ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення кібербезпеки інформаційної системи організації за допомогою AD»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
(код, найменування спеціальності)
освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Олексій ДІМОГЛО

Виконав: здобувач вищої освіти групи БСДМ-61
ДІМОГЛО Олексій
(ПРІЗВИЩЕ, Ім'я)

Керівник: МАРЧЕНКО Віталій
д.ф., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дімоглу Олексію Георгійовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія забезпечення кібербезпеки інформаційної системи організації за допомогою AD»
керівник кваліфікаційної роботи: МАРЧЕНКО Віталій, д.ф., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
технологія забезпечення кібербезпеки інформаційної системи організації за допомогою AD
наукова та технічна література, експлуатаційна документація,
нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми забезпечення кібербезпеки інформаційної системи організації.
2. Методи та засоби захисту інформаційної системи організації.
3. Технологія забезпечення кібербезпеки інформаційної системи організації на базі AD

5. Перелік ілюстративного матеріалу: Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми захисту в інформаційній системі організації	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз проблеми забезпечення кібербезпеки інформаційної системи організації.	27.10. 2023р.	
4.	Методи та засоби захисту інформаційної системи організації.	03.11.2023 р.	
5.	Технологія забезпечення кібербезпеки інформаційної системи організації на базі AD	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач вищої освіти _____ Олексій ДІМОГЛО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Дімогло О.Г. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія забезпечення кібербезпеки інформаційної системи організації за допомогою AD».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***ДІМОГЛО Олексій*** обрав тему роботи, метою якої було дослідити зміст технології забезпечення кібербезпеки організації. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ДІМОГЛО Олексій*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ДІМОГЛО Олексій*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Дімогло О.Г. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Дімогло Олексія
на тему: «Технологія забезпечення кібербезпеки інформаційної системи організації за допомогою AD».

Актуальність:
У сучасному світі кіберзагрози стають все більш складними та розповсюдженими. Хакерські атаки, віруси, фішингові атаки та інші загрози стають невід'ємною частиною кіберпростору. Застосування AD дозволяє створювати ефективні стратегії захисту від цих загроз. Організації використовують все більше інформаційних систем та облікових записів. AD допомагає в управлінні цим складом, автоматизуючи процеси автентифікації, авторизації та управління правами доступу. Один із основних аспектів кібербезпеки - це управління ідентичністю користувачів і ресурсів. AD дозволяє створювати централізовану систему управління ідентичністю, зменшуючи ризики втрати чутливої інформації через несанкціонований доступ. Усі ці аспекти роблять тему роботи актуальною та важливою для організацій в умовах сучасного цифрового середовища.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення кібербезпеки інформаційної системи організації.
2. Досліджено методи та засоби забезпечення кібербезпеки інформаційної системи організації.
3. Запропоновано варіант технології забезпечення кібербезпеки інформаційної системи організації.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б більш детально описати різні методи та засоби забезпечення кібербезпеки організації.
2. Запропонований варіант технології забезпечення кібербезпеки інформаційної системи організації доцільно було представити на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре**», а здобувач **ДІМОГЛО Олексій** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ _____

підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 68 сторінок, 31 рисунок, 15 джерел.

Об'єкт дослідження – процес забезпечення кібербезпеки інформаційної системи організації.

Предмет дослідження – технологія забезпечення кібербезпеки за допомогою Active Directory.

Мета роботи – розробити варіанти технології забезпечення кібербезпеки за допомогою Active Directory для інформаційної системи організації та рекомендації щодо застосування технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, моделювання процесу забезпечення кібербезпеки за допомогою Active Directory.

В роботі проведено аналіз проблеми забезпечення кібербезпеки інформаційної системи організації. Проведено аналіз існуючих технологій забезпечення захисту інформаційної системи.

Запропоновано варіант технологій захисту за допомогою Active Directory. Визначено основні функції, можливості, склад компонентів та архітектуру обраного рішення.

На основі проведених досліджень, в роботі розроблено варіант технології забезпечення кібербезпеки інформаційної системи організації на базі рішення Active Directory.

Галузь використання – кібербезпека корпоративної мережі.

ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ACTIVE DIRECTORY, АВТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, УПРАВЛІННЯ МЕРЕЖЕЮ ТА КОРИСТУВАЧАМИ

ABSTRACT

The text part of the qualification work for the master's degree: 68 pages, 31 figures, 15 sources.

The object of research is the process of ensuring cyber security of the organization's information system.

The subject of research is the technology of ensuring cyber security using Active Directory.

The purpose of the work is to develop options for the technology of ensuring cyber security using Active Directory for the information system of the organization and recommendations for the use of the technology.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards, modeling of the process of ensuring cyber security using Active Directory.

The paper analyzes the problem of ensuring cyber security of the organization's information system. An analysis of the existing technologies for ensuring the protection of the information system was carried out.

A variant of protection technologies using Active Directory is offered. The main functions, capabilities, composition of components and the architecture of the selected solution are defined.

On the basis of the conducted research, the paper developed a variant of the technology for ensuring cyber security of the organization's information system based on the Active Directory solution.

The field of use is cyber security of the corporate network.

INFORMATION SYSTEM, CYBER SECURITY, ACTIVE DIRECTORY, AUTHENTICATION, ACCESS CONTROL, NETWORK AND USER MANAGEMENT.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD - Active Directory

ACL - список керування доступом

RBAC - контроль доступу на основі ролей

MFA - Multi-Factor Authentication

SSO - Single Sign-On

LDAP - Lightweight Directory Access Protocol

DNS - Domain Name System

DHCP - Dynamic Host Configuration Protocol

ADFS - Active Directory Federation Services

ADUC - Active Directory Users and Computers

ВСТУП

Актуальність дослідження. У світі, який все більше цифровизується, збільшується кількість та складність кіберзагроз. Хакерські атаки, віруси, розповсюдження шкідливого програмного забезпечення та інші кіберзагрози стають реальними викликами для організацій. Active Directory надає централізований механізм управління ідентичністю користувачів, груп та ресурсів в корпоративному середовищі. Це стає критично важливим для забезпечення високого рівня безпеки та контролю доступу. З впровадженням нових регуляцій та стандартів безпеки, організації повинні дотримуватися строгих вимог щодо захисту конфіденційної інформації. AD дозволяє організаціям ефективно виконувати ці вимоги через централізований контроль доступу та аутентифікації. Організації обробляють та зберігають все більше конфіденційної інформації. Захист цієї інформації від несанкціонованого доступу стає надзвичайно важливим завданням, і AD може служити ефективним інструментом для забезпечення безпеки даних. З впровадженням нових технологій та розширенням корпоративних мереж зростає потреба в ефективних засобах управління доступом та забезпечення безпеки великої кількості ресурсів.

Узагальнюючи, технологія забезпечення кібербезпеки через використання Active Directory залишається критично важливою в сучасному світі, де безпека інформації стає ключовим пріоритетом для організацій у всіх галузях.

Вищенаведені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження технології забезпечення кібербезпеки організації за допомогою Active Directory.

Об'єкт дослідження – процес забезпечення кібербезпеки інформаційної системи організації.

Предмет дослідження – технологія забезпечення кібербезпеки за допомогою Active Directory.

Мета роботи – розробити варіанти технології забезпечення кібербезпеки за допомогою Active Directory для інформаційної системи організації та рекомендації щодо застосування технології.

Наукові завдання:

дослідити сутність проблеми забезпечення безпеки інформаційної системи організації;

проаналізувати сучасні методи та підходи до забезпечення кібербезпеки в інформаційних системах;

проаналізувати функціональні можливості Active Directory.

розглянути можливості підвищення рівня безпеки систем, побудованих на основі Active Directory, враховуючи сучасні загрози.

розробити та визначити методи та стратегії для захисту інформаційних систем організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, моделювання процесу забезпечення кібербезпеки за допомогою Active Directory.

Практичне значення одержаних результатів полягає в розробці варіанта забезпечення кібербезпеки інформаційної системи організації на базі Active Directory, а також у розробці рекомендацій щодо застосування технології захисту в інформаційних системах організацій.

Апробація результатів кваліфікаційної роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ

1.1. Аналіз основних загроз забезпечення кібербезпеки організації

Організації все більше використовують інформаційні технології (ІТ) для покращення бізнес-операцій і процесів прийняття рішень, тому інформаційна безпека є однією з найактуальніших проблем, з якими стикаються організації в усьому світі, що впливає на організаційні стійкі інформаційні системи та безперервність бізнесу. Однак багато керівників і співробітників не приділяють достатньої уваги питанням інформаційної безпеки в своїх організаціях. Як наслідок, комп'ютерні системи більшості організацій набагато менш безпечні, ніж вони повинні бути, а збитки через порушення інформаційної безпеки зростають.

Співробітники є найслабшою ланкою в інформаційній безпеці та першопричиною порушень інформаційної безпеки, або через те, що вони беруть участь у неправомірних діях на робочому місці, які загрожують інформаційній безпеці організації, або тому, що вони надають можливість комп'ютерним хакерам атакувати або зламати комп'ютери їхньої організації.

Було виявлено різні типи поганої поведінки співробітників, пов'язаної з безпекою, включаючи зловживання комп'ютером, зловживання інформаційними системами, зловживання ІТ, непов'язані з роботою обчислення, упущена поведінка та порушення інформаційної безпеки.

Було визначено чотири основні типи неетичної поведінки щодо інформаційної безпеки: неправильна поведінка в мережах/додатках, небезпечне використання Інтернету, упущення безпеки та поганий контроль доступу.

Неналежна поведінка в мережах/додатках

Діяльність у цій категорії зосереджена на зловживанні мережами та/або програмами на робочому місці. Така неналежна поведінка була проблематичною принаймні з 2000-х років і є загальною неетичною поведінкою на робочому місці.

Неналежна поведінка в мережах/додатках є проблемою всередині організацій, оскільки це може надати стороннім особам можливість атакувати або іншим чином завдати шкоди комп'ютерам організації та призвести до втрати інформації компанії та витоку до третіх сторін, тим самим загрожуючи конфіденційності, власності та доступності інформації компанії. Крім того, за визначенням, неналежна поведінка в мережах/додатках передбачає використання незаконного програмного забезпечення, яке впливає на конфіденційність інформації та є загальною проблемою на робочому місці. Співробітники поводяться неналежним чином у мережах/додатках головним чином тому, що хочуть отримати особисті вигоди, такі як економія часу.

Небезпечне використання Інтернету

Діяльність, пов'язана з небезпечним використанням Інтернету, пов'язана із зловживанням Інтернетом. Особисте користування Інтернетом співробітників стосується не пов'язаного з роботою використання Інтернету в особистих цілях на роботі, і це поширена, але відносно нова форма неетичної поведінки на робочому місці. За даними Websense, близько двох третин опитаних співробітників визнали, що витрачають час на особистий Інтернет-серфінг за допомогою офісних комп'ютерів, при цьому середня кількість часу, витраченого на таку діяльність, становить близько трьох годин на тиждень. Однак деякі дослідники припустили, що дозвіл співробітникам використовувати Інтернет з особистих причин під наглядом може зробити їх більш творчими та продуктивними. Іншими словами, особисте використання Інтернету може бути корисним для організацій, якщо воно належним чином контролюється.

Таким чином, згідно з нашим визначенням неетичної поведінки щодо інформаційної безпеки, особисте користування Інтернетом співробітників не може вважатися неетичною поведінкою щодо інформаційної безпеки, якщо працівники дуже обережно переглядають Інтернет і таке використання не впливає на конфіденційність, точність, власність або доступність інформації компанії. Однак якщо працівники використовують Інтернет небезпечно, наприклад, для перегляду підозрілих веб-сайтів, така дія одразу стає прикладом неетичної поведінки щодо

інформаційної безпеки. Оскільки підозрілі веб-сайти часто є джерелами зловмисного програмного забезпечення та шахрайства, така поведінка може призвести до витоку інформації про компанію або злому комп'ютерної системи компанії, що створює загрозу інформаційній безпеці для організації.

Таким чином, небезпечне використання Інтернету є типом неетичної поведінки щодо безпеки інформації, яка впливає на власність і доступність інформації компанії. Крім того, якщо працівникам взагалі заборонено переглядати Інтернет на робочому місці (тобто будь-яке особисте використання Інтернету заборонено), тоді будь-яке використання Інтернету з особистих причин вважається небезпечним використанням Інтернету згідно з нашим визначенням неетичної поведінки щодо безпеки інформації як така поведінка не відповідає політиці організації. Співробітники можуть отримати особисту вигоду через небезпечне використання Інтернету: наприклад, завантажувати музичні файли з підозрілих веб-сайтів для задоволення.

Недостатні дії для забезпечення безпеки

Такі дії виникають, коли працівники, які знають, як захистити інформацію компанії, не роблять цього. Це стосується розриву «знання–роблення» в інформаційній безпеці. Співробітники, які ведуть такий тип поведінки, можуть не мати наміру пошкодити свої організаційні комп'ютерні системи, але вони не піклуються про безпеку. Однак така поведінка може небезпечно вплинути на доступність, конфіденційність і цілісність інформації, оскільки залучені дії можуть спричинити витік інформації, що, у свою чергу, загрожує власності інформації компанії. Наголошується, що недостатні дії для забезпечення безпеки загрожує цілісності критично важливих систем і потребує серйозної уваги. Недостатня безпека охоплює широкий спектр дій співробітників, як-от залишення роздруківок без нагляду в офісі або забуття резервного копіювання комп'ютерних систем.

Поганий контроль доступу

Контроль доступу тісно пов'язаний з уразливістю інформаційної безпеки та конфіденційністю інформації. Успішний підхід до контролю доступу гарантує безпеку інформації та запобігає несанкціонованому доступу до даних компанії.

Навпаки, поганий контроль доступу порушує правила компанії щодо безпеки даних. Поганий контроль доступу передбачає не лише неадекватний контроль безпеки даних, наприклад несанкціонований доступ, але й слабкі заходи захисту даних, наприклад неправильне використання пароля. Обидва типи поведінки можуть призвести до витоку інформації. Багато досліджень виявили, що працівники не мають належних заходів захисту для захисту інформації на своїх робочих комп'ютерах і, як правило, створюють прості паролі, які легко запам'ятати, для зручності. Деякі співробітники навіть залишають написані паролі на видних місцях, наприклад, на листочках, приклеєних до своїх моніторів. Хоча працівники зазвичай не отримують миттєвої особистої вигоди від такої поведінки, поганий контроль доступу є фізичним типом неетичної поведінки щодо безпеки інформації, яка може призвести до неправомірного доступу неавторизованих користувачів до інформації компанії [1].

1.2. Аналіз концепцій забезпечення інформаційної безпеки організації

Оскільки комп'ютери та інші цифрові пристрої стали важливими для бізнесу та торгівлі, вони також дедалі частіше стають об'єктами атак. Для того, щоб компанія чи окрема особа могли впевнено використовувати комп'ютерний пристрій, вони спочатку повинні бути впевнені, що пристрій жодним чином не скомпрометовано та що всі комунікації будуть безпечними. Розглянемо фундаментальні концепції безпеки інформаційних систем і заходи, які можна вжити для пом'якшення загроз безпеці.

Тріада безпеки

Рис.1.1. Тріада інформаційної безпеки: конфіденційність, цілісність, доступність (CIA)

Конфіденційність

Захищаючи інформацію, потрібно обмежити доступ для тих, кому дозволено її переглядати; всім іншим має бути заборонено дізнаватися що-небудь про його зміст. Наприклад, федеральний закон вимагає, щоб університети обмежували доступ до приватної інформації про студентів. Університет повинен бути впевнений, що лише авторизовані особи мають доступ до перегляду записів оцінок.

Цілісність

Цілісність — це впевненість у тому, що інформація, до якої здійснюється доступ, не була змінена та справді відповідає призначенню. Інформація може втратити свою цілісність через зловмисний намір, наприклад, коли неавторизована особа вносить зміни, щоб навмисно спотворити щось. Прикладом цього може бути те, що хакера наймають, щоб зайти в систему університету та змінити оцінку.

Цілісність також може бути втрачена ненавмисно, наприклад, коли стрибок напруги комп’ютера пошкоджує файл або хтось, уповноважений вносити зміни, випадково видаляє файл або вводить неправильну інформацію.

Доступність

Доступність інформації – третя частина тріади. Доступність означає, що будь-хто, уповноважений на це, може отримати доступ до інформації та змінити її у відповідний проміжок часу. Залежно від типу інформації відповідні часові рамки

можуть означати різні речі. Наприклад, біржовий трейдер потребує негайної доступності інформації, тоді як продавець може бути радий отримати дані про продажі за день у звіті наступного ранку. Такі компанії, як Amazon.com, вимагатимуть, щоб їхні сервери були доступні двадцять чотири години на добу, сім днів на тиждень. Інші компанії можуть не постраждати, якщо їхні веб-сервери час від часу не працюють на кілька хвилин.

Щоб забезпечити конфіденційність, цілісність і доступність інформації, організації можуть вибирати з безлічі інструментів. Кожен із цих інструментів можна використовувати як частину загальної політики інформаційної безпеки.

Автентифікація

Інструменти автентифікації використовуються для того, щоб переконатися, що особа, яка отримує доступ до інформації, справді є тією, за кого себе представляє [4].

Автентифікацію можна здійснити шляхом ідентифікації людини за одним або декількома з трьох факторів: те, що вони знають, те, що вони мають, або те, чим вони є. Наприклад, найпоширенішою формою автентифікації сьогодні є ідентифікатор користувача та пароль. У цьому випадку автентифікація виконується шляхом підтвердження того, що користувач знає (його ідентифікатора та пароля). Але цю форму автентифікації легко скомпрометувати, і іноді потрібні більш надійні форми автентифікації. Ідентифікувати когось лише за тим, що у нього є, наприклад, за ключем чи карткою, також може бути проблематично. Якщо ідентифікаційний маркер втрачено або викрадено, ідентифікаційну інформацію можна легко вкрасти. Набагато важче піти на компроміс із останнім фактором, яким ви є. Цей фактор ідентифікує користувача за допомогою фізичних характеристик, таких як сканування ока або відбиток пальця. Ідентифікація людини за її фізичними характеристиками називається біометрією.

Більш безпечний спосіб автентифікації користувача — багатофакторна автентифікація. Поєднуючи два чи більше факторів, перерахованих вище, комусь стає набагато важче представити себе в оманливій формі. Прикладом цього може бути використання Маркер RSA SecurID. Пристрій RSA — це те, що залишається

у користувача, і він генеруватиме новий код доступу кожні шістдесят секунд. Щоб увійти на інформаційний ресурс за допомогою пристрою RSA, поєднується відомий чотиризначний PIN-код із кодом, згенерованим пристроєм. Єдиний спосіб належної автентифікації — це знати код і мати пристрій RSA.

Управління доступом

Після автентифікації користувача наступним кроком є переконатися, що він може отримати доступ лише до відповідних інформаційних ресурсів. Це робиться за допомогою контролю доступу. Контроль доступу визначає, хто з користувачів має право читати, змінювати, додавати та/або видаляти інформацію. Існує кілька різних моделей контролю доступу, наприклад: список керування доступом (ACL) і контроль доступу на основі ролей (RBAC).

Для кожного інформаційного ресурсу, яким організація бажає керувати, можна створити список користувачів, які мають можливість виконувати певні дії. Це список контролю доступу або ACL. Для кожного користувача призначаються певні можливості, такі як читання, запис, видалення або додавання. Лише користувачі з такими можливостями можуть виконувати ці функції. Якщо користувача немає в списку, він не має можливості навіть знати про існування інформаційного ресурсу.

ACL прості для розуміння та обслуговування. Однак вони мають кілька недоліків. Основним недоліком є те, що кожним інформаційним ресурсом керують окремо, тому, якщо адміністратор безпеки захоче додати або видалити користувача до великого набору інформаційних ресурсів, це буде досить важко. І зі збільшенням кількості користувачів і ресурсів, ACL стає важче підтримувати. Це призвело до вдосконаленого методу контролю доступу, який називається контроль доступу на основі ролей або RBAC. За допомогою RBAC замість надання певним користувачам прав доступу до інформаційного ресурсу користувачам призначаються ролі, а потім цим ролям призначається доступ. Це дозволяє адміністраторам окремо керувати користувачами та ролями, спрощуючи адміністрування та, як наслідок, покращуючи безпеку.

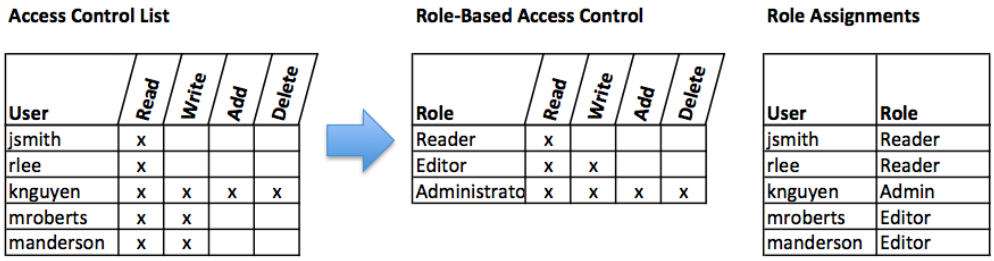

Рис.1.2. Порівняння ACL і RBAC

Шифрування

Багато разів організації потрібно передавати інформацію через Інтернет або переносити її на зовнішні носії, такі як компакт-диск або флеш-накопичувач. У цих випадках навіть за належної автентифікації та контролю доступу неавторизована особа може отримати доступ до даних. Шифрування – це процес кодування даних під час їх передачі або зберігання, щоб лише авторизовані особи могли їх прочитати. Це кодування виконується комп'ютерною програмою, яка кодує звичайний текст, який потрібно передати; потім одержувач отримує зашифрований текст і декодує його (дешифрування). Щоб це працювало, відправник і одержувач повинні домовитися про метод кодування, щоб обидві сторони могли правильно спілкуватися. Обидві сторони мають спільний ключ шифрування, що дозволяє їм кодувати та декодувати повідомлення один одного. Це називається шифруванням із симетричним ключем. Цей тип шифрування є проблематичним, оскільки ключ доступний у двох різних місцях.

