Міністерство освіти і науки України

АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ ТА СИСТЕМ

Конспект лекцій
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Комп'ютерна інженерія «
галузь знані 12 (F) Інформаційні технології
спеціальності 123 (F7) Комп'ютерна інженерія
денної та заочної форм навчання

Луцьк 2026

УДК 004.65(07)
А31

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від « _____ « _____ 20 26 року.
Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ
Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки
ЛНТУ, протокол № _____ від « _____ « _____ 20 26 року.
Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладач: _____ Наталія БАГНЮК, кандидат технічних наук,
доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ
_____ Катерина БОРТНИК, кандидат технічних наук,
доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Роман ГРУДЕЦЬКИЙ, старший викладач
кафедри автоматизації та комп'ютерно-інтегрованих технологій,
проректор з НПР та цифрової трансформації ЛНТУ

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат
технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ
Національного університету харчових технологій»

А31 Адміністрування комп'ютерних мереж та систем: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань 12 (F) Інформаційні технології спеціальності 123 (F7) Комп'ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2026. 328 с.

Конспект лекцій з дисципліни «Адміністрування комп'ютерних мереж та систем» складено відповідно до діючої програми курсу.

Призначено для здобувачів вищої освіти спеціальності 123 (F7) Комп'ютерна інженерія освітньої програми «Комп'ютерна інженерія».

ЗМІСТ

Тема 1 Основи IP-адресації та підмереж, розуміння мережевої операційної системи 5
Тема 2 Віртуалізація та серверні середовища 19
Тема 3 Встановлення та основи адміністрування Windows Server 45
Тема 4 Active Directory 74
Тема 5 Групові політики 110
Тема 6 Служба DNS 146
Тема 7 Служба DHCP 170
Тема 8 RDS в Active Directory 184
Тема 9 Реалізація нових удосконалень безпеки у Windows Server 2025 200
Тема 10 Веб-сервер IIS 232
Тема 11 Основи Linux-адміністрування. Мережеві служби Linux. Веб-сервісна інфраструктура у Linux 249
Тема 12 Комплексне адміністрування мереж і систем 291
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 321

ВСТУП

Дисципліна «Адміністрування комп’ютерних мереж та систем» є фундаментальною складовою професійної підготовки фахівців у галузі комп’ютерної інженерії та інформаційних технологій. Сучасні інформаційні системи, корпоративні мережі, хмарні сервіси та критично важливі цифрові інфраструктури базуються на складних мережевих і серверних платформах, ефективне функціонування яких неможливе без професійного адміністрування. Саме тому вивчення принципів побудови, налаштування, супроводу та захисту комп’ютерних мереж і серверних операційних систем є необхідною умовою підготовки конкурентоспроможних фахівців.

Метою вивчення дисципліни є формування у здобувачів вищої освіти системного розуміння архітектури комп’ютерних мереж, принципів IP-адресації та підмережування, функціонування мережевих протоколів, а також набуття практичних навичок адміністрування серверних операційних систем у середовищах клієнт-сервер і хмарних інфраструктурах. Особлива увага приділяється сучасним мережевим операційним системам, зокрема Windows Server та Linux Server, які є основою більшості корпоративних і датацентрових рішень.

У межах курсу розглядаються питання організації мережевих служб, керування обліковими записами користувачів і пристроїв, налаштування доменних структур, забезпечення доступності ресурсів, резервного копіювання, моніторингу та реагування на інциденти. Значний акцент зроблено на проблемах інформаційної безпеки, сегментації мереж, управління доступом і забезпечення стійкості мережевих сервісів до сучасних кіберзагроз.

Конспект лекцій побудовано з урахуванням сучасних тенденцій розвитку інформаційно-комунікаційних технологій, зокрема переходу до гібридних і хмарних інфраструктур, використання віртуалізації, контейнеризації та централізованих засобів керування. Матеріал подано таким чином, щоб поєднати теоретичні засади мережевих технологій із практичними аспектами адміністрування реальних систем.

Використання даного конспекту лекцій дозволить здобувачам вищої освіти сформувати цілісне уявлення про функціонування сучасних комп’ютерних мереж і серверних платформ, підготуватися до виконання практичних і лабораторних робіт, а також закласти основу для подальшого вивчення дисциплін, пов’язаних із кібербезпекою, хмарними технологіями та обробкою інцидентів.

Тема 1
Основи IP-адресації та підмереж, розуміння мережевої операційної системи

Розуміння хостів, вузлів і архітектури клієнт-сервер

Для усвідомлення значущості комп'ютерних мереж та мережевих операційних систем доцільно звернутися до історії їх виникнення. Потреба у спільному використанні ресурсів стала поштовхом до початкової розробки мережевих технологій у 1960-х та 1970-х роках. Зі зростанням попиту відбувався розвиток цих технологій, що призвело до формування вичерпної термінології та концепцій, необхідних для опису комп'ютерних мереж та всього, що з ними пов'язано. Так виникли поняття типів мереж, топологій, архітектур та компонентів, що визначило комп'ютерні мережі як одну з монументальних комунікаційних інновацій людства. Інтернет є яскравим прикладом глибоких суспільних переваг комп'ютерних мереж, об'єднуючи незліченну кількість комп'ютерів та долаючи географічні відстані в комунікації.

