключене. Ця дія є загальнодоступною, тому підключення до AD є проблемою програми, а не окремих модулів. Основна частина вікна - це заповнювач для вибраного модуля. Отже, модуль має два основні простори, які є основною частиною вікна та меню дій.

HomeView представляє подання домашнього модуля. Це займає весь доступний основний простір у MainWindow. Він складається з двох частин - лівої частини з TreeView та правої частини з поданням для обраного об’єкта AD. TreeView використовується для показу вмісту AD.

Він повинен відображати всі об'єкти з AD і призначений для використання як спосіб зміни атрибутів для окремого об'єкта AD професіоналами зі знанням імен атрибутів. Після успішного вибору AD object з TreeView, права частина представлення оновлюється, щоб відображати властивості та атрибути вибраного об'єкта. Ця частина пропонує два способи побачити фактичні атрибути об’єкта.

Вкладка Properties використовується для обробки найпоширеніших випадків і простіша у використанні. Він пропонує більше описових назв та міток для обраної кількості атрибутів і повинен використовуватися для зміни найпоширеніших атрибутів. На даний момент існує можливість перегляду Properties лише для вибраної кількості типів об'єктів - OU, Container, Domain, User і Group. Однак це найчастіше використовувані об'єкти в AD і є в даний час достатньо для застосування. Ці, а також всі інші атрибути об'єктів можна побачити у другому типі view - Attribute Editor. Цей простий редактор показує таблицю всіх атрибутів, які можуть бути присвоєні об’єкту, разом із їхніми фактичними значеннями (якщо на даний момент у них встановлено значення). Він також показує тип атрибута та інформацію, чи є цей атрибут однозначним з багатозначним. Щоб змінити значення атрибута, користувачеві потрібно двічі клацнути на вибраному атрибуті, і відкриється нове діалогове вікно. Наразі підтримуються типи, які можна змінити: Bool, DirectoryString, DNString, GeneralizedTime, Int64, Int та OctetString. Це не повний перелік усіх доступних типів для значення атрибута, але він представляє найбільш часто використовувані. Інші типи більш-менш використовуються і встановлюються внутрішньо AD. Після успішного підтвердження змін фактичний відповідальність за зміну значення надсилається на підключений ViewModel, а видимі компоненти оновлюються належним чином.

UsersView, GroupsView. Вони дуже схожі на HomeView. Позиція елементів така ж, як і в Home View, за винятком їх з'єднання з View Model. Вони мають

окремі View Models, що пропонують інший набір даних, прив’язаних до View. Вони обидва також пропонують перегляд властивостей атрибутів та Attribute Editor.

3.5.6 Communication

Зв'язок між раніше згаданими логічними блоками є важливим аспектом, оскільки висока зв'язок може призвести до неможливого коду. Тому можна розпізнати три основні частини комунікації:

- Data Service communication – Для того, щоб зменшити зв'язок між елементами, рівень Data Service спілкується лише з двома іншими компонентами – Business model та Active Directory Services. Дано чіткий потік зв'язку. Бізнес-модель отримує доступ до інтерфейсу Data Service, що включає всі дії, які вона пропонує. Після виклику дії Data Service оцінює тип виклику і може вирішити або змінити значення Entities, або виконати запит на Active Directory Services для отримання або створення нової інформації. Після отримання або створення нової інформації в Active Directory Services виконуються зміни в сутності. Business model прив’язана до цих UEntities і автоматично отримує змінену інформацію, коли виникає подія Property Changed.
- Business model communication – спосіб роботи з Views та їх кореспондентськими View models часто важко знайти. Ця програма використовує послуги двох додаткових компонентів - Messenger та DialogCoordinator. Messenger також використовується в системі interViewModelcommunication. Щоб відкрити нове вікно, у Messenger надсилається повідомлення із необхідними параметрами. Потім Messenger оцінює, до яких компонентів це повідомлення має перерозподілятися, виходячи з типу повідомлення та логіки Messenger. У разі відкриття нового вікна воно надсилає повідомлення до Dialog Coordinator. Потім оцінка повідомлення триває і виконуються необхідні зміни з поданням. Зв'язок від

View до View Model забезпечується шляхом прив'язки змін у View до команд у ViewModel і виклику цих команд. Усі зміни у поданні надсилаються у View Model, де виконуються відповідні оновлення даних, і View автоматично змінюється для відображення даних у View Model.