Альтернативою шифруванню з симетричним ключем є шифрування з відкритим ключем. У шифруванні з відкритим ключем використовуються два ключі: відкритий і закритий. Щоб надіслати зашифроване повідомлення, ви отримуєте відкритий ключ, кодуєте повідомлення та надсилаєте його. Потім одержувач використовує закритий ключ для його декодування. Відкритий ключ можна надати кожному, хто бажає надіслати одержувачу повідомлення. Кожному користувачеві просто потрібен один приватний ключ і один відкритий ключ, щоб захистити повідомлення. Приватний ключ необхідний, щоб розшифрувати щось, надіслане з відкритим ключем.

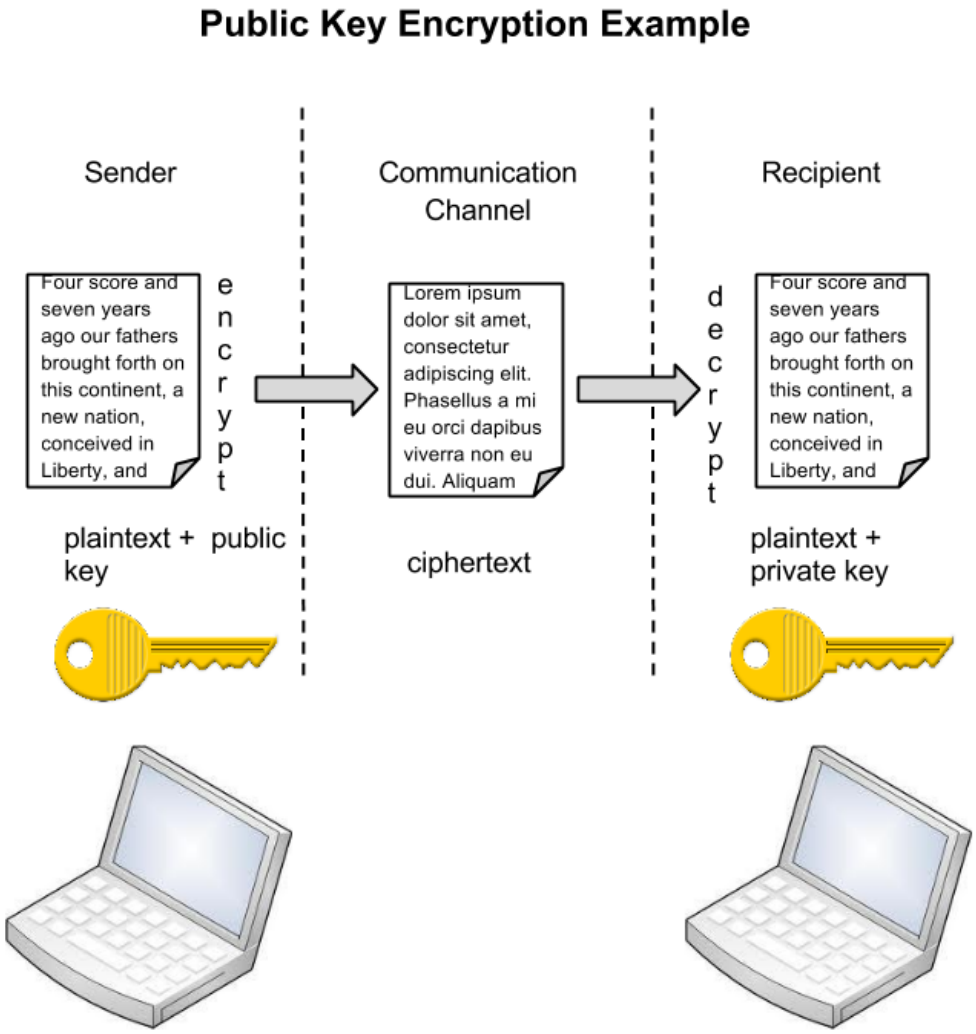

Рис.1.3. Шифрування відкритим ключем

Безпека пароля

Однофакторну автентифікацію надзвичайно легко скомпрометувати. Необхідно запровадити хорошу політику паролів, щоб гарантувати, що паролі не можуть бути скомпрометовані. Нижче наведено деякі з найпоширеніших політик, які організації повинні запровадити.

Вимагати складних паролів. Однією з причин зламу паролів є те, що їх легко вгадати. Нещодавнє дослідження показало, що трійкою найпопулярніших паролів у 2012 році були пароль 123456 і 12345678. Пароль не повинен бути простим або словом, яке можна знайти в словнику. Одна з перших речей, які зробить хакер, це спробує зламати пароль, перевіривши кожен термін у словнику! Натомість хороша політика паролів передбачає використання щонайменше восьми символів і

принаймні однієї літери верхнього регістру, одного спеціального символу та однієї цифри.

Регулярно змінюйте паролі. Важливо, щоб користувачі регулярно змінювали свої паролі. Користувачі повинні змінювати свої паролі кожні шістдесят-дев'яносто днів, гарантуючи, що жодні паролі, які могли бути вкрадені або вгадані, не зможуть бути використані проти компанії.

Навчіть співробітників не розголошувати паролі. Одним із основних методів, який використовується для викрадення паролів, є просто з'ясувати їх, запитавши користувачів або адміністраторів. Надсилання претексту відбувається, коли зловмисник телефонує до служби підтримки або адміністратора безпеки та видає себе за певного авторизованого користувача, який має проблеми з входом. Потім, надаючи особисту інформацію про авторизованого користувача, зловмисник переконує особу безпеки скинути пароль і повідомити йому, що Це є. Інший спосіб, за допомогою якого співробітники можуть бути обманом змусити надати паролі, — це фішинг електронної пошти. Фішинг виникає, коли користувач отримує електронний лист, який виглядає так, ніби він надійшов із надійного джерела, наприклад від банку чи роботодавця. В електронному листі користувача просять натиснути посилання та увійти на веб-сайт, який імітує справжній веб-сайт, і ввести свій ідентифікатор і пароль, які потім переймаються зловмисником.

Резервні копії

Іншим важливим інструментом інформаційної безпеки є комплексний план резервного копіювання для всієї організації. Слід створювати резервні копії не лише даних на корпоративних серверах, але й окремих комп'ютерів, які використовуються в організації. Хороший резервний план повинен складатися з кількох компонентів.

1. Повне розуміння інформаційних ресурсів організації.
2. Регулярне резервне копіювання всіх даних.
3. Окреме зберігання резервних копій даних
4. Тест відновлення даних.

Брандмауери

Ще один метод, який організація повинна використовувати для підвищення безпеки у своїй мережі, — це брандмауер. Брандмауер може існувати у вигляді апаратного чи програмного забезпечення (або обох). Апаратний брандмауер – це пристрій, підключений до мережі та фільтруючий пакети на основі набору правил. Програмний брандмауер працює в операційній системі та перехоплює пакети, щойно вони надходять на комп'ютер. Брандмауер захищає всі сервери та комп'ютери компанії, зупиняючи пакети ззовні мережі організації, які не відповідають суворому набору критеріїв. Брандмауер також може бути налаштований для обмеження потоку пакетів, що залишають організацію. Це може бути зроблено, щоб виключити можливість перегляду відео YouTube або використання Facebook із комп'ютера компанії.

Деякі організації можуть запровадити кілька брандмауерів як частину конфігурації безпеки мережі, створивши одну або кілька частково захищених частин своєї мережі. Цей сегмент мережі називають DMZ, запозичивши термін демілітаризована зона у військових, і це місце, де організація може розміщувати ресурси, які потребують більш широкого доступу, але все ще потребують безпеки.

Системи виявлення вторгнень

Іншим пристроєм, який можна розмістити в мережі з метою безпеки, є система виявлення вторгнень або IDS. IDS не додає додаткової безпеки; натомість він надає функціональні можливості для виявлення атаки на мережу. IDS можна налаштувати для спостереження за певними типами дій, а потім сповіщення персоналу служби безпеки, якщо така діяльність відбувається. IDS також може реєструвати різні типи трафіку в мережі для подальшого аналізу. IDS є важливою частиною будь-якої надійної системи безпеки.

Віртуальні приватні мережі

Використовуючи брандмауери та інші технології безпеки, організації можуть ефективно захистити багато своїх інформаційних ресурсів, зробивши їх невидимими для зовнішнього світу.

VPN дозволяє користувачеві, який знаходиться за межами корпоративної мережі, обійти брандмауер і отримати доступ до внутрішньої мережі ззовні.

Завдяки поєднанню програмного забезпечення та заходів безпеки це дозволяє організації дозволити обмежений доступ до своїх мереж, водночас забезпечуючи загальну безпеку.

Фізична безпека

Організація може запровадити найкращу у світі схему автентифікації, розробити найкращий контроль доступу та встановити брандмауери та засоби запобігання вторгненням, але її безпека не може бути повною без впровадження фізичної безпеки. Фізична безпека — це захист фактичного обладнання та мережевих компонентів, які зберігають і передають інформаційні ресурси. Щоб запровадити фізичну безпеку, організація повинна ідентифікувати всі вразливі ресурси та вжити заходів, щоб гарантувати, що ці ресурси неможливо фізично підробити або вкрасти. Ці заходи включають наступне.

Політика безпеки

Окрім перелічених вище технічних засобів контролю, організаціям також необхідно запровадити політику безпеки як форму адміністративного контролю. Насправді ці політики повинні стати відправною точкою в розробці загального плану безпеки. Хороша політика інформаційної безпеки містить вказівки щодо використання працівниками інформаційних ресурсів компанії та забезпечує компанію регресом у випадку, якщо працівник порушує політику.

За даними Інституту SANS, хороша політика — це «формальна, коротка заява або план високого рівня, який охоплює загальні переконання організації, цілі, завдання та прийнятні процедури для певної предметної галузі». Політики вимагають відповідності; недотримання політики призведе до дисциплінарної відповідальності. Політика не визначає конкретних технічних деталей, натомість вона зосереджується на бажаних результатах. Політика безпеки має ґрунтуватися на керівних принципах конфіденційності, цілісності та доступності.

Хорошим прикладом політики безпеки, яка багатьом знайома, є політика використання Інтернету. Політика використання веб-сайтів визначає обов’язки працівників компанії, коли вони використовують ресурси компанії для доступу до Інтернету.

Політика безпеки також повинна регулювати будь-які державні чи галузеві норми, які стосуються організації. Наприклад, якщо організація є університетом, вона повинна знати про Закон про права сім'ї на освіту та конфіденційність (FERPA), який обмежує доступ до інформації про студентів. Організації охорони здоров'я зобов'язані дотримуватися кількох нормативних актів, наприклад Закону про перенесення та підзвітність медичного страхування (HIPAA).

Мобільна безпека

Оскільки використання мобільних пристроїв, таких як смартфони та планшети, поширюється, організації повинні бути готові вирішувати унікальні проблеми безпеки, пов'язані з використанням цих пристроїв. Одне з перших питань, яке повинна розглянути організація, це чи дозволяти мобільні пристрої на робочому місці взагалі. Створення політики BYOD («Візьміть свій власний пристрій») дозволяє співробітникам повніше інтегрувати себе у свою роботу та може принести працівникам більше задоволення та продуктивності. У багатьох випадках може бути практично неможливо заборонити співробітникам мати власні смартфони чи iPad на робочому місці. Якщо організація надає пристрої своїм співробітникам, вона отримує більше контролю над використанням пристроїв, але також наражає себе на ймовірність адміністративного (і дорогого) безладу.

Мобільні пристрої можуть створювати багато унікальних проблем безпеки для організації. Ймовірно, однією з найбільших проблем є крадіжка інтелектуальної власності. Для співробітника зі зловмисними намірами було б дуже простим підключити мобільний пристрій до комп'ютера через USB-порт або бездротовим способом до корпоративної мережі та завантажити конфіденційні дані. Також було б легко таємно зробити якісний знімок за допомогою вбудованої камери.

Коли працівник має дозвіл на доступ і збереження даних компанії на своєму пристрої, виникає інша загроза безпеці: цей пристрій тепер стає мішенню для злодіїв. Крадіжка мобільних пристроїв (в даному випадку, включаючи ноутбуки) є одним із основних методів, які використовують викрадачі даних.

Отже, що можна зробити для захисту мобільних пристроїв? Почнеться з хорошої політики щодо їх використання. Згідно з дослідженням SANS, організаціям слід розглянути можливість розробки політики щодо мобільних пристроїв, яка стосується таких питань: використання камери, використання запису голосу, придбання програм, шифрування в стані спокою, налаштування автоматичного з'єднання Wi-Fi, налаштування Bluetooth, використання VPN, налаштування пароля, звіт про втрачений або викрадений пристрій і резервне копіювання.

Крім політики, існує кілька різних інструментів, які організація може використовувати для пом'якшення деяких із цих ризиків. Наприклад, якщо пристрій вкрадено або втрачено, програмне забезпечення геолокації може допомогти організації знайти його. У деяких випадках може навіть мати сенс інсталювати програмне забезпечення для віддаленого видалення даних, яке видалить дані з пристрою, якщо вони становлять загрозу безпеці.

Юзабіліті

Прагнучи захистити інформаційні ресурси, організації повинні збалансувати потребу в безпеці з потребою користувачів ефективно отримувати доступ до цих ресурсів і використовувати їх. Якщо заходи безпеки системи ускладнюють її використання, користувачі знайдуть способи обійти безпеку, що може зробити систему більш вразливою, ніж це було б без заходів безпеки. Візьмемо, наприклад, політику паролів. Якщо в організації потрібен надзвичайно довгий пароль із кількома спеціальними символами, працівник може вдатися до того, щоб записати його та покласти в ящик, оскільки його буде неможливо запам'ятати [2].

1.3. Аналіз методів та засобів забезпечення кібербезпеки організації

Для забезпечення кібербезпеки організації використовуються різні методи та засоби, наприклад:

Multi-Factor Authentication (MFA): метод аутентифікації, який використовує два або більше різних методів перевірки ідентичності користувача для

забезпечення доступу до системи або послуги. Основна ідея MFA полягає в тому, щоб ускладнити процес несанкціонованого доступу, вимагаючи додаткові форми ідентифікації, окрім традиційного пароля. MFA допомагає підвищити рівень безпеки, оскільки навіть якщо один елемент аутентифікації (наприклад, пароль) стає відомим або компромітованим, інші фактори забезпечують додатковий шар захисту. Використання MFA стає все більш важливим у світлі зростання кількості кіберзагроз і намагань надзвичайно підвищити рівень безпеки в інформаційних системах.

Endpoint Protection відноситься до комплексу заходів та технологій, спрямованих на захист кінцевих точок (endpoint) в інформаційних системах від різних кіберзагроз та вразливостей. Кінцеві точки можуть включати комп'ютери, ноутбуки, смартфони, планшети та інші пристрої, які мають доступ до корпоративної мережі або Інтернету. Захист кінцевих пристроїв важливий для бізнесів та користувачів, оскільки кінцеві точки часто є місцем атак для кіберзлочинців. Застосування відповідних заходів допомагає зменшити ризик витоку інформації, втрати даних та завдання шкоди системам.

Role-Based Access Control (RBAC) - стратегія управління доступом, при якій доступ до ресурсів та функціональності системи контролюється на основі ролі, яку виконує користувач. У рамках RBAC, користувачам надається доступ до ресурсів відповідно до їхніх ролей в організації або системі. RBAC є популярною моделлю управління доступом та використовується в різних галузях, включаючи інформаційні технології, банківську сферу, охорону здоров'я та інші області, де забезпечення безпеки та ефективного управління доступом є критично важливими.

Single Sign-On (SSO) — це метод аутентифікації та авторизації, який дозволяє користувачам отримувати доступ до різних систем та служб із використанням одного набору облікових даних. Замість того, щоб вводити ідентифікаційні дані (логін і пароль) для кожної окремої системи, користувач вводить їх лише один раз, і ці дані використовуються для доступу до різних ресурсів. Процес SSO може бути реалізований різними технічними методами, такими як використання токенів, куки, аутентифікація за допомогою сертифікатів тощо. Популярні протоколи для

реалізації SSO включають OAuth, OpenID Connect, SAML (Security Assertion Markup Language) та інші.

SSO використовується в різних областях, таких як корпоративні мережі, хмарні сервіси, веб-сайти та інші системи, де важливо забезпечити зручний та безпечний доступ до ресурсів для користувачів.

Active Directory (AD) є сервісом керування ідентичністю та доступом, який розроблений компанією Microsoft і використовується для управління користувачами, групами, комп'ютерами та іншими ресурсами в мережевому середовищі. AD використовується з різними технологіями для забезпечення кібербезпеки, такими як:

— LDAP (Lightweight Directory Access Protocol): Active Directory використовує LDAP для доступу до своєї бази даних ідентичності. Інші системи, особливо ті, які також використовують концепції каталогу, можуть використовувати LDAP для управління ідентичністю.

— Kerberos: протокол аутентифікації, який широко використовується в сфері кібербезпеки. Active Directory використовує Kerberos для забезпечення безпечної аутентифікації користувачів.

— Single Sign-On (SSO): використовується як джерело ідентичності для систем SSO.

— Role-Based Access Control (RBAC) Active Directory може використовуватись для реалізації RBAC, але існують інші системи керування доступом, які також використовують цей принцип..

— Multi-Factor Authentication (MFA) Active Directory може інтегруватись з системами MFA для забезпечення додаткового рівня безпеки.

— Захист кінцевих пристроїв: Active Directory може використовуватися для централізованого управління політикою безпеки для кінцевих точок [5].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЧЕННЯ КІБЕРБЕЗПЕКИ ОРАГНІЗАЦІЇ ЗА ДОПОМОГОЮ ACTIVE DIRECTORY

2.1. Призначення, можливості та функції Active Directory

У величезному просторі сучасних технологій організації значною мірою покладаються на надійні та ефективні системи керування своєю цифровою інфраструктурою. У тому числі Active Directory (AD) виділяється як фундаментальний компонент підприємств будь-якого розміру.

Active Directory, розроблена Microsoft, слугує центральним вузлом для управління та організації користувачів, комп'ютерів та інших ресурсів мережі. Завдяки своїм універсальним можливостям та комплексним функціям AD спрощує адміністрування та підвищує безпеку широкого спектру мережевих служб, що робить його незамінним інструментом у сфері забезпечення кібербезпеки організації [3].

Служби каталогів є критично важливими базовими компонентами для середовища архітектури корпоративних інформаційних технологій (IT). Вони несуть основну відповідальність за зберігання та керування ідентифікаційними даними та членством у пов’язаній групі (ролі). Microsoft Active Directory (AD) містить структуроване сховище даних, яке зазвичай використовується організаціями для зберігання та керування об’єктами даних корпоративного каталогу, включаючи політики, користувачів, пристрої, облікові дані та інші мережеві ресурси. AD може бути привабливою мішенню для зловмисників, які шукають шляхи до мережі вашої організації, щоб отримати доступ до ваших систем і даних.

Служба Microsoft Active Directory (AD) — це структуроване сховище даних, яке зазвичай використовується організаціями для зберігання та керування об’єктами даних корпоративного каталогу. Основна одиниця безпеки в AD

називається «ліс». Ці ліси можна розділити на субодиниці, які називаються «доменами». Якщо організація зіткнеться з компрометацією будь-де в межах лісу, це може призвести до компрометації всього лісу. Тривала історія компрометацій AD демонструє, що потрібна більша безпека, що передбачає потенційно вищі операційні витрати та більше зусиль для запобігання більш значним і дорогим порушенням. Захист і посилення служби Microsoft AD має вирішальне значення для захисту корпоративної мережі.

До загального визнання AD, ідентифікаційні дані часто виключалися на основі окремої послуги. Це вимагало від користувачів авторизації для кожної служби. AD централізував цей досвід, забезпечивши систему єдиного входу (SSO) для багатьох користувачів; однак такий підхід може призвести до єдиного джерела компромісу. Якщо зловмисники можуть скомпрометувати облікові дані, включені в систему єдиного входу, вони мають можливість використовувати єдиний набір облікових даних для розблокування інших систем або сховищ даних. Були численні приклади компрометації системи єдиного входу з використанням різних типів атак, як-от атаки на крадіжку облікових даних системи єдиного входу. Компрометація системи єдиного входу є тенденцією, яка, як очікується, продовжиться.

Microsoft AD можна використовувати для керування доступом до багатьох IT-ресурсів організації через роль або членство в групах, наприклад до мережевої інфраструктури, служб електронної пошти, служб інфраструктури відкритих ключів (PKI), бездротових служб.

Active Directory пропонує багатий набір служб та функцій, у тому числі:

Полегшений протокол доступу до каталогів (LDAP): AD підтримує протокол LDAP, що забезпечує просту інтеграцію з різними програмами та службами, яким потрібний доступ до каталогу.

Єдиний вхід (SSO): Користувачі можуть отримати доступ до кількох ресурсів у мережі, використовуючи один набір облікових даних, що підвищує продуктивність та знижує необхідність багаторазового входу до системи.