Згідно зі словником Merriam-Webster, мережа визначається як група людей або організацій, які тісно пов'язані та працюють один з одним. Крім того, мережа описується як обмін інформацією або послугами між окремими особами, групами або установами. Ці визначення забезпечують просту, конкретну основу для розуміння комп'ютерних мереж [3].

По суті, комп'ютерна мережа – це група комп'ютерів, з'єднаних за допомогою мережевих пристроїв та середовищ передачі даних для спільного використання ресурсів. Ці ресурси зазвичай включають дані, мережеві служби та периферійні пристрої. Наприклад, спільне використання файлів, програм, принтерів та іншої периферії є стандартною практикою в мережевому середовищі. Важливо розрізняти, чим є комп'ютерна мережа і що вона виконує. Перше пояснює структуру та компоненти, тоді як друге висвітлює переваги та функціональні можливості. На рисунку 1.1 проілюстровано, що комп'ютерна мережа складається зі з'єднаних комп'ютерів, які спільно використовують ресурси [1].

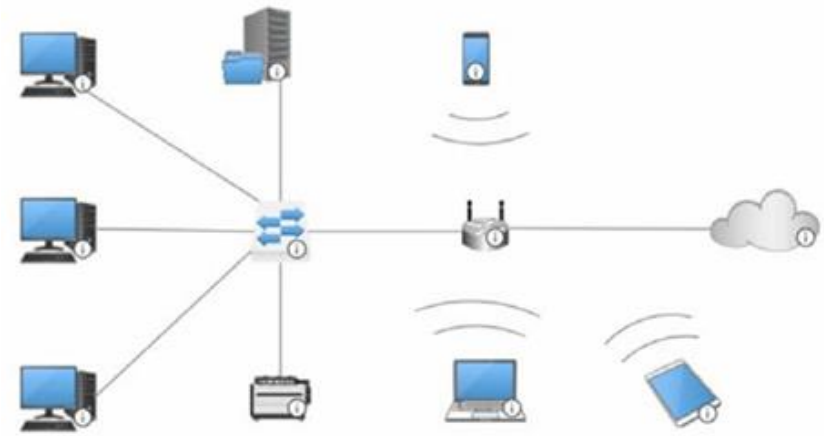

Рисунок 1.1 – Типовий приклад комп'ютерної мережі [3]

Комп’ютерні мережі бувають різних типів, кожен з яких служить різним цілям і охоплює різні території. Проектування та побудова комп’ютерної мережі є процесом, тісно пов’язаним з її визначенням. В основі комп’ютерної мережі лежить наявність щонайменше двох комп’ютерів. Кількість комп’ютерів і спосіб їх доступу до спільних ресурсів визначають категоризацію типів мереж. Загалом, комп’ютерні мережі класифікуються на основі території, яку вони охоплюють, та їх цільового призначення.

Персональна мережа (Personal Area Network – PAN), зображена на рисунку 1.2, з’єднує та передає дані між пристроями в межах приватної зони, що зазвичай належить окремій особі. Наприклад, у домашньому офісі ноутбук, смартфон, принтер і навушники можуть бути підключені через Bluetooth або Wi-Fi [1].

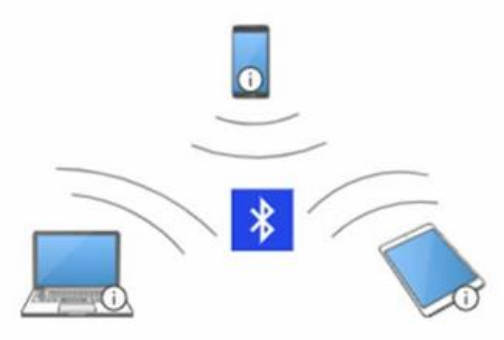

Рисунок 1.2 – Персональна мережа (PAN) [3]

Іншим типом мережі є локальна мережа (Local Area Network – LAN), яка має значно більшу зону покриття порівняно з PAN. LAN з’єднує два або більше комп’ютерів у межах локальної території, такої як одна кімната, поверх, кілька поверхів, будівля або кілька суміжних будівель. У LAN зазвичай використовуються центральний пристрій і мережеві середовища, такі як вита пара, коаксіальний або оптоволоконний кабель, для з’єднання комп’ютерів. На рисунку 1.3 проілюстровано розширену LAN, яка використовує два комутатори для підключення кількох пристроїв [1].

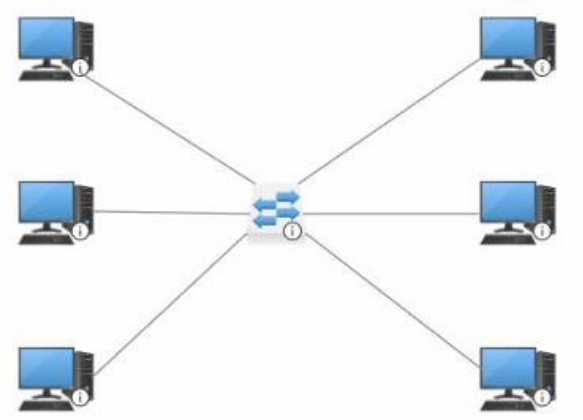

Рисунок 1.3 – Локальна мережа (LAN) [3]

Така конфігурація збільшує пропускну здатність мережі та дозволяє досягти більшої масштабованості, забезпечуючи зв'язок між різними сегментами мережі. Використання кількох комутаторів у розширеній LAN гарантує ефективну передачу даних між пристроями, покращуючи загальну продуктивність і надійність мережі. Це налаштування зазвичай використовується у великих середовищах для задоволення зростаючих потреб мережі при збереженні оптимальної продуктивності та мінімальної затримки.