- Resources and Settings – Resources та Settings існують як глобальні об'єкти, де кожна частина програми має до них доступ. Тим не менше, для пом'якшення зв'язку, Settings прив'язані лише до ViewModels і в разі потреби перерозподіляються звідти. Ресурси прив’язані як до View, так і до ViewModels і містять тексти та інші дані про локалізацію вибраною мовою.

3.6 Висновки

Коли доступні завдання для базового управління AD, потреба зводиться до фактичного управління користувачами. Можна встановити параметри програми для атрибутів створення за замовчуванням та їх відповідні значення. Пізніше вони використовуються під час створення нового об’єкта User. Адміністратор може створити новий об'єкт користувача в AD та встановити його стандартні атрибути разом із попередньо визначеними. Адміністратор також може редагувати ці атрибути під час створення нового об'єкта User. Після створення користувач також може бачити всі властивості об'єкта User та змінювати їх значення, якщо це необхідно. Налаштування програми також дозволяють визначити налаштування за замовчуванням для створення нової фотографії профілю користувача. Сюди входять розміри, ширина та висота та розміри фотографії. Створення фотографії профілю користувача додається до процесу створення, а також до подання властивостей вибраного об'єкта Користувача. Також додаються основні завдання для користувацьких об'єктів - увімкнення та вимкнення облікового запису, скидання пароля, розблокування облікового запису користувача.

ВИСНОВКИ

Метою даної дипломної роботи було розробити та впровадити систему авторизації користувачів на основі Active Diretory. Ця програма охоплює функціонал, який зазвичай вимагає використання декількох безкоштовних інструментів або придбання дорогих сторонніх програм, які можуть це зробити.

Ця дипломна робота пояснила основні поняття Active Directory. Після представлення логічних та фізичних компонентів, було описано використання цих понять. Безліч серверів, що використовують ці служби, та безліч програм для управління Active Directory, що доводить, що це поняття широко використовується навіть сьогодні. Були відкриті нові можливості для полегшення управління доменом Active Directory та визначено нову концепцію управління додатком. Дизайн включає оцінку необхідних функціональних можливостей, та розглянуто безліч пропозицій щодо покращення графічного інтерфейсу користувача. Дизайн порівнюється з існуючими на даний момент програмами і пропонує простий для розуміння погляд на переваги нової програми. Нова програма була розроблена щоб повністю охоплювати функціональність інших існуючих програм і бути готовим до розширень та майбутніх змін. Відповідно до концепції було розроблено нову програму, що підтримує управління авторизацією користувачів та групами, та реалізація додаткових функцій, таких як профіль редагування, та визначення індивідуального процесу створення об'єкта.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Адміністрування локальних мереж Windows NT / 2000 / .NET: Навчальний посібник. Назаров С. В. - 2-ге видання., Перев. і доп. - М .: Фінанси і статистика, 2018. - 492 с.

2. Адміністрування мереж на прикладах. Поляк-Брагінський А. В. - СПб .: БХВ-Санкт-Петербург, 2016. - 323 с.

3. Аппаратні засоби локальних мереж. Енциклопедія / М. Гук, - СПб .: Санкт-Петербург, 2013. - 573 с.

4. Архітектура комп’ютерних систем і мереж: Навчальний посібник / Т.П. Барановска, В.І. Лойко та інш.; під ред. В.І. Лойко. - М .: Фінанси і статистика, 2013. - 256 с.

5. Віртуальні машини: кілька комп’ютерів в одному (+ CD). / А.К. Гультяев - СПб .: Санкт-Петербург. 2014. - 224 с .: ил.

6. Обчислювальні системи, мережі та телекомунікації / В. Л. Бройдо - СПб: Харків, 2013. - 688 с.

7. Вичисливі системи, мережі та телекомунікації: Посібник. - 2-е вид., Перероб. і доп. / А. П. Пятибратов, Л. П. Гудино, А. А. Кириченко; Під ред. А. П. Пятибратова - М .: Фінанси та статистика, 2015. – 512 с.

8. Захист комп'ютерної інформації від несанкціонованого доступу. А. Ю. Щеглов. - СПб .: Видавництво «Наука та техніка», 2014. - 384 с.