Редактор локальної групової політики: адміністратори можуть визначати та застосовувати політики на груповій або індивідуальній основі, що дозволяє

централізовано керувати налаштуваннями безпеки, розгортанням програмного забезпечення та іншими конфігураціями.

Безпека та контроль доступу: Active Directory включає надійні механізми безпеки, такі як протоколи автентифікації, шифрування та списки керування доступом (ACL), для захисту мережевих ресурсів та забезпечення доступу до них лише авторизованим користувачам.

Копіювання: AD підтримує реплікацію між контролерами домену, гарантуючи синхронізацію змін, внесених до каталогу, у кількох місцях, підвищуючи стійкість до відмов і доступність.

Довірчі відносини: Active Directory дозволяє встановлювати довірчі відносини між доменами або лісами, полегшуючи спільну роботу та спільне використання ресурсів через різні адміністративні кордони.

Важливість AD в управлінні мережею

Active Directory (AD) грає вирішальну роль управлінні мережею, пропонуючи організаціям безліч переваг і переваг. Ось кілька ключових причин, чому AD необхідний у сфері управління мережею:

Централізоване управління користувачами: AD надає централізовану платформу для керування обліковими записами користувачів, паролями та дозволами. Це спрощує адміністрування користувачів, дозволяючи адміністраторам створювати, змінювати та видаляти облікові записи користувачів з одного місця. Це забезпечує одноманітний контроль доступу та зручність роботи користувачів у мережі, заощаджуючи час та скорочуючи адміністративні витрати.

Ефективне управління ресурсами: За допомогою Active Directory адміністратори можуть легко організовувати мережні ресурси, такі як комп'ютери, принтери та спільні папки та керувати ними. Ієрархічна структура AD забезпечує ефективний розподіл ресурсів та спрощує контроль доступу, дозволяючи користувачам швидко знаходити та використовувати мережні ресурси.

Підвищена безпека: AD підвищує безпеку мережі за рахунок застосування суворих протоколів автентифікації та механізмів контролю доступу. Він підтримує багатофакторну автентифікацію, політики паролів та політики блокування

облікових записів, які допомагають захистити від несанкціонованого доступу та витоку даних. Active Directory також забезпечує детальний контроль над дозволами на ресурси, гарантуючи, що лише авторизовані користувачі матимуть відповідні права доступу.

Можливість єдиного входу (SSO): Active Directory забезпечує єдиний вхід, дозволяючи користувачам увійти в систему один раз і без перешкод отримати доступ до безлічі ресурсів і служб. Це не тільки покращує взаємодію з користувачем, а й знижує навантаження на керування кількома паролями та обліковими даними.

Управління груповими політиками: AD включає групову політику - потужну функцію, яка дозволяє адміністраторам визначати та застосовувати політики безпеки, конфігурації та розгортання програмного забезпечення в мережі. Це забезпечує узгодженість налаштувань та стандартів у всій організації, спрощуючи управління та знижуючи ризик неправильної конфігурації.

Масштабованість та гнучкість: Active Directory призначений для роботи з великомасштабними мережами з тисячами користувачів та ресурсів. Він підтримує ієрархію доменів, дозволяючи організаціям розширювати свою мережеву інфраструктуру в міру потреби, зберігаючи при цьому централізоване управління та контроль.

Співробітництво та інтеграція: AD полегшує спільну роботу, дозволяючи встановлювати довірчі стосунки між доменами чи лісами. Це дозволяє користувачам із різних доменів отримувати доступ до спільних ресурсів та безперешкодно співпрацювати над проектами. Більш того, AD підтримує інтеграцію з іншими технологіями та програмами Microsoft, що спрощує впровадження та керування широким спектром мережевих служб.

Відмовостійкість та висока доступність: Active Directory використовує механізми реплікації, які гарантують синхронізацію змін, внесених до каталогу, на кількох контролерах домену. Це забезпечує стійкість до відмов і високу доступність, оскільки користувачі можуть продовжувати отримувати доступ до мережевих ресурсів, навіть якщо один контролер домену стає недоступним.

Active Directory відіграє життєво важливу роль в управлінні мережею, спрощуючи адміністрування користувачів, підвищуючи безпеку, оптимізуючи управління ресурсами та сприяючи спільній роботі. Його комплексні функції та можливості роблять його незамінним інструментом для організацій будь-якого розміру, дозволяючи IT-фахівцям ефективно управляти та захищати свою мережеву інфраструктуру [6].

2.2. Компоненти та архітектура розгортання Active Directory

Ключові компоненти Active Directory

Домени та контролери домену

Домени — це логічні контейнери, які становлять адміністративні кордони всередині мережі. Вони надають можливість організовувати мережеві ресурси, включаючи облікові записи користувачів, комп'ютери та політики безпеки та керувати ними. Кожен домен має принаймні один контролер домену, який є сервером, відповідальним за автентифікацію користувачів, збереження інформації каталогу та дотримання політик безпеки в домені.

Ліси та дерева

Ліс - це сукупність одного або декількох доменів, що мають загальну схему, конфігурацію та глобальний каталог. Він є найвищим рівнем організації в Active Directory. Домени всередині лісу з'єднані в ієрархічну структуру, відому дерево. Ліс забезпечує основу для встановлення довірчих відносин, спільного використання ресурсів та реалізації політик у масштабі всього підприємства.

Організаційні підрозділи (OU)

Організаційні одиниці – це контейнери всередині доменів, які дозволяють здійснювати подальшу логічну організацію мережевих ресурсів. Підрозділи надають можливість групувати об'єкти, такі як користувачі, комп'ютери та групи, та керувати ними на основі певних критеріїв, таких як відділ, місцезнаходження чи посадові функції. Вони використовуються для делегування адміністративного

контролю та застосування групових політик до певних підмножин мережевих об'єктів.

Довірчі відносини

Відносини довіри встановлюють рівень довіри між доменами або лісами, що дозволяє користувачам в одному домені отримувати доступ до ресурсів в іншому домені. Трасти можуть бути односторонніми або двосторонніми і можуть бути транзитивними, тобто можуть виходити за межі двох безпосередньо пов'язаних доменів. Відносини довіри забезпечують спільну роботу, спільне використання ресурсів та автентифікацію через різні адміністративні кордони.

Ці ключові компоненти працюють разом, створюючи ієрархічну та організовану структуру в Active Directory, забезпечуючи ефективне управління, безпечну автентифікацію та ефективне делегування адміністративних завдань

Розуміння цих компонентів має вирішальне значення для проектування та реалізації інфраструктури Active Directory, що відповідає вимогам управління мережею організації.

Структура Active Directory

Active Directory має ієрархічну структуру, де домени утворюють основні одиниці. Домени організовані в ієрархічну деревоподібну структуру, відому як дерево доменів. Декілька дерев доменів можна об'єднати в ліс.

Ліс є контейнером верхнього рівня, який охоплює всі домени і визначає межі для спільного використання ресурсів і встановлення довірчих відносин.

Кожен домен Active Directory має унікальне ім'я, що відповідає певній угоді про імена. Доменні імена зазвичай базуються на ієрархії DNS (системи доменних імен) в Інтернеті та використовують формат ім'я_домена.tld (наприклад, company.com). Угоди про імена повинні відповідати правилам і рекомендаціям, встановленим організацією, та враховувати такі фактори, як брендинг, місцезнаходження та підрозділи.

Функціональні рівні визначають доступні функції та можливості у лісі чи домені. Існує два типи функціональних рівнів: функціональний рівень лісу та функціональний рівень домену.

Функціональний рівень лісу**:** Функціональний рівень лісу є загальним набором функцій, доступних у лісі. Він визначає сумісність та доступність розширених функцій, таких як довіра між лісами, перейменування домену та впровадження нових версій операційних систем Windows Server. Функціональний рівень лісу встановлюється в корені лісу та впливає на всі домени у лісі.

Функціональний рівень домену**:** Функціональний рівень домену є набір функцій, доступних в окремому домені. Він визначає доступність функцій, специфічних для домену, таких як вкладення груп, покращення реплікації та механізми автентифікації. Функціональний рівень домену може бути різним для кожного домену в лісі і зазвичай встановлюється на основі найстарішої версії операційної системи контролера домену в цьому домені.

Вибір функціональних рівнів лісу та домену повинен відповідати вимогам організації та потребам у конкретних функціях чи сумісності зі старими системами. Важливо ретельно планувати та враховувати вплив оновлень або змін функціонального рівня, щоб забезпечити сумісність та мінімізувати збої в Active Directory.

Служби Active Directory

Аутентифікація та безпека

Active Directory служить службою автентифікації та безпеки, перевіряючи особистість користувачів та надаючи їм доступ до мережевих ресурсів. Він підтримує різні протоколи автентифікації, такі як Kerberos та NTLM, забезпечуючи безпечну автентифікацію та запобігаючи несанкціонованому доступу. AD також дозволяє реалізувати політики безпеки, політики паролів та політики блокування облікових записів для підвищення безпеки мережі.

Керування користувачами та групами

AD пропонує надійні можливості керування користувачами та групами. Він дозволяє створювати, змінювати та видаляти облікові записи користувачів, дозволяючи адміністраторам контролювати права доступу та дозволу користувачів. Користувачі можуть бути організовані до груп, що спрощує управління контролем доступу та дозволами на ресурси. AD також підтримує

створення вкладених груп та керування доступом на основі ролей (RBAC), забезпечуючи гнучкість керування користувачами.

Управління ресурсами

Active Directory забезпечує централізоване управління ресурсами, що дозволяє адміністраторам ефективно керувати мережевими ресурсами, такими як комп'ютери, принтери, спільні папки та мережні пристрої. Він забезпечує організацію та категоризацію ресурсів, спрощуючи їх пошук та контроль доступу до них. Адміністратори можуть делегувати завдання управління ресурсами конкретним користувачам чи групам, оптимізуючи адміністрування ресурсів.

Управління політикою

AD включає групову політику - потужну функцію, яка дозволяє адміністраторам визначати та застосовувати політики по всій мережі. Групова політика забезпечує централізоване керування параметрами безпеки, встановленням програмного забезпечення та конфігураціями. Це дозволяє послідовно застосовувати політики до користувачів, комп'ютерів або груп, забезпечуючи відповідність вимогам, стандартизацію та ефективне керування мережними ресурсами.

Ці служби Active Directory відіграють важливу роль в управлінні мережею, забезпечуючи комплексну основу для аутентифікації, управління користувачами та групами, адміністрування ресурсів та застосування політик. Використовуючи ці послуги, організації можуть ефективно керувати своєю мережевою інфраструктурою, підвищувати безпеку, оптимізувати операції та підтримувати узгоджене та контрольоване середовище.

Інтеграція з Active Directory

Інтеграція з операційними системами Windows Server

Active Directory тісно інтегровано з операційними системами Windows Server. Це основний компонент Windows Server, який забезпечує базову інфраструктуру для автентифікації користувачів, управління ресурсами та застосування політик. AD легко інтегрується зі службами Windows Server, такими як DNS (система

доменних імен), DHCP (протокол динамічної конфігурації хоста) та файлові служби, забезпечуючи уніфіковане та інтегроване керування мережею.

Інтеграція з іншими службами Microsoft

Active Directory інтегрується з рядом служб Microsoft, розширюючи їхню функціональність і забезпечуючи зручність роботи з користувачем. Наприклад:

Сервер обміну: Інтеграція AD з Exchange Server дозволяє використовувати уніфіковані служби електронної пошти та спільної роботи. Облікові записи електронної пошти та дозволи користувачів керуються через Active Directory, що спрощує керування поштовими скриньками та дозволяє використовувати єдиний вхід (SSO) для доступу до ресурсів Exchange.

SharePoint**:** інтеграція Active Directory з SharePoint забезпечує безперешкодну автентифікацію користувачів та контроль доступу до сайтів та контенту SharePoint. Користувачі можуть використовувати облікові дані AD для входу до SharePoint, а SharePoint може використовувати групи безпеки AD для керування дозволами.

Microsoft Команди: інтеграція Active Directory з Microsoft Teams забезпечує безпечну автентифікацію користувачів та керування ними. Користувачі можуть використовувати свої облікові дані AD для доступу до Teams, а групи AD можна використовувати для керування доступом до каналів та ресурсів Teams

Інтеграція із середовищами сторонніх виробників

Хоча Active Directory в першу чергу є технологією Microsoft, вона також підтримує інтеграцію із середовищем сторонніх виробників за допомогою стандартних протоколів та технологій:

LDAP (полегшений протокол доступу до каталогів):AD підтримує LDAP, що забезпечує інтеграцію з широким спектром додатків та служб, які використовують LDAP для доступу до каталогів та автентифікації користувачів.

Єдиний вхід (SSO)**:** Можливості єдиного входу Active Directory можна використовувати в середовищах, відмінних від Microsoft, дозволяючи користувачам використовувати облікові дані AD для доступу до різних програм і служб, незалежно від базової технології.

Стандарти безпеки: Active Directory може інтегруватися з протоколами встановлення автентифікації, такими як Security Assertion Markup Language (SAML) та OpenID Connect, що забезпечує безпечну та просту аутентифікацію користувачів у різних середовищах.

Active Directory дозволяє організаціям використовувати можливості централізованого керування користувачами, автентифікації та безпеки у всій мережевій екосистемі, надаючи можливості інтеграції з Windows Server, службами Microsoft та середовищами, що не належать Microsoft. Така інтеграція сприяє сумісності, спрощує адміністрування та підвищує продуктивність та безпеку користувачів [7].

Каталог Microsoft AD можна розгортати в різних архітектурах, від суто локальних (або в безпосередньо керованому центрі обробки даних) до гібридної хмари та повних рішень у межах хмарних платформ.

AD локально

Спочатку AD призначався для керування традиційною локальною інфраструктурою та програмами. Цей варіант розгортання дозволяє організації повністю керувати службою каталогів від кінця до кінця.

Хмара AD (локальна, самокерована в хмарі)

Розгортання та міграцію гібридної хмари слід ретельно розглядати. Під час включення будь-якої функції хмарного сервісу мається на увазі використання гіпервізора. Це може докорінно змінити стан безпеки в порівнянні з локальним розгортанням, оскільки вводить інші проблеми безпеки та мережеві функції, які необхідно враховувати.

AD все ще можна використовувати для можливостей ICAM для хмари за допомогою існуючих локальних рішень. Зазвичай це називають «гібридним» за своєю природою, оскільки певні елементи контролюються та працюють локально, тоді як деякі елементи підключаються та потім синхронізуються зі службами каталогів CSP. У деяких розгортаннях конфігурації самого сервера AD залишаться незмінними, оскільки основна відмінність або зміна полягає у використанні платформи CSP «Інфраструктура як послуга» (IaaS). У такому типі розгортання

контроль над певними фізичними та мережевими аспектами змінюватиметься відповідно до моделі спільної відповідальності в хмарних обчисленнях.

Існує два основних підходи до гібридної архітектури:

Локальні (у центрі обробки даних споживача): Контролери домену об’єднані з хмарними службами через локальну ADFS.

Розширено на території приміщення (самокероване): Контролери домену як локальні, так і розгорнуті на платформі IaaS CSP.

Використовуючи той самий ліс або довіру до лісу, домени, розгорнуті таким чином, є технічно гібридними, оскільки вони синхронізуються та об’єднуються локально, імовірно також за допомогою локальної ADFS, а також об’єднання.

У цьому випадку досі немає прямої або повної синхронізації ідентифікаційних даних із постачальником ідентифікаційної інформації (IdP), щоб створити власну хмарну ідентифікаційну інформацію.

Хоча цей тип архітектури можливий, він не є рекомендованим довгостроковим підходом, оскільки існують фундаментальні зміни в системі безпеки. Цей підхід, як правило, слід розглядати як перехідну або міграційну стратегію.

Служби каталогів у хмарі

Як автентифікацію, так і авторизацію в хмарному середовищі можна проводити без локальних можливостей. Автентифікація лише в хмарі стосується процесів керування ідентифікацією та доступом, які здійснюються виключно через рішення CSP ICAM або стороннє рішення для керування ідентифікацією. Ця опція дозволяє організації створювати ідентифікаційні дані користувачів, права та контроль доступу та керувати ними за допомогою сторонньої програми без необхідності створювати, володіти або керувати інфраструктурою на місці. Рішення автентифікації лише в хмарі можна використовувати для керування доступом як до загальнодоступних хмарних робочих навантажень, так і до приватно керованих локальних програм, таких як Azure AD Domain Services. Кілька протоколів автентифікації керують тим, як створюються, розповсюджуються та керуються ідентифікатори, права та авторизації. Організація повинна провести

оцінку ризиків, щоб визначити потенційні ризики для бізнес-процесів і даних, перш ніж прийняти цей варіант.

Розглядаючи розгортання нової мережі або створення стратегії мережевої архітектури для організації, важливо зазначити, що цей підхід, а також гібридні варіанти, згадані раніше, все ще дійсні, але вимагатимуть розгляду капітальних витрат і поточних операційних витрат. для кожного відповідно. У разі використання послуги CSP або IdP споживач дозволяє формувати та використовувати всі облікові дані та ідентифікаційні дані користувача в рамках цих послуг. Це має переваги, оскільки деякі аспекти виправлення та оновлення рішення ICAM проводяться CSP як частина передплати організації[8].

2.3. Переваги використання Active Directory в організаціях

Основною перевагою Active Directory є його здатність централізувати керування користувачами та доступ до мережевих ресурсів.

Active Directory централізує керування наступним:

— Централізоване управління обліковими записами користувачів

— Централізоване управління дозволами

— Централізоване керування параметрами політики

Централізоване керування обліковими записами користувачів

Active Directory надає централізовану платформу для керування мережевими ресурсами. Він спрощує адміністрування мережі з допомогою об'єднання облікових записів користувачів, об'єктів комп'ютерів та інших мережевих ресурсів на єдину базу даних каталогів. Такий централізований підхід спрощує такі завдання, як підготовка користувачів, управління паролями та розподіл ресурсів, скорочуючи адміністративні витрати та забезпечуючи однакові методи управління у всій мережі.

Наприклад, в Active Directory Pro працює 100 співробітників, і всім їм потрібна можливість доступу до мережі. Адміністратор використовуватиме

користувачів Active Directory і комп’ютерну консоль і створюватиме всі облікові записи в одному центральному місці.

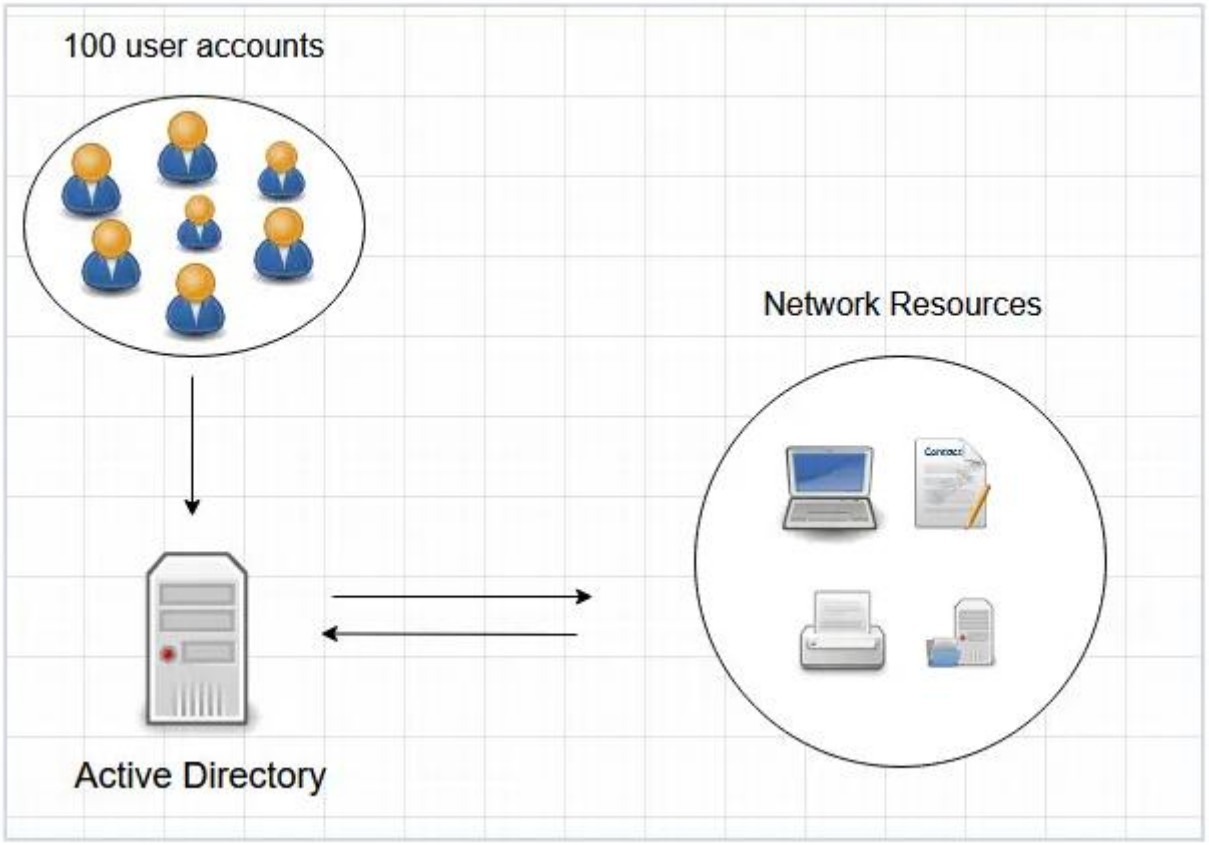

Рис.2.1. Керування створенням облікових записів користувачів

Тепер співробітники можуть увійти в комп’ютер і отримати доступ до всіх ресурсів, до яких вони мають доступ.