Наступним типом мережі є муніципальна мережа (Metropolitan Area Network – MAN), яка має ще більше покриття, ніж LAN. MAN з'єднує кілька LAN у межах міста або містечка (рис. 1.4). MAN існують для полегшення спільного використання ресурсів і доступу в межах мегаполісу. Вони пропонують більше покриття, ніж LAN, але менше, ніж глобальні мережі (WAN). MAN є швидшими за LAN і WAN, часто використовуючи оптоволокно та гігабітні комутатори 3-го рівня для високошвидкісного з'єднання [1].

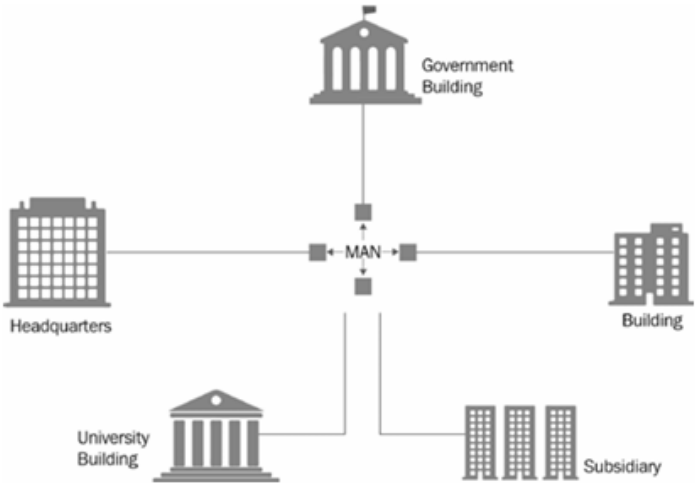

Рисунок 1.4 – Муніципальна мережа (MAN) [3]

Нарешті, розглядається глобальна мережа (Wide Area Network – WAN), яка має найбільше покриття. Вона охоплює великі географічні території за межами досяжності LAN і MAN. WAN використовують виділені телекомунікаційні лінії, такі як телефонні лінії, орендовані лінії або супутники, що робить їх доступними незалежно від географічних обмежень. Інтернет є квінтесенцією прикладу WAN [2].

Подібно до того, як персональні комп'ютери (ПК) мають свої компоненти, комп'ютерні мережі також складаються з необхідних елементів. У той час як ПК та периферійні пристрої знайомі більшості людей, IT-фахівці зосереджуються на таких компонентах, як мережеві пристрої, мережеві середовища та мережеві операційні системи (NOS).

У контексті комп'ютерної мережі клієнти та сервери зосереджені навколо доступу та надання мережевих ресурсів. Клієнти зазвичай ініціюють запити на ресурси, тоді як сервери

відповідають за доставку та керування доступом до цих ресурсів. Обидва відіграють життєво важливі ролі в мережевих операціях. Наприклад, як зображено на рисунку 1.5, сервер, підключений безпосередньо до принтера, пропонує послуги друку для ПК, які діють як ініціатори запитів на друк.

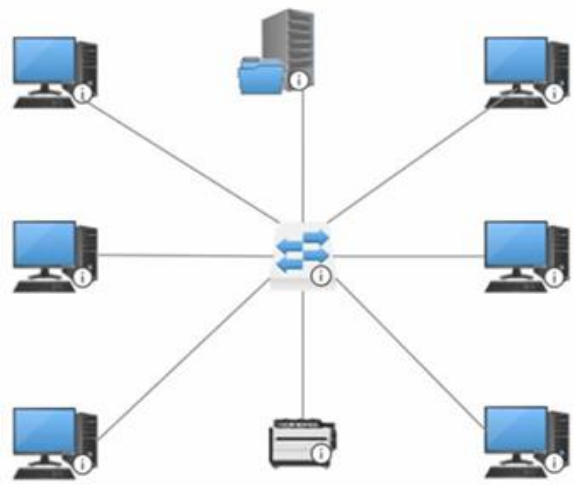

Рисунок 1.5 – Клієнт і сервер у комп’ютерній мережі [3]

Сам термін «сервер» походить від слова «служити» (англ. serve), що вказує на його роль у наданні корисних послуг. У комп’ютерній мережі сервери виконують цю роль, обслуговуючи клієнтів [3].

Хоча клієнти та сервери є фундаментальними мережевими компонентами, їхні ролі визначаються по-різному в мережевій термінології. Далі розглядається, як вони вписуються в ширшу структуру мережі.

Поняття хостів і вузлів часто викликають питання щодо їх відмінностей. Хоча на перший погляд вони можуть здаватися схожими, хости та вузли виконують різні функції в мережевій комунікації. Усі хости можна вважати вузлами, але не кожен вузол функціонує як хост.