9. Захист комп'ютерної інформації. Анін Б. Ю. - СПб .: Харків, 2013. - 384 с.

10. Знайомство з Microsoft Windows Server 2012 / Пер. с англ. / Дж. Ханікат - М .: Видавництво Торговий Дім, 2014. - 464 с.

11. Протоколи безпеки. Навчальний курс. Блэк У. - СПб .: Санкт-Петербург, 2015. - 288 с.

12. Інформатика: Навч. посібник для студ. пед. вузів / А.В. Могилев, Н.И.Пак, Е.К.Хеннер; Під ред. Е.К.Хеннера. - 3-е изд., Перераб. и доп. - М .: Видавничий центр «Академія», 2015. - 848 с.

13. Комплексний захист інформації в комп'ютерних системах: Навчальний посібник. Завгородний В.И. - М .: Логос; ПБОЮЛ Н.А. Егоров, 2016. - 264 с.

14. Комплексний захист інформації в комп'ютерних системах: Навчальний посібник. Завгородний В. И. - М .: Логос; ПБОЮЛ Н. А. Егоров, 2016. - 269 с.

15. Комп’ютерні комунікації. Навчальний курс. Іванов В. - СПб .: Санкт-Петербург 2014. – 225 с.

16. Комп'ютерні мережі. 4-е вид. / Э. Таненбаум. - СПб .: Київ, 2017. - 993 с.

17. Комп'ютерні мережі. Практика побудови. Для професіоналів. 2-е вид. / М. В. Кульгин. СПб .: Київ, 2015. 462 с.

18. Комп'ютерні мережі. Принципи, технології, протоколи. 3-е вид. / В. Г. Оліфер, Н. А. Оліфер. - СПб .: Київ, 2016. - 958 с .

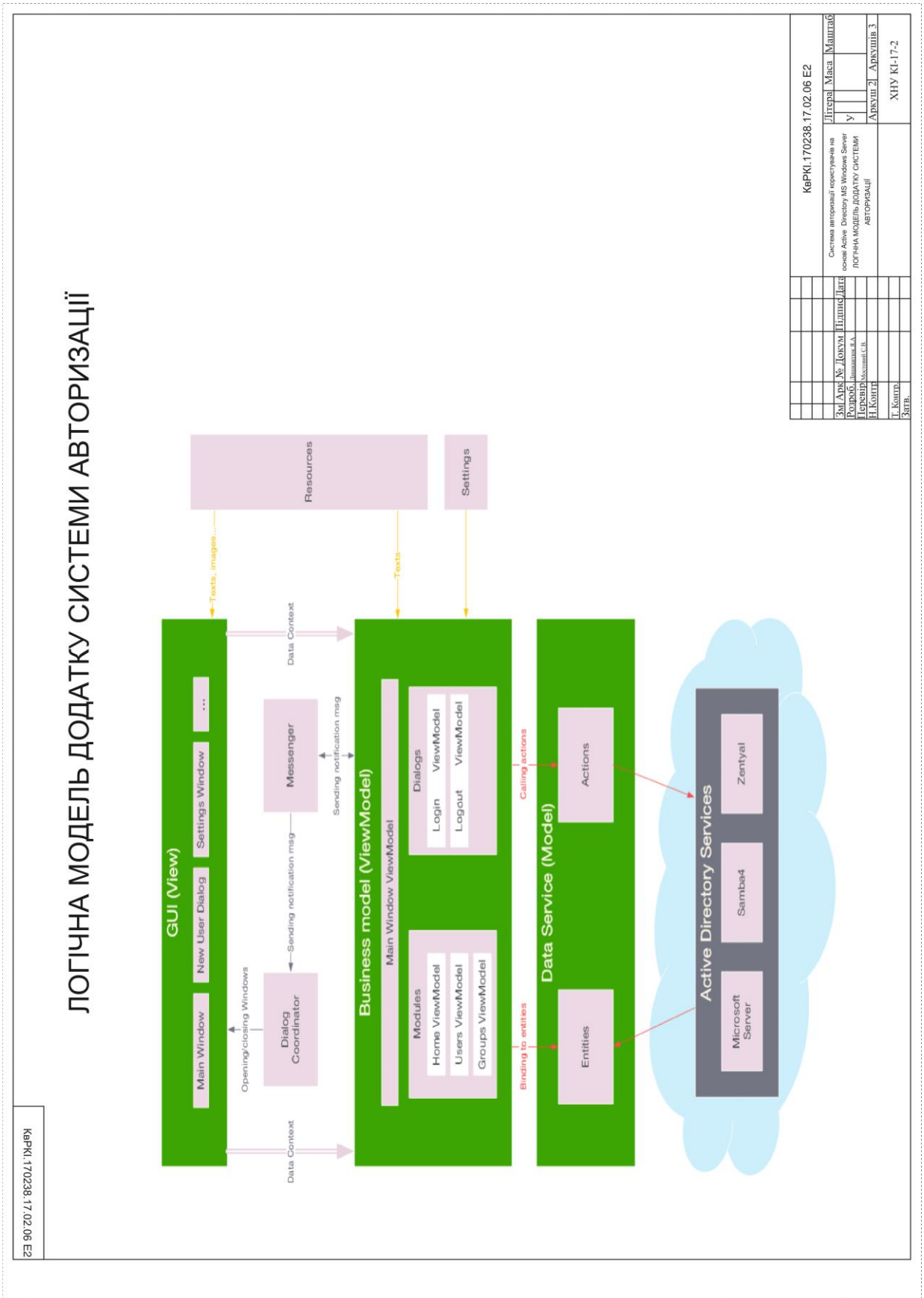
19. Комп'ютерні мережі. Принципи, технології, протоколи / В. Г. Оліфер, Н. А. Оліфер. - СПб .: Київ, 2014. - 672 с.