За відсутності Active Directory доведеться входити в кожен ресурс і створювати обліковий запис. Керувати цим було б кошмаром, і це зайняло б багато часу.

Підвищена безпека та контроль доступу

Active Directory посилює безпеку мережі за рахунок застосування надійних механізмів автентифікації та політик контролю доступу. Він підтримує багатофакторну аутентифікацію, політику надійних паролів та політику блокування облікових записів, захищаючи від несанкціонованого доступу.

Функції детального контролю доступу AD дозволяють адміністраторам призначати детальні дозволи користувачам та групам, гарантуючи, що користувачі матимуть доступ лише до тих ресурсів, які їм необхідні.

Спрощене керування користувачами та ресурсами

Active Directory спрощує управління користувачами та ресурсами завдяки своїй організаційній структурі та можливостям управління. Адміністратори можуть організовувати користувачів, комп'ютери та інші ресурси до логічних одиниць, таких як домени, організаційні одиниці (OU) та групи.

Така організація спрощує застосування політик, делегування адміністративних завдань та управління дозволами на доступ. Крім того, AD пропонує такі функції, як вкладення груп, управління груповими політиками та масове управління користувачами, що полегшує загальні адміністративні завдання.

Наприклад, є кілька користувачів, яким потрібен доступ до облікових ресурсів (сервер, файл контракту, спільний файл). Щоб легко надати доступ до всіх цих ресурсів, потрібно додати користувачів до групи безпеки Active Directory, яка має дозволи на ці ресурси.

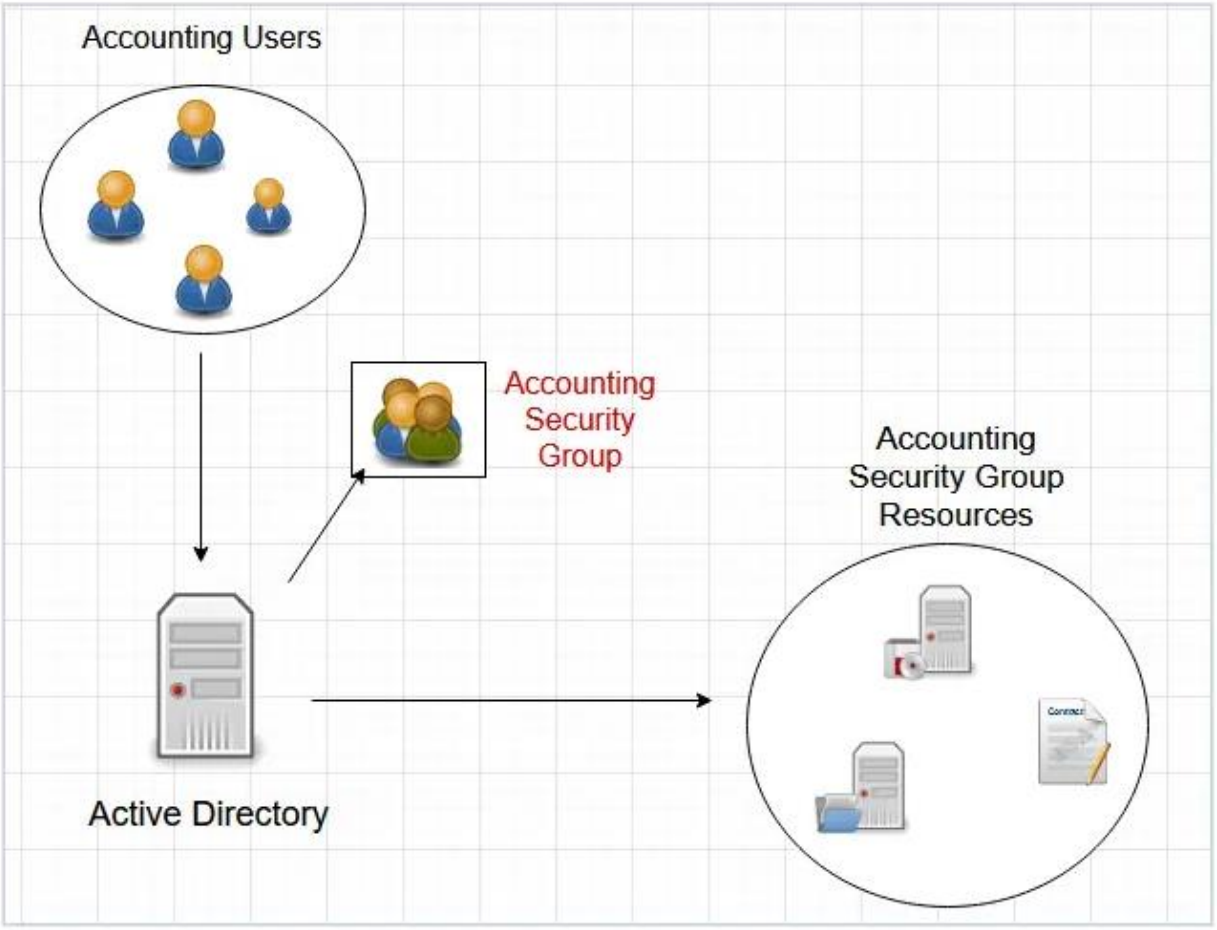

Рис.2.2. Керування доступу до ресурсів

Використовуючи групи безпеки Active Directory, можна легко надавати та видаляти дозволи. Коли працівник залишає групу або потребує видалення дозволів, ви просто видаляєте обліковий запис із групи.

Централізоване керування параметрами політики

Групові політики дозволяють адміністраторам визначати та застосовувати певні параметри та конфігурації в мережі. Адміністратори використовують управління груповою політикою для створення об'єктів групової політики (GPO), які застосовують параметри до користувачів та комп'ютерів, та управління ними. Ці політики можуть контролювати параметри безпеки, встановлення програмного забезпечення, зіставлення дисків та інші конфігурації.

Наприклад, якщо потрібно, щоб усі користувачі змінювали свої паролі кожні 60 днів, можна налаштувати політику паролів, яка застосовуватиметься до всіх

користувачів. Якщо необхідно застосувати параметри живлення до всіх комп'ютерів, це можна зробити за допомогою групової політики.

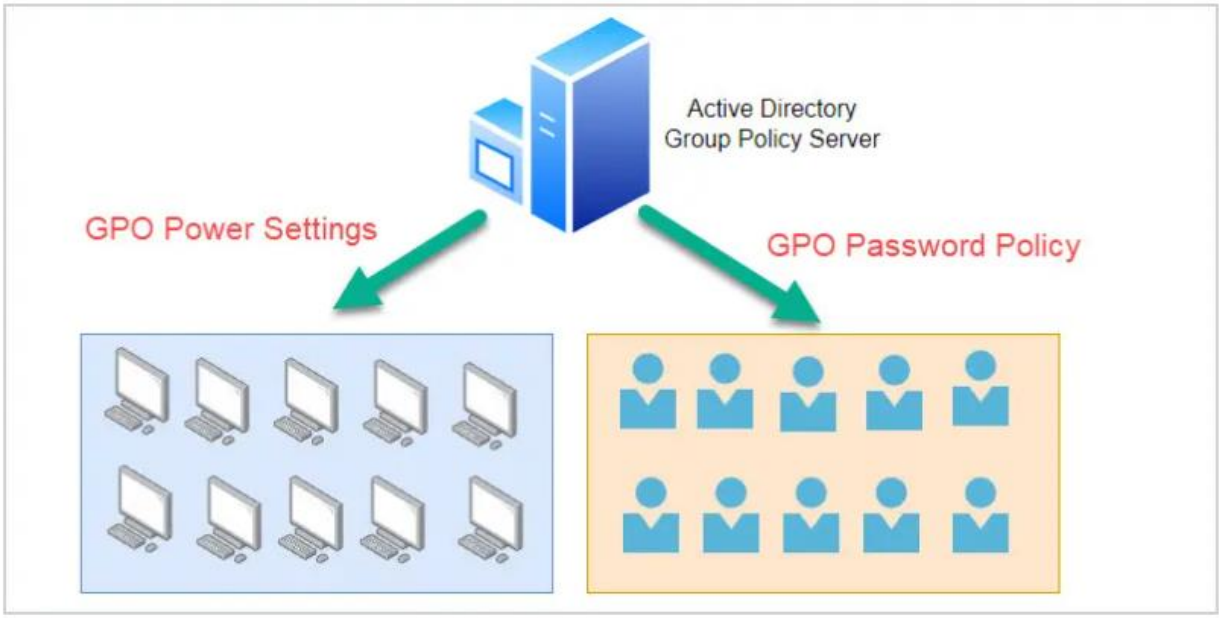

Рис.2.3. Керування груповими політиками

За відсутності Active Directory або групової політики потрібно буде налаштувати параметри політики на кожному комп'ютері. Це було б неможливо впоратися у великих середовищах. Організації, які на 100% працюють у хмарі, використовують Microsoft Intune для керування параметрами політики. Intune також можна використовувати в гібридних середовищах.

Масштабованість та гнучкість

Active Directory призначений для масштабування від малого бізнесу до великих підприємств, пристосовуючись до мережевих інфраструктур. Він підтримує ієрархічні структури доменів, дозволяючи додавати нові домени чи ліси в міру розширення організації. Гнучка архітектура AD дозволяє додавати додаткові контролери домену, забезпечуючи стійкість до відмов і високу доступність.

Більше того, Active Directory інтегрується з різними службами Microsoft та сторонніх виробників, що дозволяє організаціям адаптувати та інтегрувати її до своєї існуючої інфраструктури.

Переваги Active Directory включають централізоване керування мережею, підвищену безпеку, спрощене керування користувачами та ресурсами, а також

масштабованість. Ці переваги дозволяють організаціям ефективно керувати своїм мережевим середовищем, забезпечувати контроль доступу, підвищувати продуктивність та адаптуватися до мінливих потреб бізнесу. Active Directory служить наріжним каменем ефективного мережевого адміністрування, сприяючи оптимізації операцій та створенню безпечного обчислювального середовища.

Створення та керування користувачами та групами

Адміністратори створюють облікові записи користувачів у Active Directory та керують їх властивостями, включаючи ім'я користувача, пароль, адресу електронної пошти та членство у групах. Вони також можуть створювати групи безпеки та групи розсилки та керувати ними, що допомагає організовувати користувачів та контролювати доступ до ресурсів.

Контролери домену — це сервери, які відповідають за автентифікацію користувачів, збереження інформації каталогу та дотримання політик безпеки в домені Active Directory. Адміністратори виконують такі завдання, як додавання нових контролерів домену, виведення з експлуатації старих, моніторинг їхньої працездатності та стану реплікації, а також управління ролями та дозволами контролерів домену.

Усунення проблем з Active Directory

Усунення неполадок Active Directory включає виявлення та вирішення проблем, що впливають на автентифікацію користувачів, доступ до ресурсів або реплікацію каталогів. Це може включати усунення блокувань облікових записів, усунення збоїв реплікації, діагностику проблем DNS, дослідження проблем додатків групової політики та усунення помилок автентифікації.

Інші поширені завдання можуть включати управління довірчими відносинами між доменами або лісами, налаштування та управління сайтами та службами Active Directory для мережної топології, виконання резервного копіювання та відновлення баз даних Active Directory, моніторинг працездатності та продуктивності Active Directory, а також реалізацію заходів безпеки, таких як реалізація штрафних санкцій. детальні політики паролів або налаштування служб федерації Active Directory (ADFS) для єдиного входу.

Ці завдання потребують глибокого розуміння концепцій Active Directory, таких інструментів, як користувачі та комп'ютери Active Directory, консоль управління груповими політиками та центр адміністрування Active Directory, а також методи усунення несправностей для ефективного керування та обслуговування середовища Active Directory [9].

.

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ЗА ДОПОМОГОЮ ACTIVE DIRECTORY

3.1. Розроблення варіанта розгортання Active Directory для забезпечення кібербезпеки інформаційної системи організації

Active Directory використовується в бізнес-середовищі для спрощення керування користувачами, контролю доступу до даних і забезпечення дотримання політики безпеки компанії. Її основною функцією є забезпечення автентифікації та авторизації користувачів у мережі.

Автентифікація це процес, у якому Active Directory перевіряє облікові дані користувача (ім’я користувача та пароль). Облікові дані користувача зберігаються в базі даних Active Directory.

Авторизація це процес, який дозволяє або забороняє користувачеві робити щось, наприклад редагувати файл або отримати доступ до програми.

Основні компоненти Active Directory

Домени Active Directory, дерева та ліс

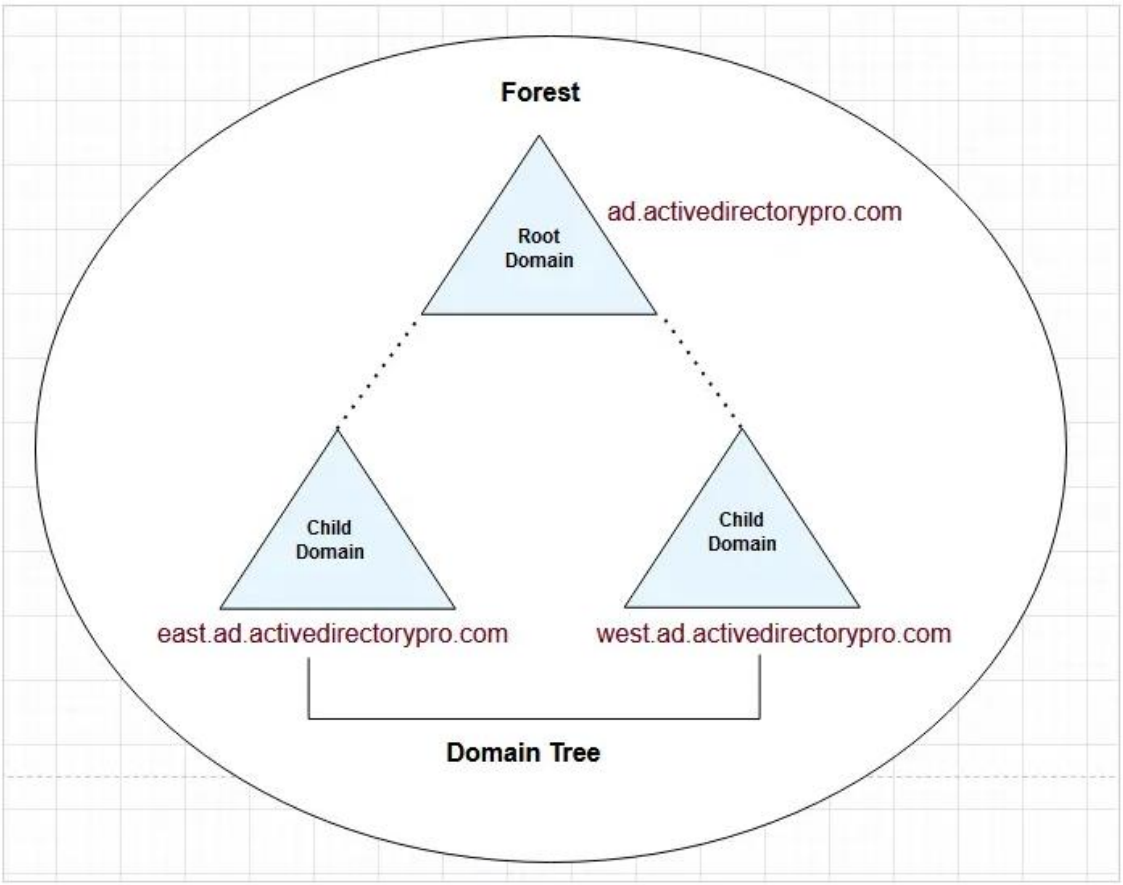

Рис.3.1. Основні компоненти AD [9]

Active Directory організовує ресурси в ієрархічну логічну структуру. Ця логічна структура допомагає організовувати об’єкти, визначати зв’язки та контролювати межі безпеки.

Ліс є контейнером верхнього рівня та є набором доменів Active Directory. Домени в лісі спільно використовують схему каталогу, конфігурацію каталогу та глобальний каталог. Домени в одному лісі автоматично мають двосторонню транзитивну довіру.

Кореневий домен Active Directory це логічна структура контейнерів і об’єктів в Active Directory. Домен містить такі компоненти:

— Ієрархічна структура для користувачів, груп, комп’ютерів та інших об’єктів.

— Служби безпеки, які забезпечують автентифікацію та авторизацію ресурсів у домені та інших доменах

— Політики, які застосовуються до користувачів і комп’ютерів

— Ім’я DNS для ідентифікації домену.

Дочірній домен це домен, який використовує той самий простір доменних імен, що й кореневий домен. Це домен із власною колекцією об’єктів.

Дерева це набір доменів, які з’єднані разом. Коли додається дочірній домен до батьківського, створюється так зване дерево доменів. Дерево доменів — це лише серія доменів, з’єднаних разом в ієрархічний спосіб, які використовують один простір імен DNS.

Схема - це набір правил, що визначає класи об'єктів і атрибутів, що містяться в каталозі.

Глобальний каталог (GC)

Глобальний каталог містить інформацію про кожен об'єкт у каталозі. Це дозволяє користувачам і адміністраторам знаходити інформацію каталогу незалежно від того, який домен у каталозі насправді містить дані. За замовчуванням перший контролер домену в домені позначається як сервер GC. Для підвищення продуктивності рекомендується мати принаймні один сервер GC для кожного сайту.

Служба реплікації

Служба реплікації синхронізувала базу даних Active Directory з іншими контролерами домену. Active Directory зазвичай розгортається з двома чи більше контролерами домену з причин надмірності. Коли створюється обліковий запис на одному контролері домену, він реплікується на інший. Якщо один контролер домену вийде з ладу, інший матиме копію бази даних.

Рис.3.2. Служба реплікації

Якщо на наведеній вище схемі користувача додано до DC1, його буде скопійовано до DC2 і навпаки.

Сайти та служби

Сайти Active Directory використовуються для об’єднання кількох контролерів домену в логічні контейнери, пов’язані з їх фізичним розташуванням. Сайти використовуються для оптимізації продуктивності Active Directory, якщо є кілька філій і контролерів домену.

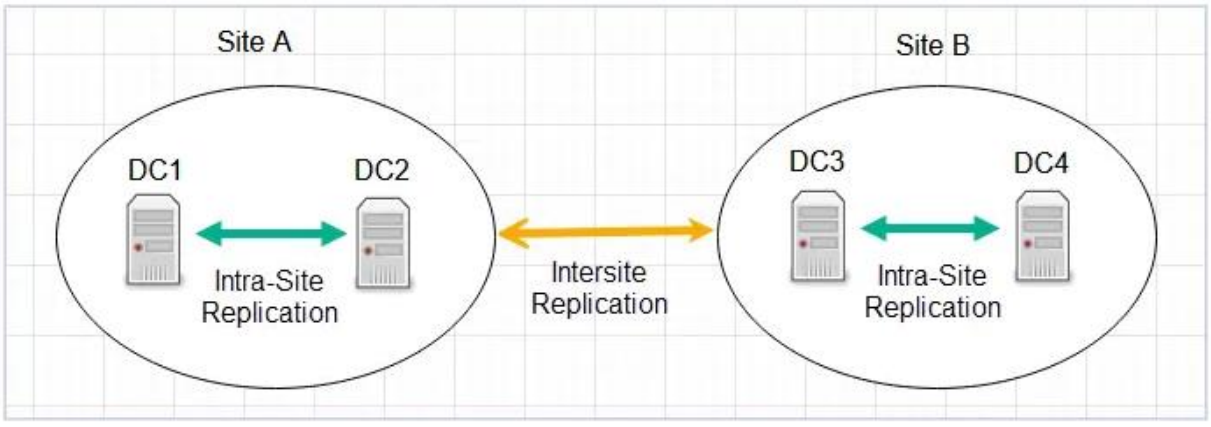

Рис.3.3. Контролери домену та реплікація між сайтами

У наведеному вище прикладі є два сайти, і кожен сайт має два контролери домену. Контролери домену на сайті A використовують реплікацію всередині сайту, щоб підтримувати синхронізацію всіх змін між DC1 і DC2. Сайт A та сайт B

використовують міжсайтову реплікацію, щоб гарантувати реплікацію змін із сайту A на сайт B і навпаки.

Kerberos

Kerberos — це протокол автентифікації, який використовується Active Directory для перевірки ідентичності користувача або хоста.

На рис. 3.4. зображено процес автентифікації, який відбувається у фоновому режимі.