Хост (англ. host) – це будь-який пристрій із призначеною IP-адресою на своєму мережевому інтерфейсі, який активно запитує або надає мережеві послуги. Зазвичай клієнти, сервери та маршрутизатори діють як хости [2].

IP-адреса (Internet Protocol address) – це логічна послідовність десяткових чисел, розділених крапками, що унікально ідентифікує хост у комп’ютерній мережі [3].

З іншого боку, вузол (англ. node) – це будь-який пристрій, здатний отримувати та передавати мережеві послуги, але який не має призначеної IP-адреси на своєму інтерфейсі (в контексті передачі даних користувача). Вузли зазвичай мають мережеві інтерфейси, що використовуються для цілей керування. Наприклад, на рисунку 1.6, ПК та файловий сервер діють як хости, тоді як комутатори функціонують як вузли.

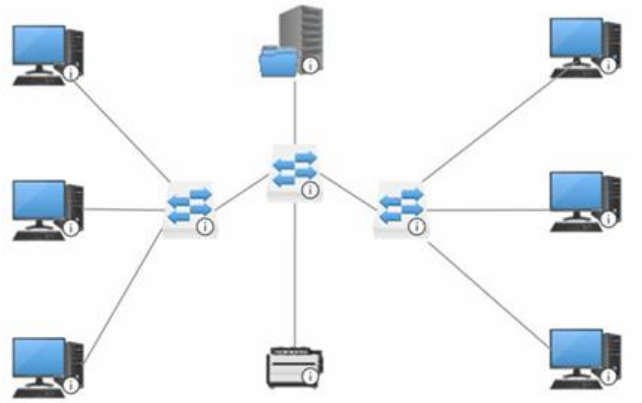

Рисунок 1.6 – Хости та вузли в комп’ютерній мережі

У середовищі Windows Server розуміння відмінності між хостами та вузлами є важливим, оскільки Windows Server часто працює в моделі клієнт-сервер. У цій моделі сервер надає ресурси, а клієнтські пристрої підключаються для доступу до цих послуг. Це налаштування підтримує ефективний розподіл ресурсів у мережах і є фундаментальним для IT-адміністрування.

Обговорення комп’ютерних мереж часто включає вивчення фундаментальних та всеосяжних концепцій, таких як компоненти, що їх складають. Це включає розгляд типів мереж на основі зон покриття, а також фізичних та логічних топологій, що керують їх фізичним розташуванням та структурною організацією. Архітектура комп’ютерної мережі охоплює комплексну структуру, яка інтегрує такі елементи, як фізичні та логічні топології, мережеві компоненти, протоколи зв’язку та принципи роботи.

Крім того, архітектура комп’ютерної мережі слугує проектною основою, що дозволяє комп’ютерам спілкуватися, використовуючи парадигму запиту та відповіді. Найбільш поширені мережеві архітектури включають однорангову (Peer-to-Peer – P2P) та клієнт-серверну моделі.

У мережі P2P хости працюють без попередньо визначених ролей. Замість цього вони динамічно перемикають ролі між клієнтом і сервером залежно від поточної мережевої активності (рис. 1.7).

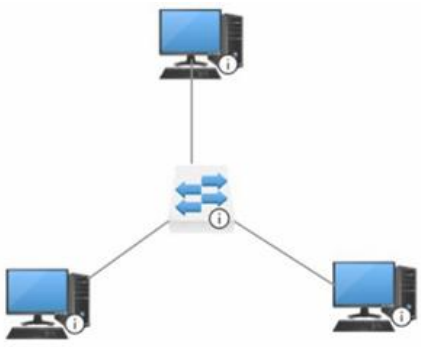

Рисунок 1.7 – Однорангова комп’ютерна мережа (P2P мережа) [3]

Наприклад, якщо PC1 запитує послуги від PC2, PC1 діє як клієнт, а PC2 служить сервером. Навпаки, якщо PC2 ініціює запит до PC1, PC2 стає клієнтом, а PC1 – сервером. Мережі PAN часто є прикладом налаштувань P2P.

В архітектурі мережі P2P усі хости беруть рівну участь. Ця рівність є фундаментальним аспектом моделі, де кожен хост може брати на себе роль клієнта або сервера за потреби.

На відміну від цього, архітектура мережі клієнт-сервер (представлена раніше на рисунку 1.6) призначає хостам конкретні ролі. Клієнти – це пристрої, які запитують послуги, тоді як сервери – це пристрої, які надають послуги в мережі. Цей структурований підхід до нетворкінгу забезпечує ефективні операції шляхом чіткого визначення ролей кожного пристрою. Зазвичай обов'язки клієнта та сервера покладаються на конкретні машини, що дозволяє оптимізувати комунікацію та керування ресурсами в мережі. Ця архітектура є фундаментальною в багатьох корпоративних середовищах, де масштабованість і надійність є вирішальними.

Кожен компонент мережі, від хостів і вузлів до архітектури клієнт-сервер, безпосередньо підтримує роботу в Windows Server 2025. Незалежно від того, чи виконується налаштування дозволів доступу, організація спільного використання ресурсів або моніторинг мережевого трафіку, ці концепції будуть повторюватися протягом усіх завдань з керування сервером [3].