20. Комп'ютерні мережі. Хитрості. Айвенс К. - СПб .: Санкт-Петербург, 2016. - 298 с.

ДОДАТОК А

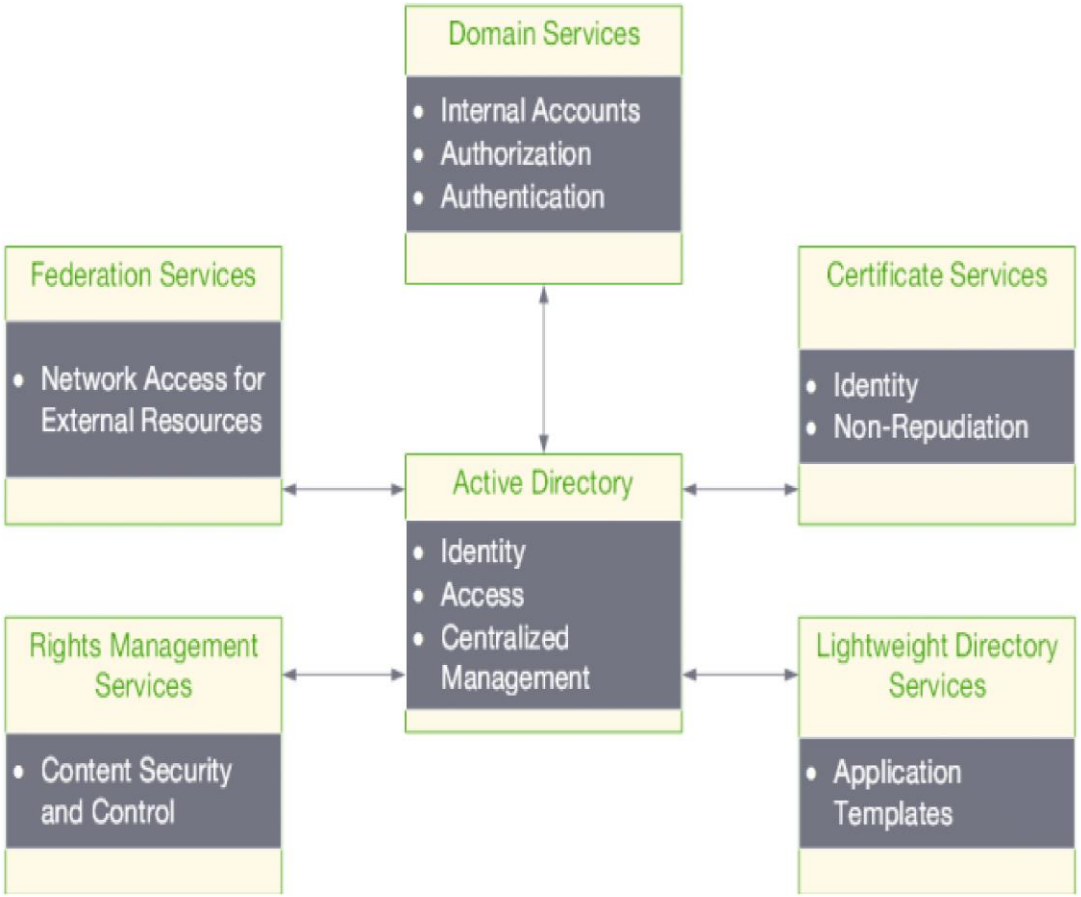
(обов'язковий)