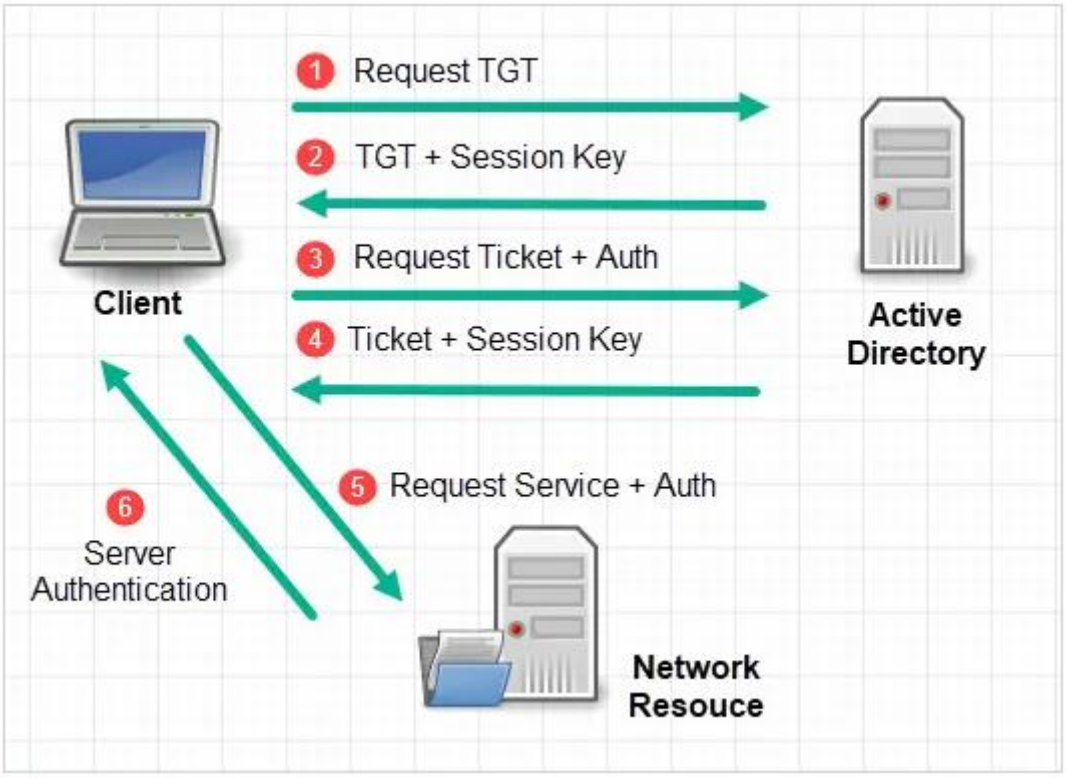

Рис.3.4. Процес автентифікації

1. Клієнт надсилає запит на сервер Active Directory.
2. Сервер відповідає TGT і ключ сеансу, який клієнт може використовувати для шифрування та автентифікації на сервері AD.
3. Клієнт надсилає запит на автентифікацію.
4. Сервер перевіряє запит і повертає службовий квиток.
5. Клієнт використовує квиток, отриманий від сервера AD, для запиту доступу до мережевого ресурсу.

6. Сервер розшифрує квиток і підтвердить запит.

Розглянемо процес розгортання нового домену для середовища Active Directory за допомогою Windows Server 2019. Це буде реалізовано шляхом встановлення відповідної ролі, а потім шляхом підвищення ролі сервера до головного контролера домену (DC). У той же час встановимо роль DNS для використання можливостей зон, інтегрованих в Active Directory.

По суті, процес виконується у два етапи: встановлення ролі Active Directory Domain Services та підвищення статусу сервера до головного контролера домену.

Встановлення ролі Active Directory Domain Services

Перш ніж приступити до виконання цього кроку, необхідно налаштувати на сервері статичну IP-адресу, а також змінити ім'я Windows Server відповідно до стандартів іменування компанії.

Потрібно відкрити керування сервером (Server Manager), натиснути Управління (Manage), а потім «Додати ролі та компоненти» (Add Roles and Features).

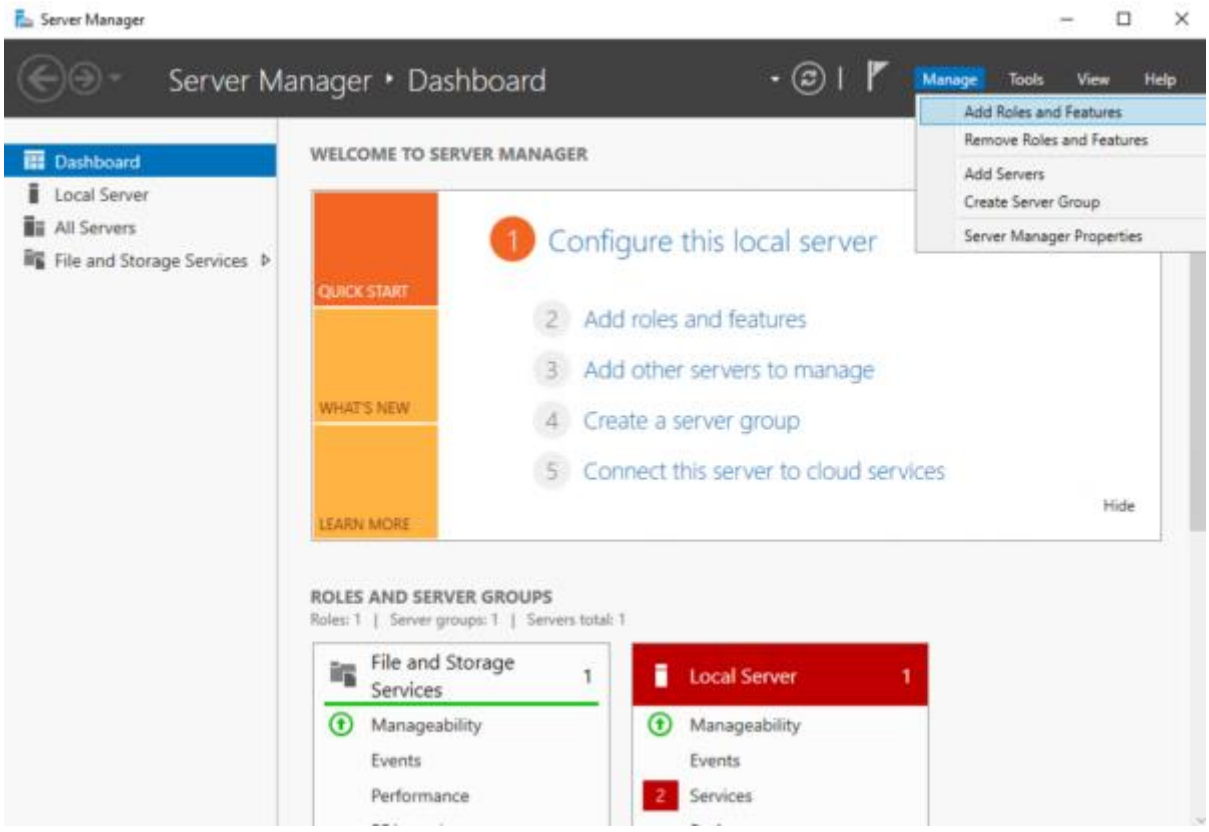

Рис.3.5. Менеджер керування сервером

Відразу після цього відкриється вікно майстра. У розділі "Тип установки" (Installation Type) потрібно вибрати установку на основі ролей сервера або на основі функції віртуальної інфраструктури.

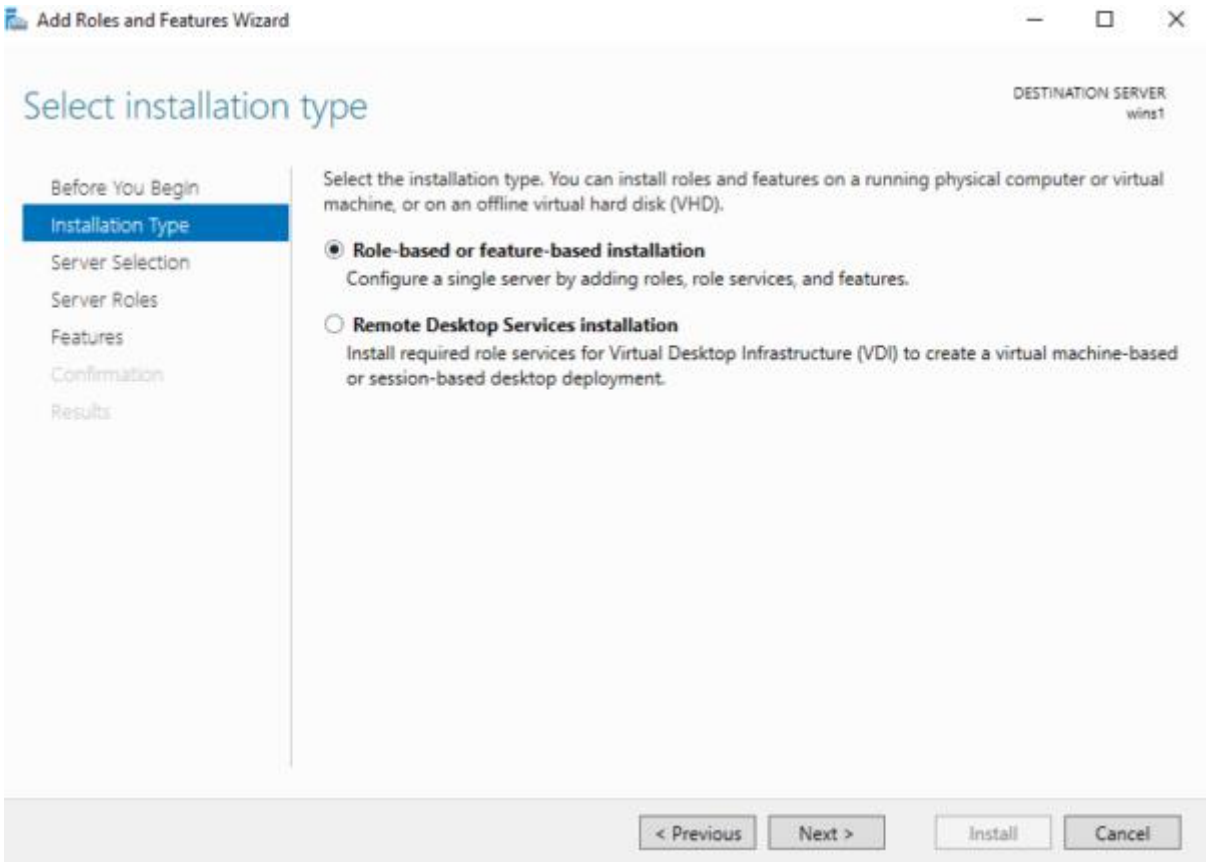

Рис.3.6. Вибір варіанту встановлення

У розділі "Ролі сервера" (Server Roles) необхідно вибрати Доменні служби Active Directory (Active Directory Domain Services). Після цього буде запропоновано додати додаткові функції.

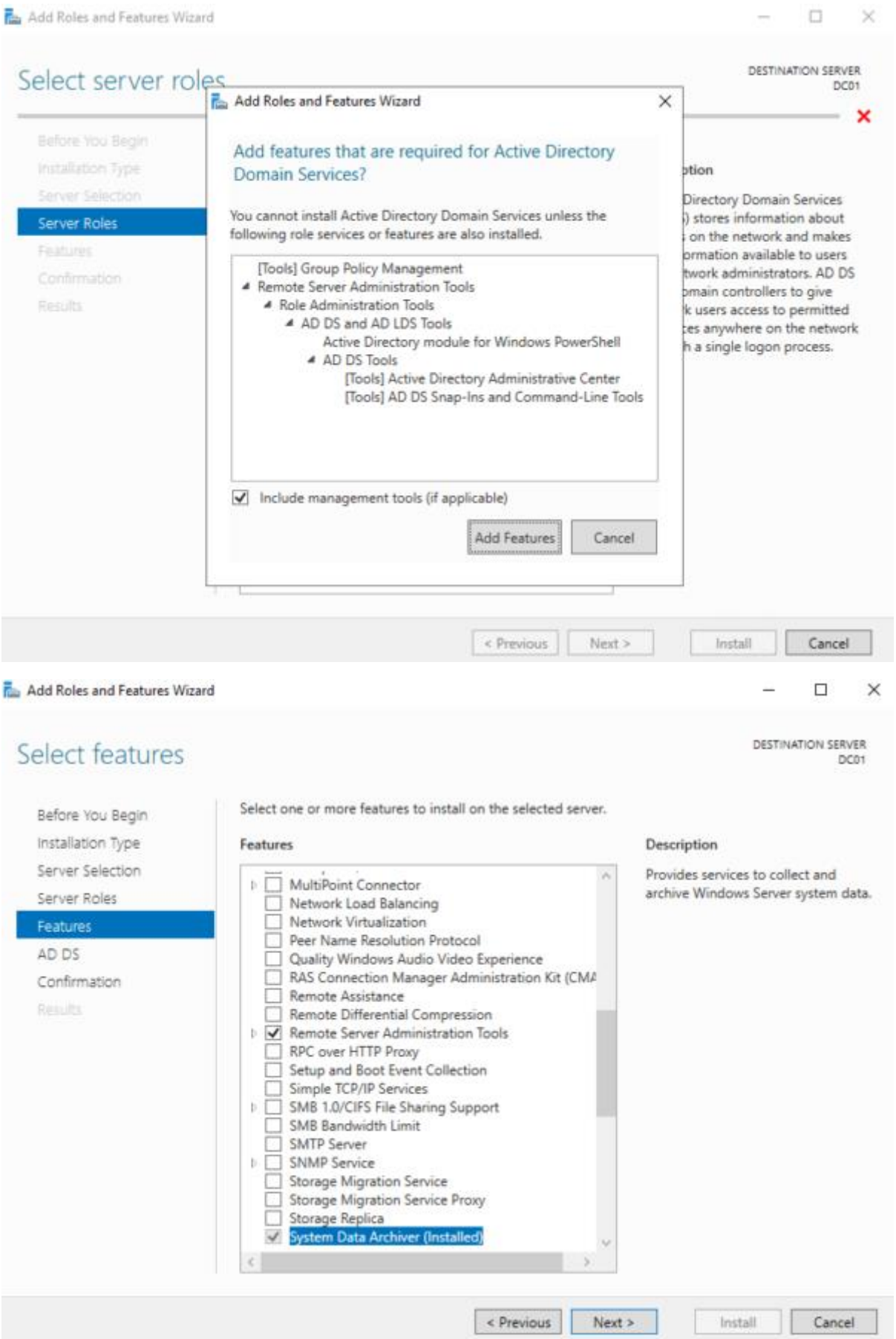

Рис.3.7. Додавання ролей та функцій

У розділі AD DS відображається інформація про AD DS. Далі, у розділі «Підтвердження» (“Confirmation”) потрібно натиснути кнопку Install, щоб перейти до встановлення ролі.

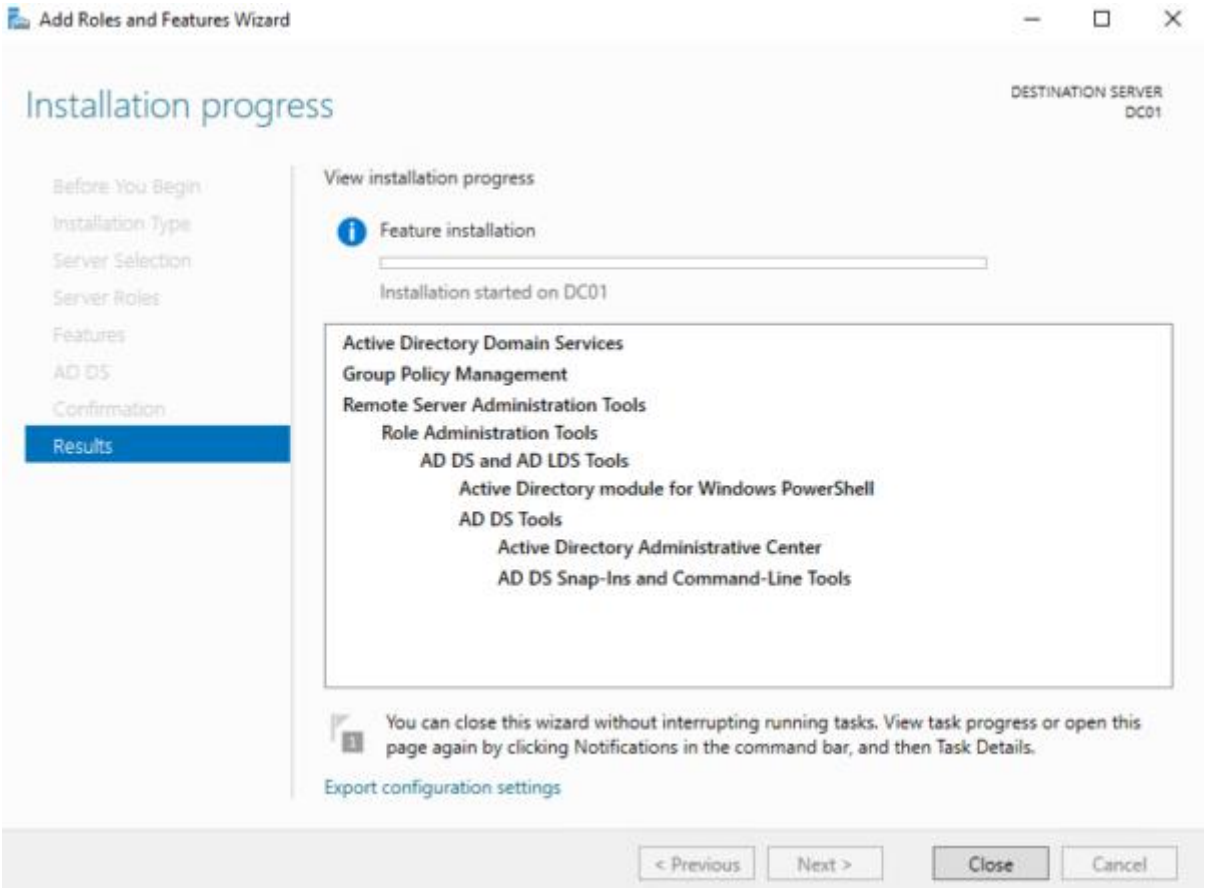

Рис.3.8. Інформація про доменні служби Active Directory

Після завершення встановлення ролі, якщо не закривати вікно, буде запропоновано підвищити сервер до контролера домену (DC). Посилання буде виділено синім текстом.

В якості альтернативи можна відкрити те саме вікно через сервер менеджер, як показано на рис. 3.9.

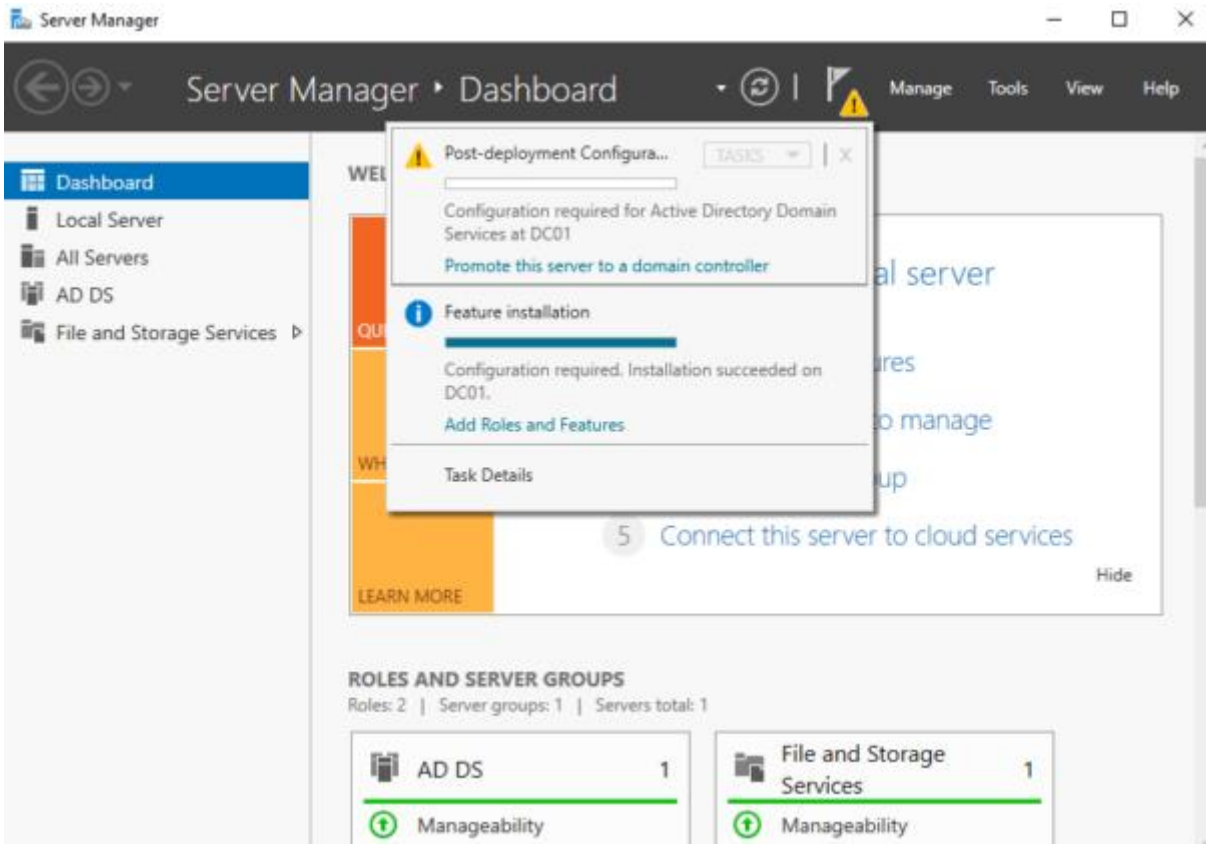

Рис.3.9. Підвищення ролі сервера

У розділі "Конфігурація розгортання" (Deployment Configuration), обирається "Додати новий ліс"-"Add a new forest" для створення та початку конфігурації нового лісу в Active Directory.