Важливо зазначити, що для того, щоб комп'ютер міг ефективно спілкуватися в мережі, потрібна IP-адреса, яка слугує його унікальним ідентифікатором у цій мережі. IP-адресу можна розглядати як унікальний ідентифікатор пристрою, подібний до поштової адреси. У керуванні серверами IP-адресація дозволяє визначити структуру мережі та налаштувати пристрої для ефективного спілкування в межах мереж та між ними.

У більш складних мережах використовується поділ на підмережі (субнетування) для визначення конкретних сегментів у межах більшої мережевої структури, розділяючи її на менші, більш керовані частини. Ця сегментація покращує як безпеку, так і продуктивність – два ключові фактори при керуванні середовищами Windows Server, де підтримка оптимізованої комунікації та потоку даних є важливою.

На даний момент у світі визнаються дві провідні технології IP-адресації: IPv4 та IPv6. Незважаючи на зростаючу важливість IPv6, IPv4 залишається домінуючим стандартом адресації в інтернет-трафіку.

Ознайомлення із розумінням мережевої операційної системи, огляд і редакції Windows Server, мінімальні та рекомендовані системні вимоги

Мережева операційна система (Network Operating System – NOS) визначається як

спеціалізоване програмне забезпечення, спроектоване для керування, підтримки та надання різноманітних послуг у мережевому середовищі. Ці послуги включають спільний доступ до файлів і програм, веб-сервіси, автентифікацію та авторизацію, контроль доступу, адміністрування користувачів і комп'ютерів, інструменти конфігурації, керування ресурсами та інші функції, пов'язані з мережею. Отже, NOS відіграє вирішальну роль у ефективному керуванні мережевими ресурсами [3].

NOS формує основу функціональності сервера, забезпечуючи централізований контроль мережевих ресурсів та взаємодію клієнт-сервер. Windows Server 2025 функціонує як NOS, пропонуючи інструменти та функції, адаптовані для безперебійного керування пристроями, розміщення програм та обробки даних. Розуміння ролі NOS є важливим для повного використання можливостей Windows Server.

Визначними прикладами NOS сьогодні є Windows Server, Linux Server та macOS Server, кожен з яких здатний надавати комплексні мережеві послуги.

Windows Server, наріжний камінь лінійки серверних продуктів Microsoft, відомий своїм надійним графічним інтерфейсом користувача (GUI) та широкими можливостями керування мережевими ресурсами. З моменту свого заснування в 1993 році Windows Server еволюціонував, щоб задовольнити вимоги сучасних обчислювальних середовищ. Розвиток розпочався з Windows NT 3.5 на початку 1990-х років і формально стартував із Windows 2000 Server. Ключові віхи включають впровадження Windows Server 2008, який приніс такі функції, як Server Core та Hyper-V, та випуск Windows Server 2016, який покращив підтримку хмарної інтеграції, ілюструючи адаптивність системи [4].

Спочатку доступний як для 32-бітних, так і для 64-бітних архітектур, Windows Server перейшов виключно на 64-бітну архітектуру з випуском Windows Server 2012. Рідною файловою системою сервера залишається файлова система нової технології (New Technology File System – NTFS). Проте у Windows Server 2012 було представлено стійку файлову систему (Resilient File System – ReFS), яка в основному використовується в додатках баз даних завдяки своїй стійкості та ефективності [4].

Оскільки організації все частіше переходять на хмарні сервіси, Windows Server залишається актуальним, надаючи гібридні рішення, які безперебійно з'єднують локальні ресурси з хмарною інфраструктурою. Рисунок 1.8 ілюструє властивості диска C: Windows, демонструючи ключові атрибути, що підтримують керування сховищем файлів та системними ресурсами. Завдяки таким функціям, як Windows Admin Center та PowerShell, Windows Server надає IT-фахівцям можливість автоматизувати та оптимізувати завдання керування сервером, забезпечуючи його постійну актуальність у світі, що стає все більш цифровим та хмарно-орієнтованим.

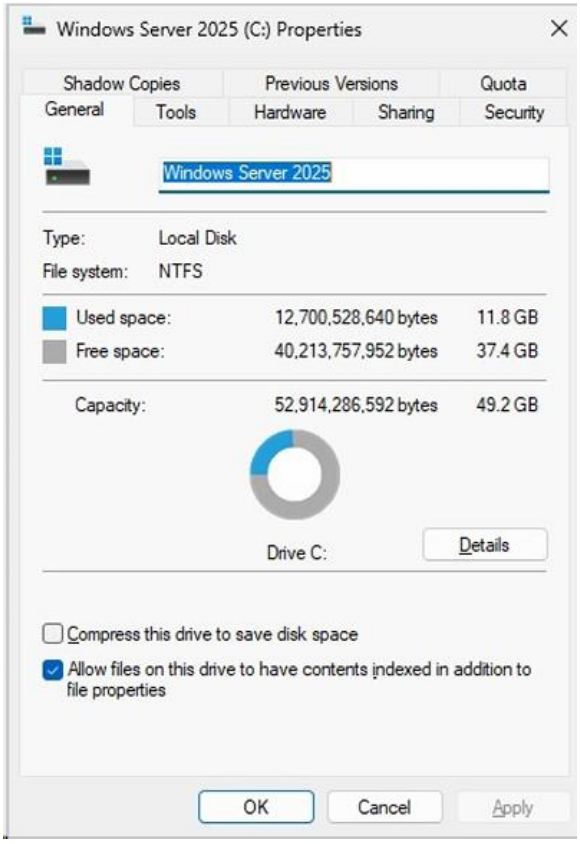

Рисунок 1.8 – Використання NTFS у Windows Server 2025 [3]