Копії графічної частини



КвРКІ.170238.17.02.06 Е1

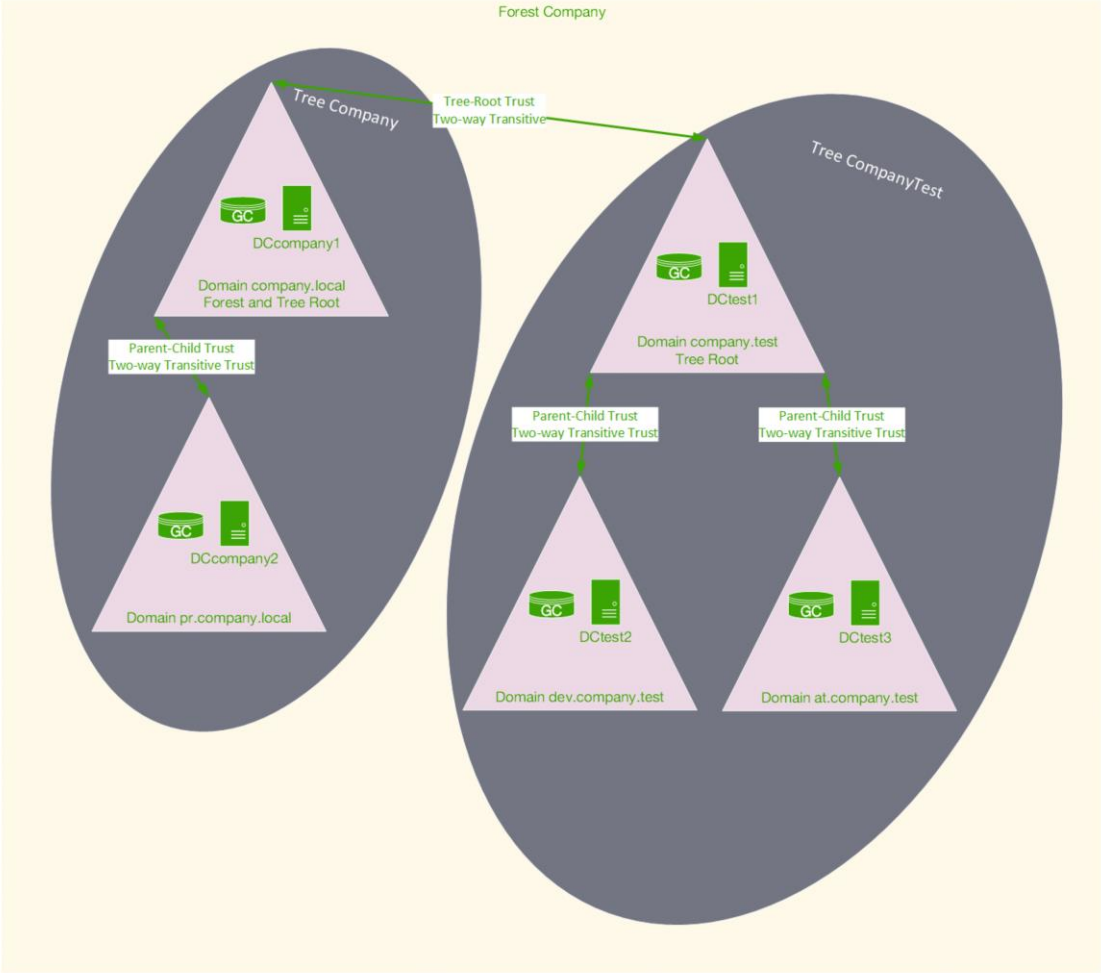
ЛОГІЧНА МОДЕЛЬ ACTIVE DIRECTORY SERVICES



						КвРКІ.170238.17.02.06 Е1	
Зм	Арк	№ Докум	Підпис	Дата	Система авторизації користувачів на основі Active Directory MS Windows Server ЛОГІЧНА МОДЕЛЬ ACTIVE DIRECTORY SERVICES	Літера	Маса / Масштаб
Розроб.		Дашкевич Я.А.				У	
Перевір		Мостовий С.В.				Аркуш 1	Аркушів 3
Н.Контр							
Т. Контр.						ХНУ КІ-17-2	
Затв.							

КвРКІ.170238.17.02.06 Е3

ЛОГІЧНА МОДЕЛЬ ВІДНОСИН ДОМЕНІВ, ДЕРЕВ ТА ЛІСІВ



						КвРКІ.170238.17.02.06 Е3	
Зм.	Арк.	№ Докум.	Підпис	Дата	Система авторизації користувачів на основі Active Directory MS Windows Server ЛОГІЧНА МОДЕЛЬ ВІДНОСИН ДОМЕНІВ, ДЕРЕВ ТА ЛІСІВ	Літера	Маса / Масштаб
Розроб.		Лишантюк Я.А.				У	
Перевір.		Мостовий С.В.				Аркуш 3	Аркушів 3
Н.Контр.						ХНУ КІ-17-2	
Т. Контр.							
Затв.							

ДОДАТОК Б

(обов’язковий)

Лістинг програми авторизації

```
------------------------------ Entities -------------------------------
namespace Project.Data.Entities
{
   public class User
   {
      public int Id { get; set; }
      public Guid Guid { get; set; }
      public string FirstName { get; set; }
      public string LastName { get; set; }
      public string Username { get; set; }
      public string Email { get; set; }
      public string SocketName { get; set; }
      public string Theme { get; set; }
      public bool IsDeleted { get; set; }
      public bool IsAdmin { get; set; }
   }
}


---------------------------------- Data ----------------------------------------
----
namespace Project.Data
{
   public class AppDbContext : DbContext
   {
      public AppDbContext(DbContextOptions<AppDbContext> options)
: base(options) { }
```

```
        public DbSet<User> Users { get; set; }

        protected override void OnModelCreating(ModelBuilder
modelBuilder)
        {
            /*
            * This causes table names in SQL Server to be their singular class
name
            * as opposed to the plural DbSet<T> name.
            *
            * In this case, the table name will be User instead of Users.
            */
            modelBuilder
                .Model
                .GetEntityTypes()
                .ToList()
                .ForEach(x =>