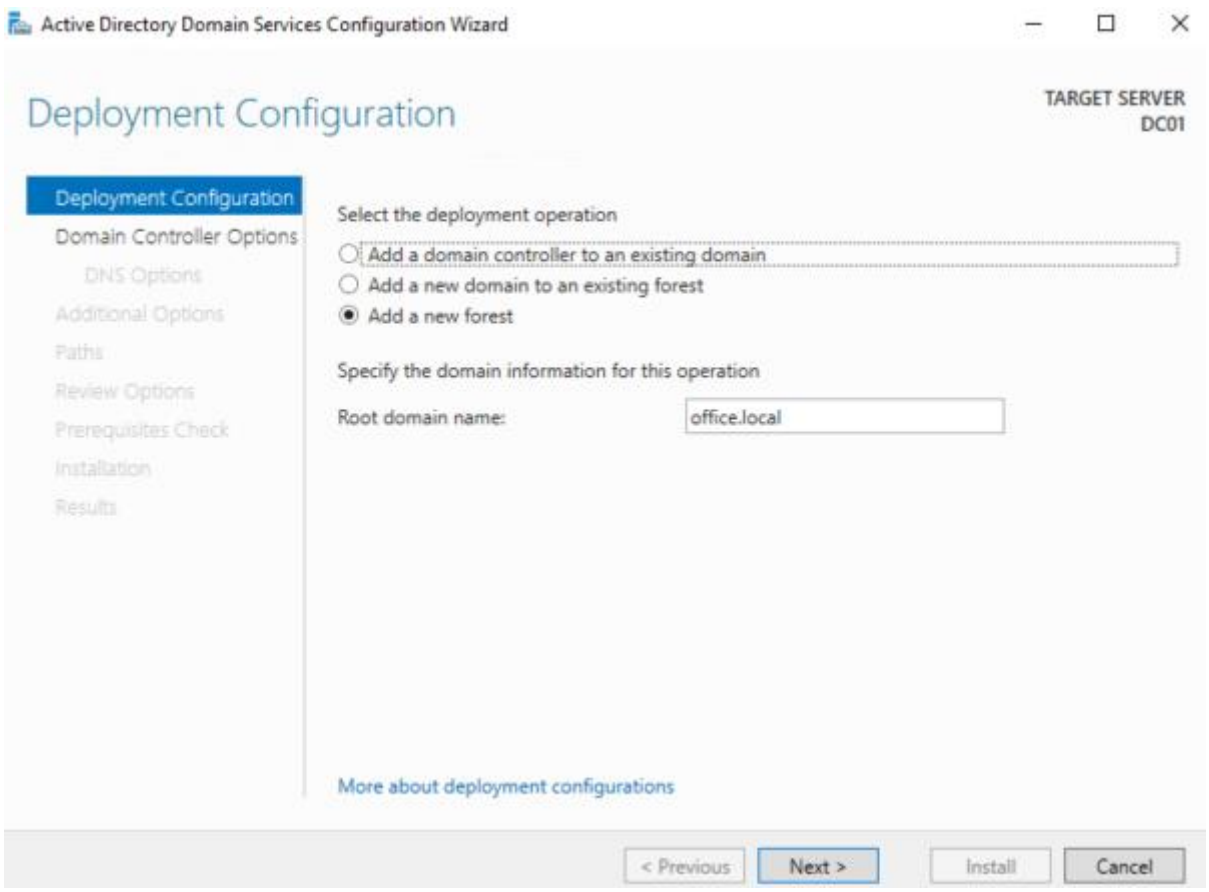

Рис.3.10. Конфігурація розгортання

У розділі «Установки контролера домену» (Domain Controller Options) обирається функціональний рівень лісу та домену. Якщо це перший ліс на Windows Server 2016, залишається значення за замовчуванням. В іншому випадку, якщо в організації є інші контролери домену, слід дізнатися про їх функціональний рівень, перш ніж приступати до необхідних дій.

Наступним кроком потрібно налаштувати опцію сервера доменних імен (DNS), щоб також встановити роль DNS на тому ж сервері, якщо не було зроблено цього раніше, а також ввести (DSRM) Directory Services Restore Mode.

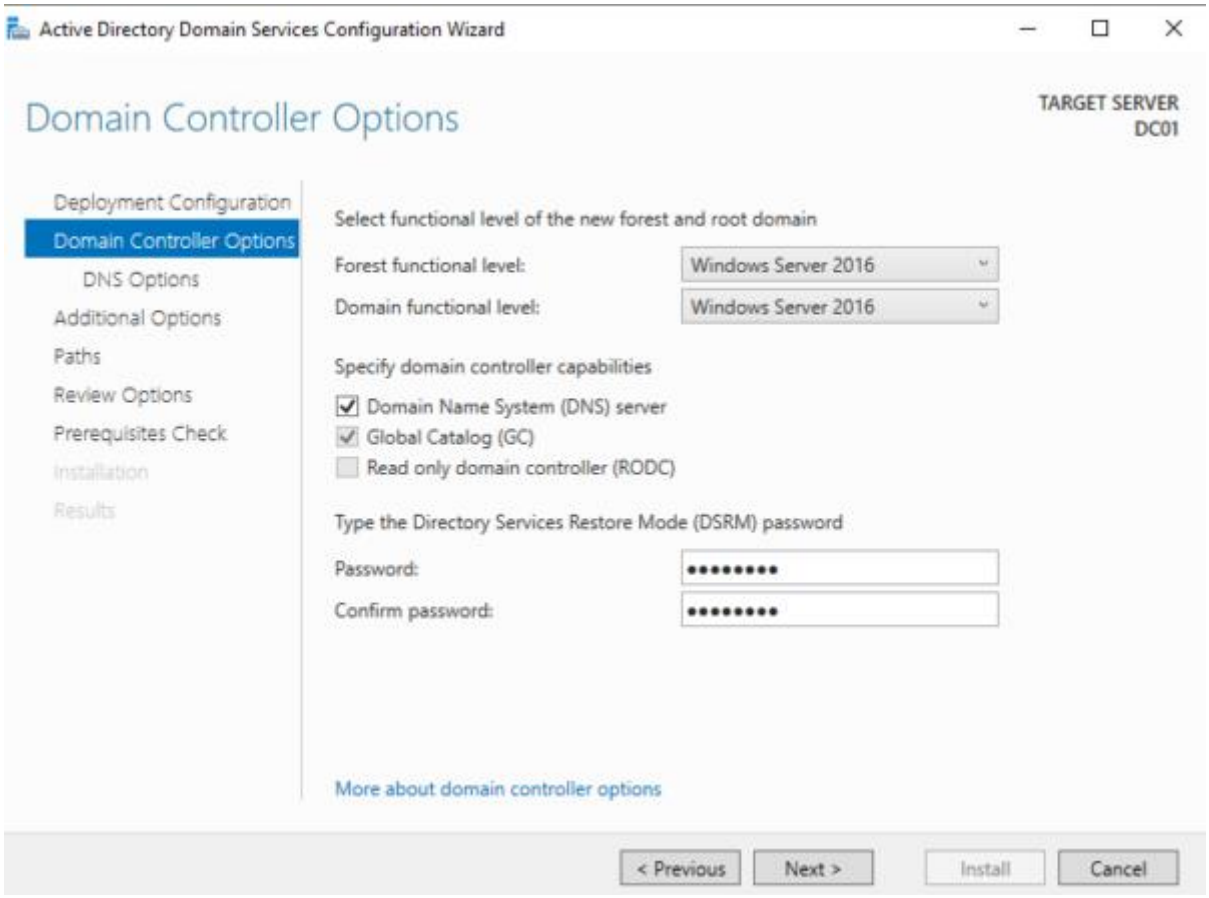

Рис.3.11. Параметри домену

У розділі «Paths» обирається, де на сервері будуть розміщені папки NTDS, SYSVOL та LOG. У цьому випадку залишимо значення за промовчанням, можна вибрати інший диск залежно від налаштувань. У розділі "Переглянути параметри" (Review Options) можна побачити зведення вибраних параметрів.

У розділі «Перевірка попередніх вимог» Prerequisites Check будуть перевірені попередні умови. Тут, якщо виникне хоча б одна помилка, не можна продовжити і потрібно буде її виправити. В іншому випадку, якщо відображаються лише попереджувальні повідомлення (які є найбільш поширеними), але перевірка пройшла успішно, як показано на рис.3.12.

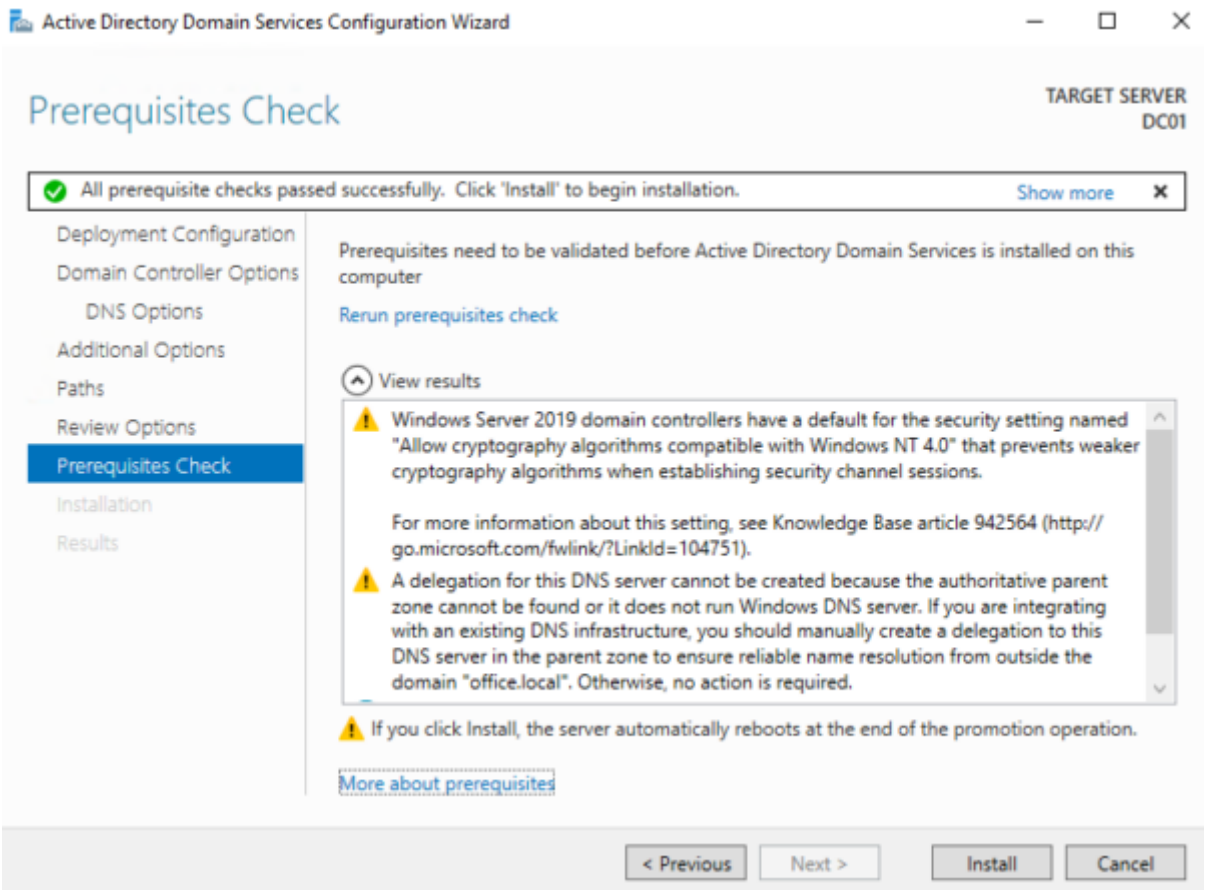

Рис.3.12. Перевірка параметрів

На цьому етапі потрібно буде почекати кілька хвилин, доки завершиться процес встановлення. Відразу після цього сервер автоматично перезавантажиться. Після перезавантаження контролер домену буде готовий [15].

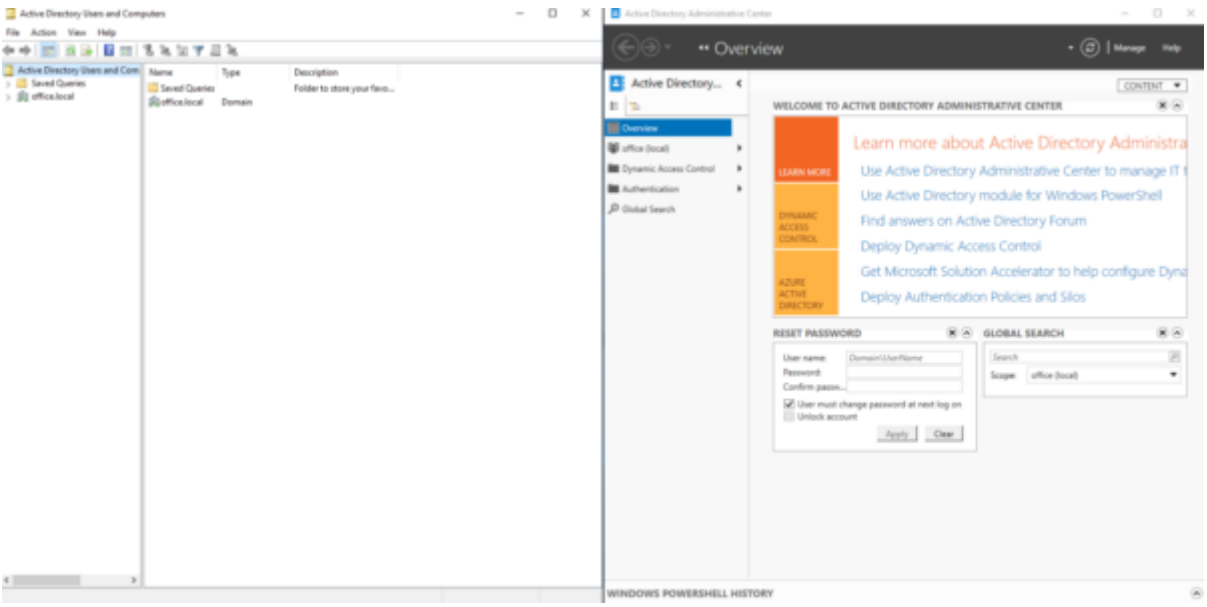

Рис.3.13. Контролер домену Active Directory

3.2. Технологія забезпечення кібербезпеки інформаційної системи організації за допомогою Active Directory

Active Directory необхідна для керування користувачами, комп’ютерами та ресурсами в мережевому середовищі. Адміністратори можуть легко керувати та захищати облікові записи користувачів, групові політики та ресурси організації використовуючи різні функції та служби, які надає AD.

Облікові записи користувачів

Облікові записи користувачів використовуються для надання співробітникам доступу до ресурсів мережі. Обліковий запис користувача зазвичай призначається кожному співробітнику, але іноді використовуються спільні облікові записи. Цей обліковий запис зберігається в базі даних Active Directory і може надавати такі відомості про працівника, як ім’я, прізвище, вулиця, штат, місто, керівник тощо.

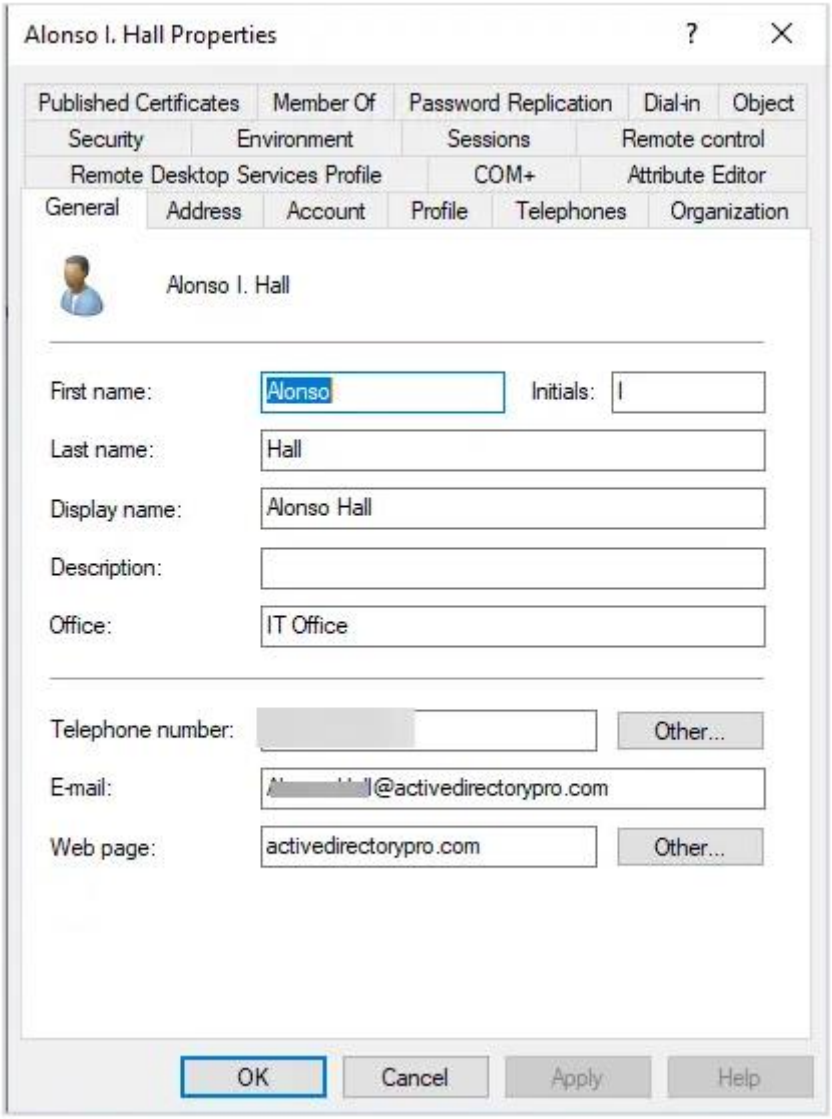

Рис.3.14. Створення облікових записів користувачів

Групи безпеки

Група безпеки — це сукупність користувачів або комп’ютерів. Це спрощує адміністрування дозволів для групи об'єктів. Наприклад, якщо 20 особам потрібен доступ до файлу, ви можете створити групу безпеки та додати 20 людей до групи. Тоді вам просто доведеться керувати доступом до файлів для групи замість 20 окремих облікових записів.

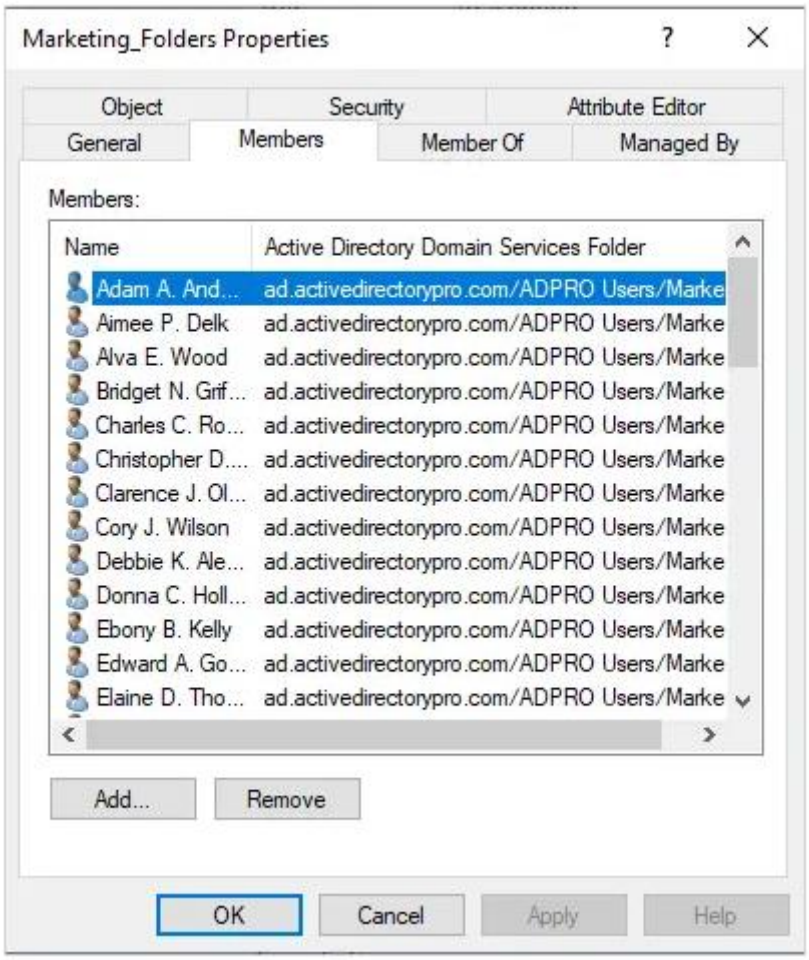

Рис.3.15. Групи безпеки

Об'єкти комп'ютерів

Коли комп’ютер приєднується до домену Active Directory, створюється об’єкт комп’ютера. Коли об’єкт створюється в Active Directory, він стає надійним об’єктом, який можна використовувати для отримання доступу до мережі. Наприклад, користувачеві потрібно увійти в мережу та отримати доступ до захищеного файлу. Користувач може увійти на надійний комп’ютер і отримати доступ до захищеного файлу (якщо користувачеві надано доступ).