Linux вирізняється в ландшафті операційних систем своєю природою відкритого вихідного коду та широкою підтримкою спільноти. Розроблений Лінусом Торвальдсом на початку 1990-х років як Unix-подібна система, Linux швидко набув популярності завдяки своїй надійності та гнучкості. Ліцензований під загальною публічною ліцензією GNU (GPL), Linux еволюціонував у численні дистрибутиви, адаптовані до різних потреб користувачів. Сервери Linux, такі як Ubuntu Server, поширені у розміщенні веб-серверів та забезпеченні роботи суперкомп'ютерів завдяки своїй безпеці та масштабованості як у локальних, так і в хмарних середовищах (рис. 1.9).

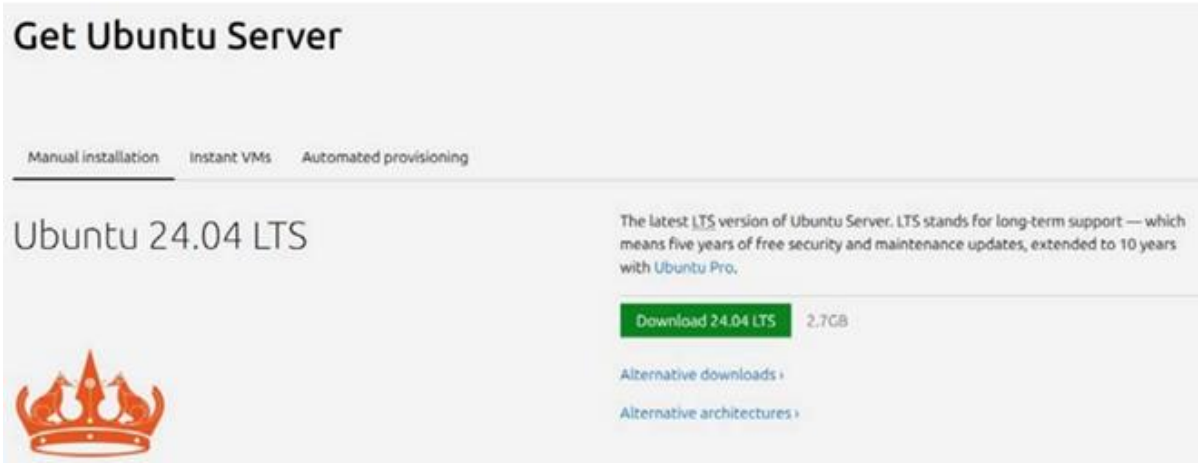

Рисунок 1.9 – Завантаження Ubuntu Server [3]

Хоча macOS Server має меншу частку ринку, ніж Windows Server та Linux Server, він відомий своєю надійністю та безперебійною інтеграцією з екосистемою Apple. Як операційна система на базі Unix, macOS Server дотримується філософії інтуїтивного дизайну GUI Apple. Спочатку підтримуючи як 32-бітні, так і 64-бітні платформи, macOS Server тепер працює виключно на 64-бітних платформах після переходу Apple на процесори Intel. Apple продовжує випускати оновлення та надавати підтримку для macOS Server, підтримуючи його актуальність у спеціалізованих середовищах [3].

Отож, Windows Server – це серверна операційна система, розроблена Microsoft, частина сімейства Windows NT. У серверних середовищах – чи то з використанням Windows Server, Linux Server або macOS Server – основною метою є забезпечення надання системою необхідних послуг для підтримки мережі організації. Однак існують значні відмінності між цими системами щодо процесів розгортання, інтерфейсів користувача, керування ресурсами та обслуговування сервера. Ці відмінності можуть суттєво впливати на загальну ефективність та результативність роботи сервера в корпоративному середовищі.

Протягом майже 30 років, починаючи з ери мас, компанія Microsoft послідовно передбачала та інтегрувала виникаючі потреби в серверному ландшафті. Розвиток Windows Server можна класифікувати за чотирма основними епохами. Перший період, що охоплює 1996-2000 роки, отримав назву «Ера сервера для мас» (англ. Server for the masses era). До цього періоду відносяться операційні системи Windows NT Server 3.5 та Windows NT Server 4.0. Наступний етап, відомий як «Ера підприємства» (англ. Enterprise era), тривав з 2000 по 2008 рік і включав випуску таких систем, як Windows 2000 Server, Windows Server 2003 та Windows Server 2008. Третій етап розвитку, «Ера дата-центру» (англ. Data center era), охоплював період з 2009 по 2013 рік, головним представником якого стала система Windows Server 2012. Сучасний етап розвитку, що розпочався у 2016 році і триває дотепер, визначається як «Хмарна ера» (англ. Cloud era). До цієї епохи належать операційні системи Windows Server 2016, Windows Server 2019, Windows Server 2022 та новітня Windows Server 2025. Ця еволюція демонструє послідовну адаптацію платформи до змінюваних вимог IT-індустрії.