                {
                    modelBuilder
                        .Entity(x.Name)
                        .ToTable(x.Name.Split('.').Last());
                });
        }
    }
}

----------------------------------Web Controllers------------------------------
namespace Project.Web.Controllers
{
    [Route("api/[controller]")]
```

```
public class IdentityController : Controller
{
    private IUserProvider provider;
    private AppDbContext db;

    public IdentityController(IUserProvider provider, AppDbContext db,
IConfiguration config)
    {
        this.provider = provider;
        this.db = db;
    }

    [HttpGet("[action]")]
    public async Task<List<AdUser>> GetDomainUsers() => await
provider.GetDomainUsers();

    [HttpGet("[action]/{search}")]
    public async Task<List<AdUser>>
FindDomainUser([FromRoute]string search) => await
provider.FindDomainUser(search);

    [HttpGet("[action]")]
    public async Task<List<User>> GetUsers() => await db.GetUsers();

    [HttpGet("[action]")]
    public async Task<List<User>> GetDeletedUsers() => await
db.GetUsers(true);

    [HttpGet("[action]/{search}")]
    public async Task<List<User>> SearchUsers([FromRoute]string
search) => await db.SearchUsers(search);
```

```
        [HttpGet("[action]/{search}")]
        public async Task<List<User>>
SearchDeletedUsers([FromRoute]string search) => await
db.SearchUsers(search, true);

        [HttpGet("[action]/{id}")]
        public async Task<User> GetUser([FromRoute]int id) => await
db.GetUser(id);

        [HttpGet("[action]")]
        public async Task<User> SyncUser() => await
provider.CurrentUser.SyncUser(db);

        [HttpPost("[action]")]
        public async Task AddUser([FromBody]AdUser adUser) => await
db.AddUser(adUser);

        [HttpPost("[action]")]
        public async Task UpdateUser([FromBody]User user) => await
db.UpdateUser(user);

        [HttpPost("[action]")]
        public async Task ToggleUserDeleted([FromBody]User user) =>
await db.ToggleUserDeleted(user);

        [HttpPost("[action]")]
        public async Task ToggleAdminUser([FromBody]User user) =>
await db.ToggleAdminUser(user);

        [HttpPost("[action]")]
```

```
        public async Task RemoveUser([FromBody]User user) => await
db.RemoveUser(user);
    }
}
```