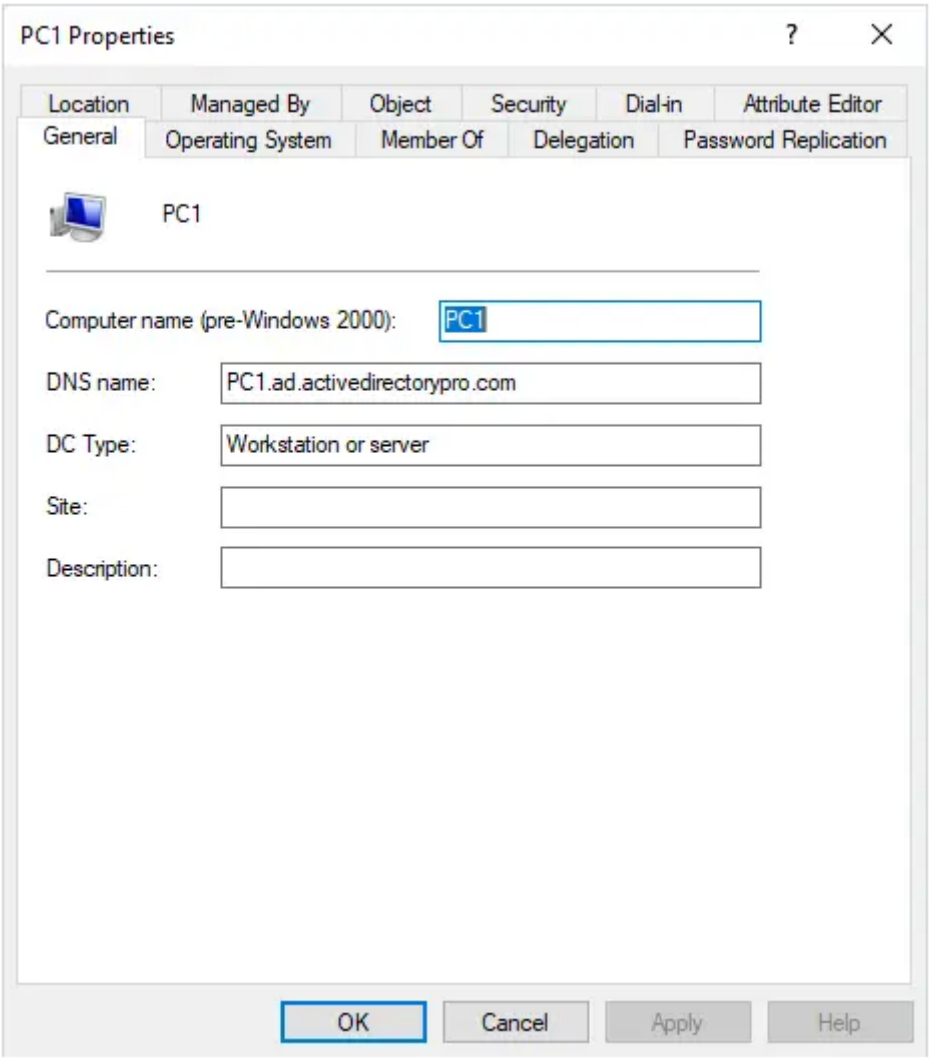

Рис.3.16. Об’єкт комп’ютера

Організаційні одиниці (OU)

В Active Directory організаційні одиниці використовуються для організації об’єктів Active Directory (користувачі, групи, комп’ютери). Упорядкування об’єктів AD полегшує адміністрування та застосування політик. Наприклад, можна організувати всіх користувачів у їхні власні папки відділу. Рекомендується розділяти користувачів і комп’ютери на окремі OU.

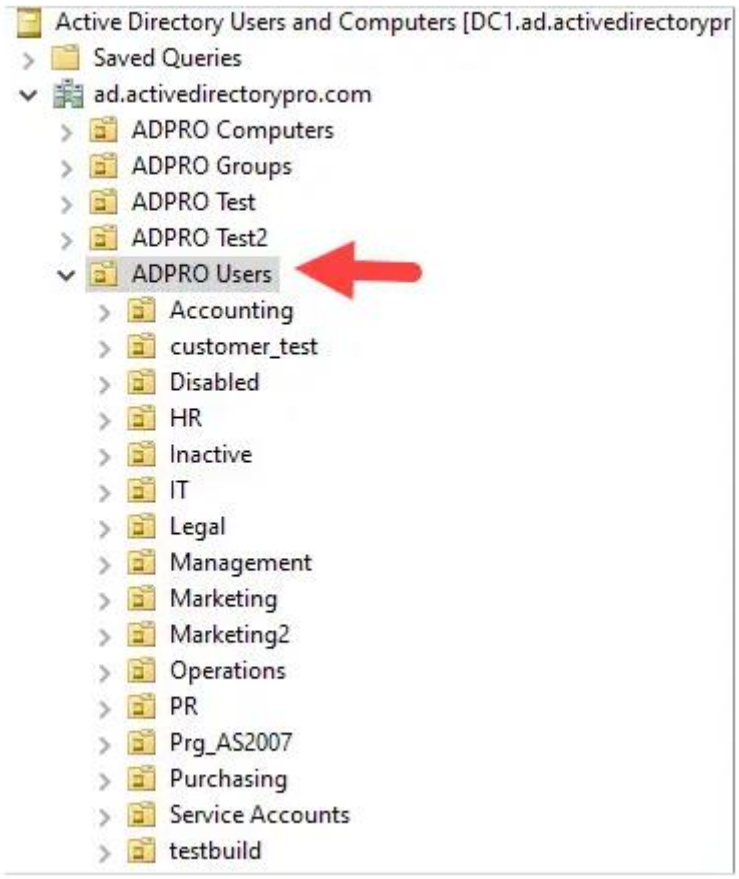

Рис.3.17. Організаційні одиниці

Інструменти, які використовуються для керування Active Directory.

Більшість із них включено під час інсталяції Active Directory на сервері. На сервері, на якому запущено Active Directory, можна отримати доступ до цих інструментів керування в папці «Windows Administrative Tools».

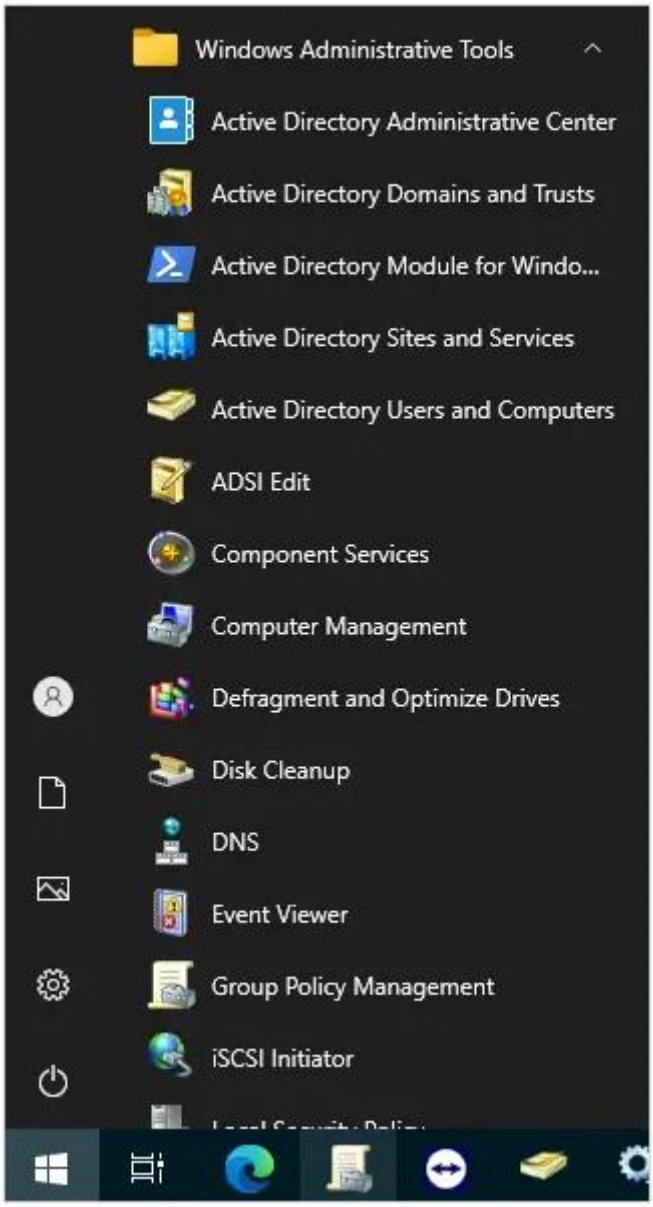

Рис.3.18. Інструменти AD

Користувачі та комп’ютери Active Directory (ADUC)

Це консоль, яка використовується для створення облікових записів користувачів, комп’ютерів і груп і керування ними. Наприклад, щоб створити новий обліковий запис користувача, потрібно відкрити консоль ADUC, щоб створити новий обліковий запис, встановити пароль і додати користувача до груп. Він також використовується для створення OU та організації об’єктів організації.

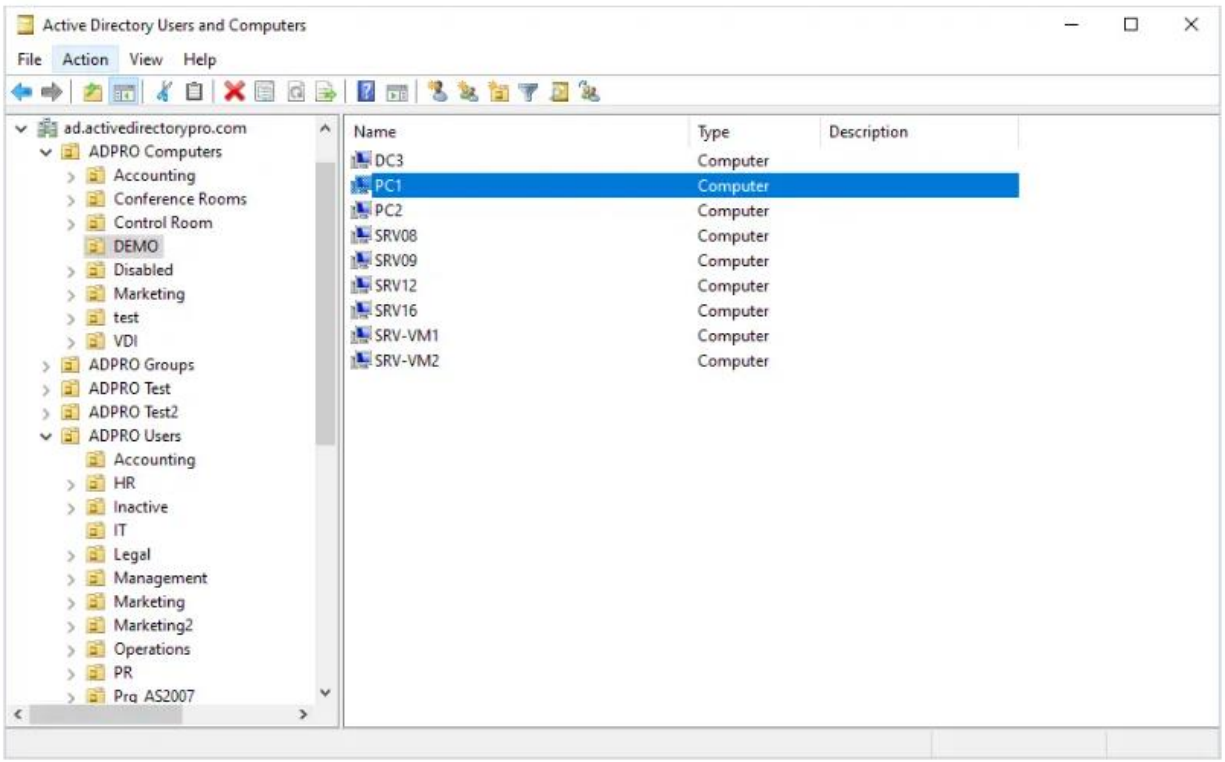

Рис.3.19. Консоль управління користувачами та комп’ютерами[10]

Сайти та служби Active Directory

Ця консоль використовується для керування вашими сайтами та підмережами. Якщо є лише один сайт, не потрібно використовувати цю консоль. Якщо Active Directory розгортається у кількох географічних регіонах, в такому випадку може знадобитися використовувати цю консоль для керування підмережами, сайтами та реплікацією.

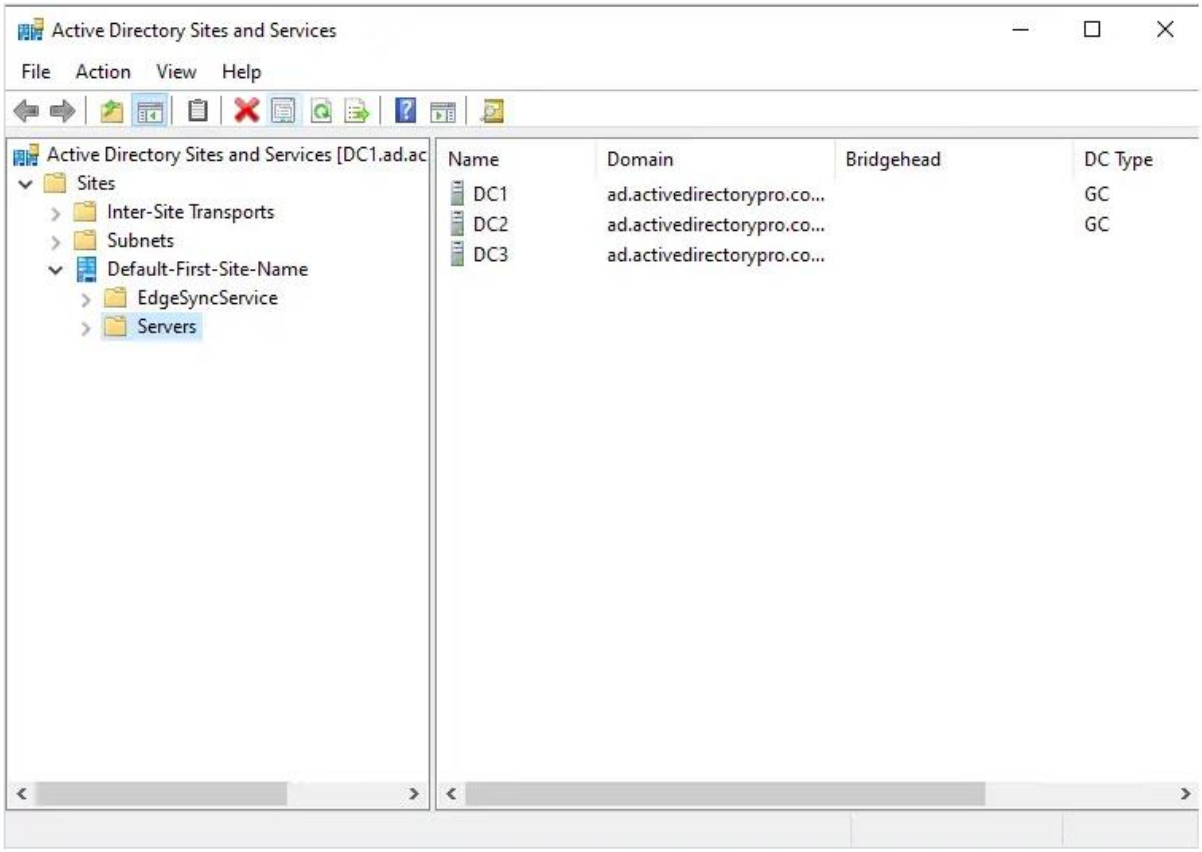

Рис.3.20. Консоль управління сайтами та сервісами

Консоль керування груповою політикою

Групова політика забезпечує централізоване керування та налаштування політики для користувачів і комп'ютерів у середовищі Active Directory. Наприклад, щоб переконатися, що всі користувачі змінюють свій пароль кожні 90 днів, адміністратори безпеки повинні використовувати групову політику та налаштувати політику паролів. Розуміння використання групової політики є важливою функцією системного адміністратора.

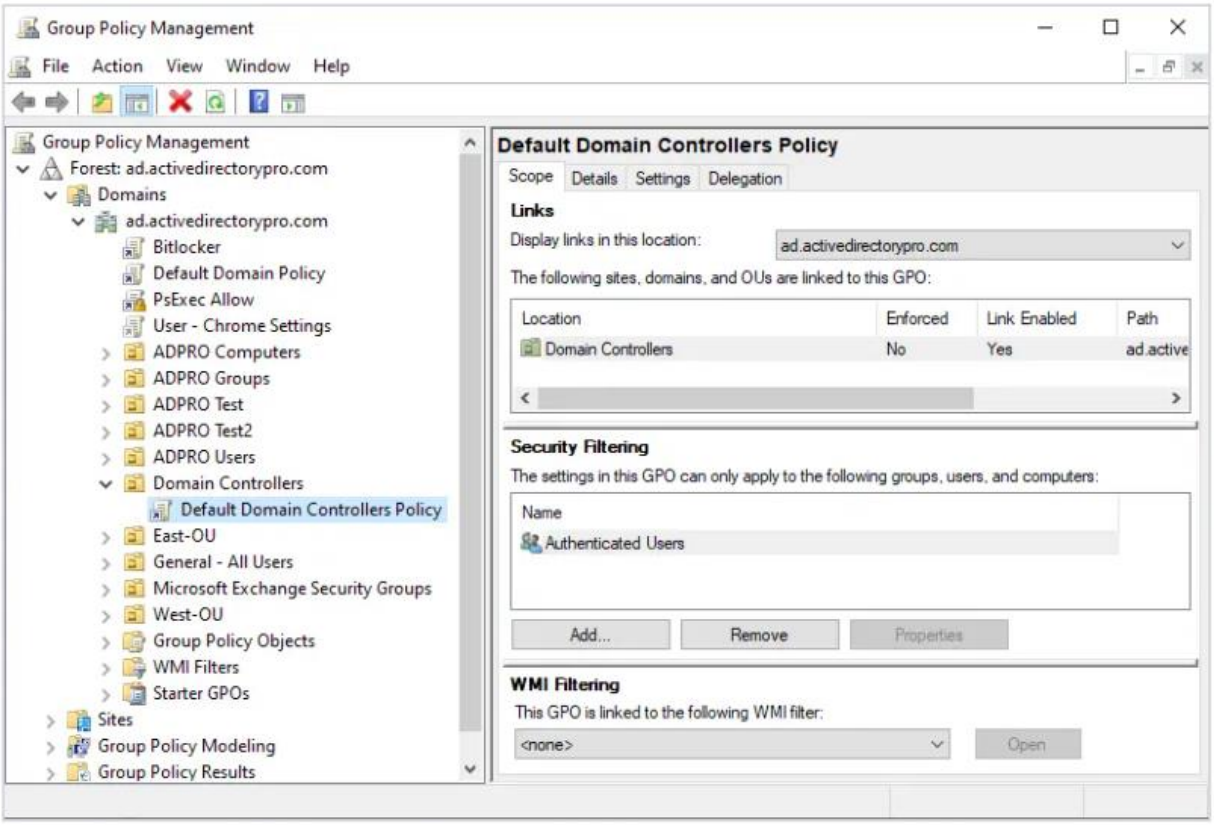

Рис.3.21. Консоль керування груповою політикою

DNS

Консоль DNS використовується для керування та створення зон DNS і записів ресурсів. Active Directory не працюватиме без DNS, він включається під час встановлення AD.

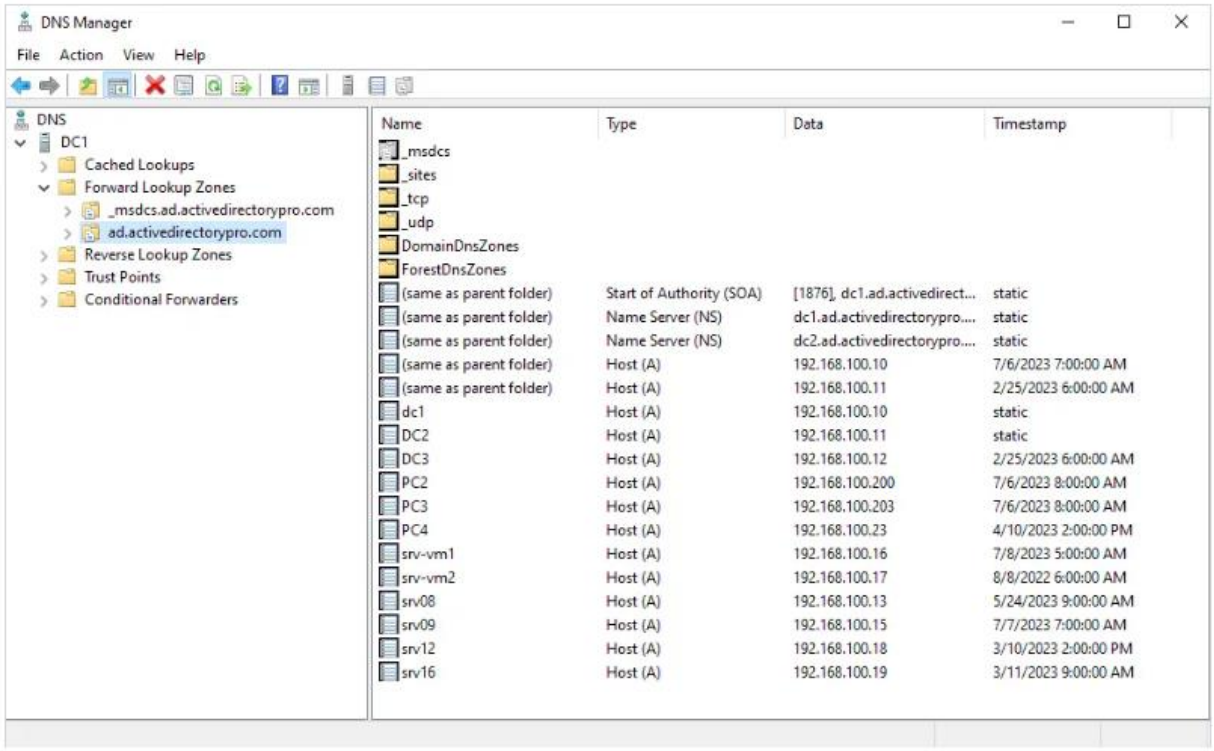

Рис.3.22. Консоль DNS

DHCP

Консоль DNS використовується для створення та керування пулами адрес DHCP у корпоративній мережі.