Перед обговоренням конкретних системних вимог важливо розрізняти мінімальні та рекомендовані апаратні специфікації. Мінімальні вимоги дозволяють здійснити базову інсталяцію та експлуатацію серверної ОС, тоді як рекомендовані специфікації забезпечують оптимальну продуктивність та роботу користувача. Розуміння цих вимог є вирішальним для вибору відповідного обладнання, що відповідає передбачуваному використанню та робочим навантаженням. Згідно з публікаціями Microsoft, Windows Server 2025 зберігає вимоги до обладнання, подібні до вимог своїх попередників.

Мінімальні системні вимоги для Windows Server 2025 передбачають наявність 64-

бітного процесора з тактовою частотою 1.4 ГГц. Обсяг оперативної пам’яті (ОЗП) повинен становити щонайменше 512 МБ, однак для варіанту інсталяції з графічним інтерфейсом (Desktop Experience) вимагається 2 ГБ. Для встановлення системи необхідно забезпечити щонайменше 32 ГБ вільного дискового простору. Мережевий адаптер повинен бути сумісним з Ethernet та забезпечувати пропускну здатність щонайменше 1 гігабіт. Графічний пристрій та монітор повинні підтримувати роздільну здатність Super VGA (1024 x 768) або вищу. Також необхідна наявність DVD-приводу (для інсталяцій з фізичних носіїв), клавіатури, миші (або сумісного вказівного пристрою), модуля TPM та доступу до Інтернету [3].

Рекомендовані вимоги до обладнання для забезпечення оптимальної продуктивності є вищими. Рекомендується використання 64-бітного процесора з частотою 2.0 ГГц або вище. Обсяг оперативної пам’яті має становити 32 ГБ або більше. Дискова підсистема повинна включати SSD-накопичувач обсягом 256 ГБ та HDD обсягом 1 ТБ. Вимоги до мережевого адаптера залишаються на рівні щонайменше 1 гігабіт Ethernet NIC. Вимоги до графічної підсистеми та периферійних пристроїв аналогічні мінімальним: підтримка Super VGA (з роширенням 1024 x 768) або вище, наявність засобів введення, TPM та доступу до Інтернету. Розуміння цих вимог дозволяє приймати обґрунтовані рішення щодо інвестицій в обладнання для задоволення потреб розгортання сервера та встановлення на нього мережевої операційної системи [3].

Загальний огляд Windows Server 2025

Операційна система Windows Server 2025 є новітнім випуском у сімействі серверних операційних систем Microsoft Windows NT, який став загальнодоступним станом на листопад 2024 року (рис. 1.10). Анонсована 26 січня 2024 року, Windows Server 2025 знаменує перехід від своїх попередників, таких як Windows Server 2016, 2019 та 2022, які були побудовані на базі Windows 10. Ця нова версія базується на Windows 11, а саме на версії 23H2 з оновленнями жовтня 2023 року. На відміну від Windows 11, Windows Server 2025 не вимагає наявності модуля TPM 2.0 для розгортання, що забезпечує підвищену гнучкість для різноманітних потреб впровадження [3].

У сучасну хмарно-орієнтовану еру серверні операційні системи повинні проектуватися з урахуванням хмарних можливостей. Ця тенденція була започаткована з випуском Windows Server 2016, який компанія Microsoft влучно назвала Windows Server для хмари. Цей фокус лише посилився з наступними випусками, такими як Windows Server 2022, який додатково розширив можливості завдяки покращеній безпеці, гнучкості та надійній підтримці гібридних розгортань, головним чином через інновації у випуску Windows Server 2022 Datacenter Azure. Кожна ітерація, включаючи Windows Server 2019, впроваджувала значні функції, такі як System Insights, інструменти гібридної хмари та посилені заходи

безпеки, наприклад, службу міграції сховища (Storage Migration Service) та підтримку Kubernetes.