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1008348584

Check date:
22.06.2021 21:52:16 EEST

Check type:
Doc vs Internet

Report date:
22.06.2021 21:59:51 EEST

User ID:
100005590

File name: **Дипломна робота Дишкантюк Ярослав (Repaired)(1)_пл**

Page count: **62** Word count: **15559** Character count: **121101** File size: **788.00 KB** File ID: **1008418648**

4.7% Matches

Highest match: **4.38%** with Internet source (**https://studopedia.net/1_48106_rozrahunok-zagalnogo-obsyagu-robit-po-stoa.html**)

4.7% Internet sources **7** ..... Page 64

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters **52**

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 95216 Название: Система автризації користувачів на основі Active Directory MS Windows Server Добавлено в БД: 2021-06-22 Авторы: Дишкантюк Я.А Руководители: Мостовий С.В. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	102763	818	212 (0%)	2 (0%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИУКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Дишкантюк Ярослав Андрійович

Тема Система авторизації користувачів на основі Active Directory MS Windows Server

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3 ; кількість сторінок записки 64.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розробленосистему авторизації користувачів на основі Active Directory MS Windows Server

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційнароботане в повній мірі відповідає поставленому завданню

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, сформульована актуальність. У першому розділі проведено огляд засобів аудиту подій операційнихсистем, виконанеобгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділіметодологічні підходи до вирішення поставленої задачі, особливості процесу авторизації та аутентифікації, та засоби адміністрування віддаленого серверу Windows. В третьому розділірозглянуто мінімальні вимоги щодо встановлення, визначені задачі, які необхідно вирішити для досягнення поставленої мети, проведена оцінка необхідної функціональності, описані стадії розробки та процес реалізації

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність результатів кваліфікаційної роботи полягає у створені системи авторизації на основі Active Directory

5. Негативні сторони роботиРозроблений в роботі модуль має вузький функціонал

6. Оцінка графічного оформлення та пояснювальної записки роботиГрафічне оформлення виконане відповідно до темикваліфікаційноїроботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно,пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційнаробота заслуговує позитивної оцінки.

8. Інші зауваженняОкремі описи в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі.

9. Оцінка кваліфікаційноїроботиВраховуючи всі позитивні та негативні сторони представленоїкваліфікаційноїроботи, можна зробити висновок, що воназаслуговує оцінку «задовільно»D.

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Бурмак О.В. зав. кафедр. КНіТ

«24» Червня 2021. (підпис)

Завідувачу кафедри КБКСМ,
доцент Кльоц Ю.П.

Дишкантюк Я.А.
ПІБ здобувача вищої освіти

ФПКТС, 4 курсу, групи КІ-17-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність плагіату ознайомлений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозиторії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

24.06.2021
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИКОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система авторизації користувачів на основі Active Directory

Автор: Дишкантюк Ярослав Андрійович

Спеціальність: 123 – Комп'ютерна інженерія та програмування

Освітня програма: освітньо-професійна

Науковий керівник: Мостовий Сергій Володимирович, старший викладач

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано послідовності чотирьохрозрядних двійкових кодів, які є вхідними даними до великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.(Тут текст можна і треба модифікувати)

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 0.88% і адресується до 34 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ С. В. Мостовий

Гарант ОП _____ С. М. Лисенко

Завідувач кафедри КІСП _____ Ю. П. Кльоц