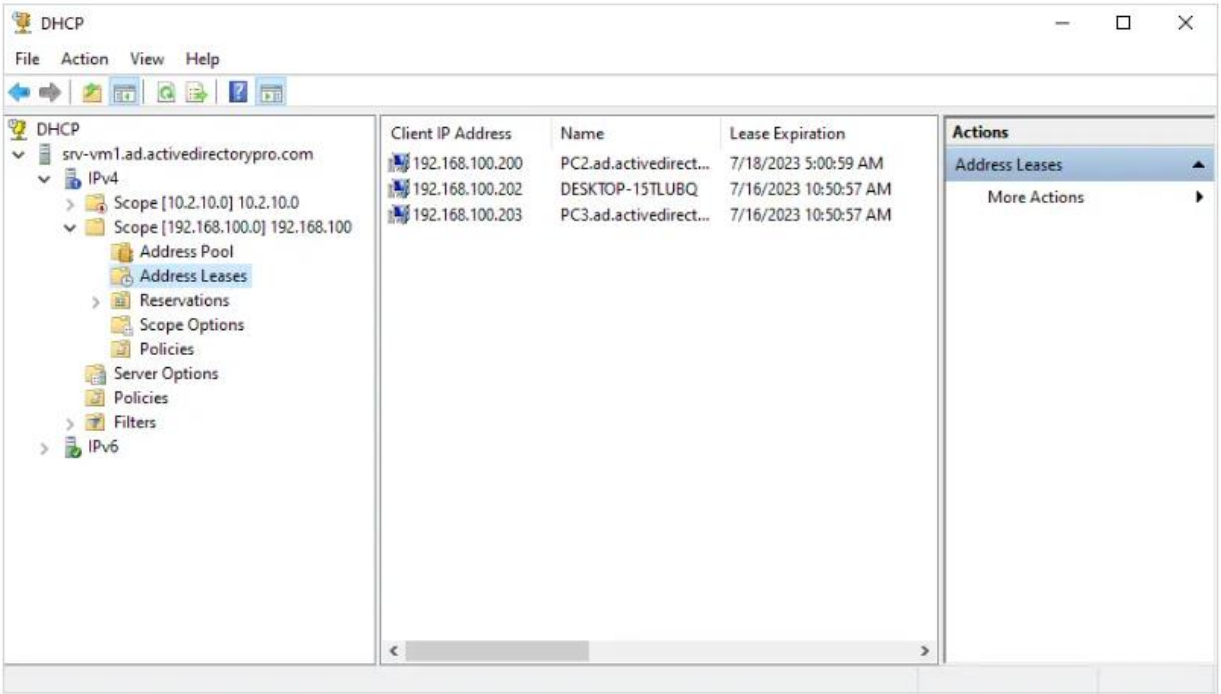

Рис.3.23. Консоль DHCP

PowerShell

PowerShell — це інструмент командного рядка, який допомагає автоматизувати багато рутинних завдань, таких як створення, оновлення та звітування про об’єкти в Active Directory [11].

Типи Active Directory

Існують різні типи розгортань Active Directory (AD), кожен із яких адаптований задоволення конкретних потреб організації та мережного середовища. Ось три основні типи Active Directory:

Локальний Active Directory

Локальна служба Active Directory — це традиційне розгортання інфраструктури Active Directory у власному центрі обробки даних організації або локальному середовищі. У цьому налаштуванні організації підтримують власні контролери домену, які зберігають і керують інформацією каталогу мережі. Локальна служба Active Directory забезпечує повний контроль та налаштування інфраструктури, але вимагає, щоб організація несла відповідальність за обслуговування обладнання, безпеку та масштабованість.

Azure Active Directory (Azure AD)

Azure Active Directory (Azure AD) – це хмарна служба каталогів та керування ідентифікацією Microsoft. Azure AD призначений для забезпечення керування ідентифікацією та доступом для хмарних програм та служб. Він пропонує такі функції, як єдиний вхід (SSO), багатофакторну автентифікацію (MFA) та інтеграцію з різними програмними програмами як послуги (SaaS). Azure AD можна використовувати незалежно або у поєднанні з локальною Active Directory, створюючи гібридне рішення для керування ідентифікацією та доступом.

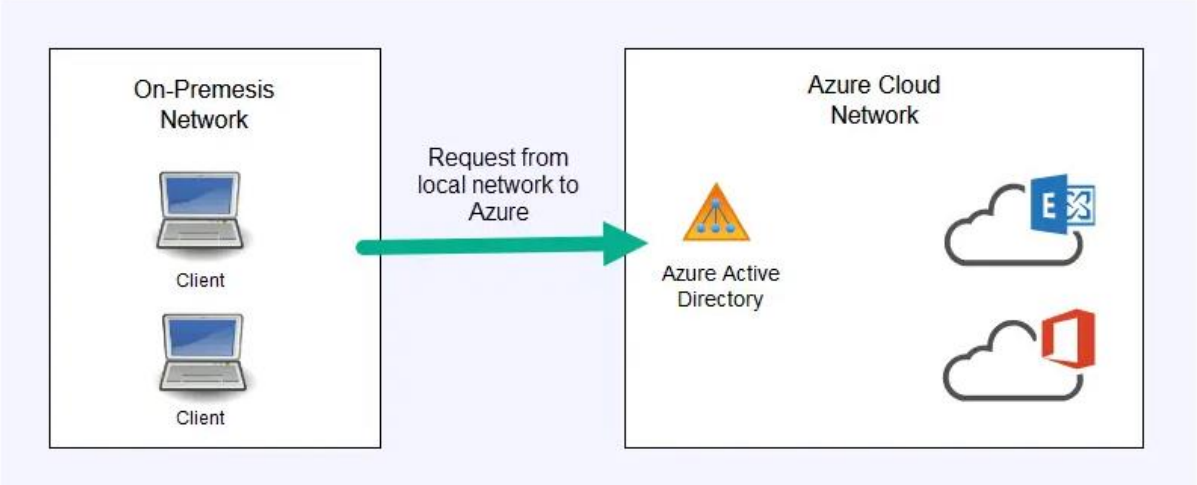

Рис.3.24. Azure Active Directory

ADDS – доменні служби Active Directory (локальний Active Directory).

AAD – Azure Active Directory (хмарний Active Directory).

Гібридна Azure AD

Гібридний каталог Active Directory — це коли у вас є локальний каталог Active Directory (ADDS) і синхронізація його з хмарою Azure Active Directory (AAD). У гібридному режимі ви можете синхронізувати свою локальну AD з Azure AD за допомогою програмного забезпечення Microsoft під назвою Azure AD Connect. Це дає змогу мати тих самих користувачів і паролі як на локальному, так і в хмарному сховищі. Це робиться для того, щоб користувачі мали єдиний вхід як до локальних ресурсів, так і до хмарних ресурсів [13].

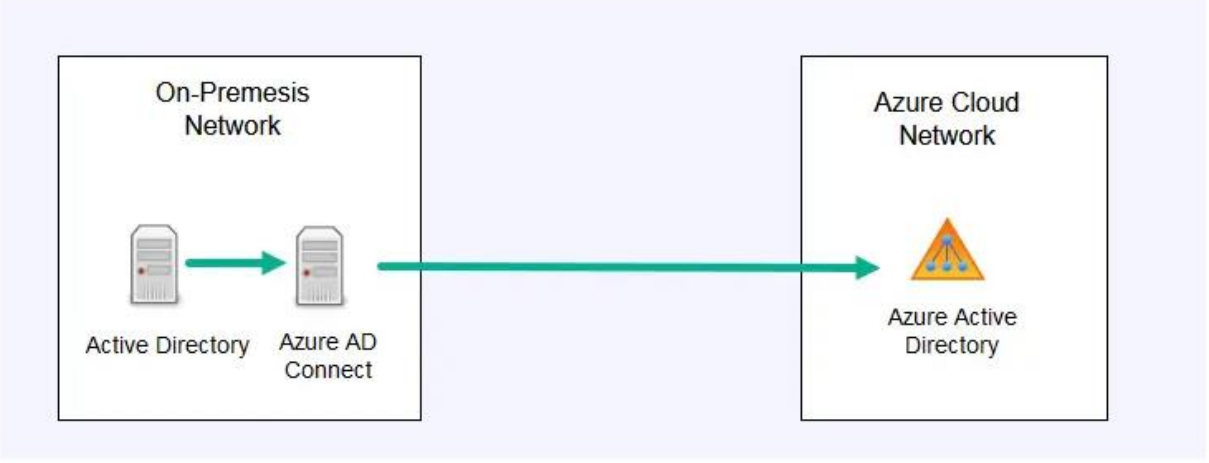

Рис.3.25. Гібридна Azure AD

Служби федерації Active Directory (AD FS)

Служби федерації Active Directory (AD FS) – це компонент Active Directory, який забезпечує можливості єдиного входу (SSO) у різних організаціях та мережах. AD FS дозволяє користувачам пройти автентифікацію один раз і отримати доступ до кількох ресурсів або служб, навіть якщо вони розміщуються в різних організаціях або використовують різних постачальників посвідчень. AD FS використовує довірених постачальників посвідчень та токени безпеки для спрощення єдиного входу та встановлення довірчих відносин між організаціями.

Ці типи Active Directory можна використовувати в гібридних середовищах, де організації поєднують локальну Active Directory з хмарними рішеннями, такими як Azure AD і AD FS. Це забезпечує плавне та інтегроване управління ідентифікацією та доступом до локальних та хмарних ресурсів.

Зрештою вибір типу Active Directory залежить від таких чинників, як організаційні вимоги, потреба у хмарних сервісах, масштабованість та бажаний рівень контролю та налаштування. Перш ніж приймати рішення, організаціям слід оцінити свої конкретні потреби та розглянути переваги та недоліки кожного типу [12].

3.3. Рекомендації щодо забезпечення безпеки організації на базі Active Directory

Локальні розгортання Microsoft AD можна захистити від численних загроз шляхом посилення засобів захисту та контролю. Стратегії посилення та пом’якшення вимагають захисту облікових даних, систем, процесів та ідентифікаційних даних.

Управління системою

Керування системою стосується контролю за встановленням меж для системи та впровадженням безпечного плану для забезпечення надання та постійного безпечного доступу до служби AD. Таким чином, для створення

надійного середовища для роботи захищеної інфраструктури AD слід реалізувати наступне:

— використовувати спеціальні адміністративні робочі станції для всіх завдань адміністратора з апаратною багатофакторною автентифікацією (MFA);

— використовувати окремі привілейовані облікові записи для завдань адміністратора;

— виведення з експлуатації або відокремлення застарілих служб і програм AD;

— обмеження мережеві підключення до та від серверів AD – жодного вхідного чи вихідного підключення до Інтернету;

— налаштування унікальних привілейованих облікових записів та паролі локального адміністратора для серверів і робочих станцій;

— блокування привілейованих облікових записів від використання в неавторизованих системах;

— здійснення віддаленого адміністрування лише з виділеної адміністративної робочої станції та лише за допомогою RDP із шифруванням TLS.

Управління обліковим записом

Управління обліковими записами стосується основних елементів керування для безпечного керування всіма обліковими записами користувачів і привілейованими обліковими записами від надання до виведення з експлуатації в середовищах служби AD. Деякі приклади привілейованих облікових записів включають локальні та доменні адміністративні облікові записи, службові облікові записи та вбудовані адміністративні облікові записи.

Для керування обліковим записом має бути реалізовано наступне:

— ввімкнений апаратний маркер MFA (наприклад, смарт-картку та клавіатуру, USB-ключ) для всіх облікових записів користувачів і адміністратора відповідно до вказівок Microsoft в AD і на всіх кінцевих точках;

— використання принципу найменших привілеїв для призначення адміністративних прав і привілеїв і керування ними;

— надання доступу на основі принципу найменших привілеїв і використання керованих сервісних облікових записів, де це можливо;

— уникнення призначення облікових записів служб у стандартних привілейованих групах, таких як локальні адміністратори або групи адміністраторів домену;

— облікові записи служб повинні використовуватися лише програмами чи службами, а не користувачами;

— фільтрація паролів AD, щоб заблокувати використання скомпрометованих або неправильних паролів.

Безпека та захист додатків

Обмежуючи додатки, дозволені на серверах AD, і дозволяючи або встановлюючи лише служби та програми, які мають вирішальне значення для виконання та підтримки функцій служб каталогів, організація матиме більш надійну позицію захисту від AD. Зменшення роботи програмного забезпечення до мінімуму є ключовим кроком у зміцненні та зменшенні вектору атаки.

Системи служби каталогів повинні мати лише явно схвалені програми, встановлені шляхом застосування дозволених списків програм на серверах і адміністративних робочих станціях. Для запобігання несанкціонованому встановленню та використанню додатків на серверах на серверах AD і виділених адміністративних робочих станціях слід запроваджувати засоби керування на основі хостів і політик.

Журналювання, аудит і моніторинг

Слід увімкнути моніторинг, аудит і журналювання для діяльності служби каталогів. Усі події мають надсилатися на віддалений сервер, яким неможливо керувати за допомогою основних облікових даних. Журнали подій також можна пересилати на централізований сервер безпеки та керування подіями (SIEM), щоб полегшити агрегацію, консолідацію та аналіз подій у журналах активності. Необхідно запровадити автоматичні механізми попередження, щоб виявити серйозніші порушення політики безпеки для швидшого реагування. Події збою та

успіху, пов’язані з конфіденційними або критичними операціями сервера, слід реєструвати, відстежувати та перевіряти. Організація також має видалити застарілі або неактивні облікові записи користувачів і запровадити моніторинг подій, пов’язаних із використанням цих облікових записів.

Вкрай важливо, щоб організація відстежувала, реєструвала та перевіряла використання всіх привілейованих або адміністративних облікових записів. Можна ввімкнути параметри системного аудиту, щоб регулярно перевіряти облікові записи з привілейованим або адміністративним доступом.

Виявлення загрози та реагування

Під час виявлення та реагування на загрози слід враховувати потенційні сценарії загроз, як-от компрометація ваших активів AD учасником загрози, а також засоби керування виявленням, які необхідно запровадити.

Організація може покращити запобігання та виявлення відомих методів атак за допомогою індикаторів компрометації (IoC) і автоматизованих технологій запобігання загрозам. Слід відстежувати чутливі події активності Windows, пов’язані з AD, які можуть свідчити про спробу або успішну компрометацію. Використовуючи рішення для виявлення та запобігання загрозам у мережі та кінцевих точках, організація може виявляти та реагувати на спроби скомпрометувати AD.

Виправлення та керування змінами

Інфраструктуру AD необхідно підтримувати та оновлювати в усіх випадках. Це включає планування виправлень, тестування вікон і підтвердження сумісності виправлень із бізнес-додатками. Сервери AD слід налаштувати за допомогою інкрементальної стратегії з можливістю відкату, коли доступні матеріали для обслуговування програмного забезпечення від Microsoft, і з мінімальними запланованими вікнами простою. Це забезпечить обмежені збої в роботі служби, якщо буде виявлено проблему з виправленням. Це також забезпечить можливість відкату без впливу на все середовище. Формальні процеси управління змінами також повинні бути прийняті для сертифікації та перевірки застосування необхідних оновлень.

Безперервність

Безперервність вимагає від організації планування на випадок непередбачених ситуацій, щоб допомогти відновити службу каталогів від широкого спектру загроз, включаючи збої в роботі системи або інциденти кібербезпеки. Потрібно застосувати AD Recycle Bin, щоб допомогти у відновленні об’єктів AD.

Щоб допомогти забезпечити безперервність роботи, слід встановити процеси, які дозволяють автоматизований збір критично важливих системних даних і резервне копіювання інформації. Переконайтеся, що резервні копії періодично перевіряються, наприклад щокварталу або після суттєвих змін, щоб перевірити цілісність і корисність. Дані резервного копіювання мають бути ізольовані від основної мережі, і слід приділити увагу підтримці резервних копій повністю в автономному режимі на додаток до будь-яких інших стратегій резервного копіювання, які використовуються.

Окрім резервного копіювання, організація повинна створювати, тестувати та оновлювати плани відновлення інцидентів щодо потенційних сценаріїв ризику, які можуть виникнути. Потрібно підготуватися до відновлення після інцидентів безпеки, які можуть вплинути на цілісність або доступність середовища AD. Можна зробити це, налаштувавши процедури відновлення системи та документацію для середовища AD.

Навчання користувачів

Організація повинна проводити регулярні тренінги з питань безпеки для власників привілейованих облікових записів та інших кінцевих користувачів системи. Навчальна програма має бути розроблена таким чином, щоб постійно навчати всіх користувачів поточним найкращим практикам безпеки та заохочувати зміни поведінки та вдосконалення кібергігієни, щоб запобігти небажаній або ризикованій поведінці користувачів. Організація також має створити процеси для спрощення вимог безпеки для кінцевих користувачів, скориставшись формальними навчальними сесіями та засобами наочної допомоги [14].

ВИСНОВКИ

У ході роботи було проведено детальний аналіз сучасних методів забезпечення кібербезпеки, і виявлено, що AD грає ключову роль у цьому процесі. Використання централізованої системи управління ідентичністю дозволяє забезпечити ефективний контроль доступу та вдосконалити системи безпеки.

Розгляд різноманітних аспектів функціональності AD підтвердив його важливість у вирішенні завдань забезпечення безпеки. Відповідно до отриманих даних, AD забезпечує ефективний механізм керування правами доступу, аутентифікації та аудиту, сприяючи запобіганню та виявленню кіберзагроз.

В результаті дослідження були визначені переваги використання AD, такі як централізоване управління ідентичністю та автоматизація процесів безпеки. Однак виявлені й обмеження, такі як технічні труднощі та необхідність уважного управління для мінімізації ризиків.

На основі результатів дослідження висловлені конкретні рекомендації щодо оптимізації системи безпеки з використанням AD. Зокрема, важливо акцентувати увагу на постійному моніторингу, оновленні політик безпеки та регулярному аудиті для забезпечення високого рівня захисту.

В роботі було розглянуто важливість технології AD у сучасному контексті кібербезпеки. Було виявлено, що Active Directory ефективний інструмент для управління ідентичністю та забезпечення безпеки інформаційних систем організації. Однак для максимального ефекту важливо постійно вдосконалювати стратегії безпеки та враховувати нові тенденції в кібербезпеці.

Таким чином, Active Directory є важливим аспектом у забезпеченні кібербезпеки в інформаційних системах організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Amanda M. Y. Chu, Mike K. P. So. Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective. 2020.

2. Dave Bourgeois and David T. Bourgeois Information Systems for Business and Beyond. 2014.

3. Introduction to Active Directory Security. URL: https://www.linkedin.com/pulse/introduction-active-directory-security-rubén-bernardo-guzmán-mercado/ (дата звернення: 25.10.2023)

4. Identity, Credential, and Access Management (ICAM) - ITSAP.30.018. Canadian Centre for Cyber Security. 2022. URL: https://www.cyber.gc.ca/en/identity-credential-and-access-management-icam-itsap30018 (дата звернення: 05.11.2023)

5. Department of Defense, Office of the Chief Information Officer (DoD CIO). DoD Enterprise Identity, Credential, and Access Management (ICAM). June 2020. C. 39-50

6. Benefits of Active Directory Domain Services (AD DS). URL: https://www.intelecis.com/benefits-of-active-directory-domain-services/ (дата звернення: 10.11.2023)

7. Active Directory Domain Services Overview. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата звернення: 10.11.2023)

8. Active Directory Domain Services Virtualization. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-virtualization (дата звернення: 15.11.2023)

9. Dishan Francis. Mastering Active Directory Design, Deploy, and Protect Active Directory Domain Services for Windows Server 2022. 2021. C. 29, 269

10. Active Directory Users & Computers (ADUC). URL: https://activedirectory.ncsu.edu/ou-admins/tools/aduc/ (дата звернення: 15.11.2023)

11. Advanced AD DS Management Using Active Directory Administrative Center. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/advanced-ad-ds-management-using-active-directory-administrative-center--level-200- (дата звернення: 15.11.2023)

12. AD FS Overview. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview (дата звернення: 19.11.2023)

13. What is Active Directory? URL: https://activedirectorypro.com/what-is-active-directory/ (дата звернення: 25.11.2023)

14. Guidance for securing Microsoft Active Directory services in your organization - ITSM.60.100. Canadian Centre for Cyber Security. 2023. URL: https://www.cyber.gc.ca/en/guidance/guidance-securing-microsoft-active-directory-services-your-organization-itsm60100 (дата звернення: 07.12.2023)

15. Installing Windows Server 2022 & Active Directory Domain Services URL: https://medium.com/@cavan.fowler/installing-windows-server-2022-active-directory-domain-services-6b5e4f13c2f8 (дата звернення: 04.12.2023)

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)