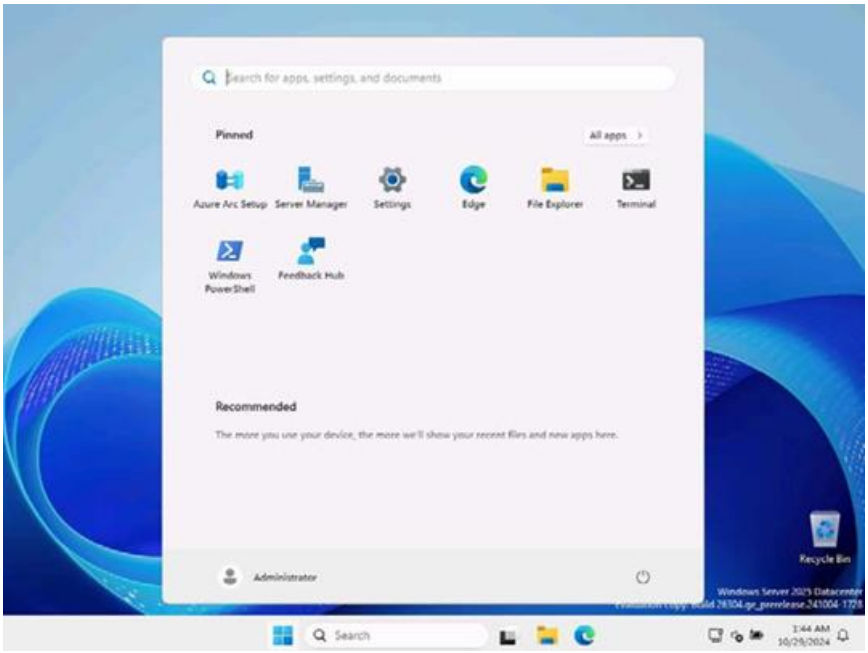

Рисунок 1.10 – Робочий стіл та меню «Пуск» у Windows Server 2025 [3]

Компанія Microsoft послідовно розвивала Windows Server для покращення безпеки, можливостей підключення, інтеграції з Azure, можливостей платформи застосунків, керування сховищем та інших важливих функцій. У сучасному ландшафті, керованому хмарами, Windows Server продовжує відігравати вирішальну роль. Його інтеграція з Microsoft Azure дозволяє безперешкодно керувати гібридними середовищами, надаючи організаціям можливість використовувати як локальні, так і хмарні ресурси. Такі функції, як Windows Admin Center та PowerShell, сприяють ефективному керуванню хмарою, підкреслюючи постійну актуальність Windows Server у світі гібридних хмар.

Базуючись на цьому фундаменті, Windows Server 2025 впроваджує кілька нових функцій, розроблених для задоволення зростаючих вимог сучасних хмарних середовищ. Зокрема, доменні служби Active Directory (AD DS) було вдосконалено завдяки підтримці більшого розміру сторінки бази даних – 32k, що підвищує масштабованість та покращує обробку даних для багатозначних атрибутів. Нові оновлення схеми розширюють функціональність AD, дозволяючи адміністраторам ефективно відновлювати об’єкти з відсутніми основними атрибутами. Крім того, у Windows Server 2025 впроваджено протокол Server Message Block over Quick UDP Internet Connections (SMB over QUIC), який дозволяє протоколу SMB працювати через QUIC, покращуючи продуктивність обміну файлами та безпеку у всіх редакціях. Покращення безпеки в межах AD DS додатково зміцнюють захист мережі, гарантуючи надійну оборону від сучасних загроз [3].

Більше того, Windows Server 2025 є піонером у можливостях гарячого виправлення, що дозволяє безперешкодно застосовувати виправлення безпеки без необхідності перезавантаження сервера. Ця функція мінімізує час простою та підвищує час безперебійної роботи системи, що є критичним для підтримки операційної безперервності. Для використання гарячого виправлення необхідно дотримуватися певних вимог, включаючи використання анклавів безпеки на основі віртуалізації (Virtualization-Based Security – VBS). Анклави VBS забезпечують ізольоване середовище, яке підвищує безпеку, захищаючи критичні процеси від потенційних загроз, гарантуючи, що гаряче виправлення може виконуватися безпечно та ефективно. Використовуючи оптимізації керування на основі штучного інтелекту, Windows Server 2025 пропонує розширені можливості керування, які надають адміністраторам проактивну аналітику та операційну ефективність. Ці досягнення підкреслюють відданість Microsoft створенню серверної ОС, яка встановлює нові стандарти продуктивності, безпеки та керованості в сучасних IT-ландшафтах, зміцнюючи її позицію на передовій інновацій хмарних обчислень.

Слід зазначити, що на відміну від засобів віддаленого адміністрування сервера (RSAT), які покладаються на традиційні методи, Windows Admin Center є сучасною платформою керування сервером, побудованою на веб-технологіях. Вона пропонує більш оптимізований та зручний для користувача досвід з інтерфейсом, що нагадує Azure, забезпечуючи безперешкодну навігацію для адміністраторів, знайомих із хмарними середовищами. Windows Admin Center надає повний набір інструментів для ефективного керування серверами та інфраструктурою. Після інсталяції Windows Server 2025 автоматично з’являється діалогове вікно Windows Admin Center, що надає користувачам безкоштовний доступ до цього потужного інтерфейсу керування, додатково спрощуючи завдання адміністрування сервера. Його можна завантажити з офіційного веб-сайту Microsoft [3].

Операційна система Windows Server 2025 доступна в різних редакціях, кожна з яких розроблена для задоволення конкретних вимог організації. Основні редакції включають Datacenter Edition, Standard Edition, Azure Edition та Annual Channel for Container Host.

Редакція Datacenter Edition ідеально підходить для широкого використання віртуалізації та хмарних середовищ. Вона пропонує необмежену кількість віртуальних екземплярів та ряд розширених функцій, при цьому для підвищення безпеки та продуктивності вимагаються анклави VBS.

Версія Standard Edition адаптована для менших організацій з меншою кількістю віртуальних екземплярів і включає всі основні серверні функції, необхідні для ефективної роботи; для цієї редакції також рекомендуються анклави VBS для забезпечення надійної безпеки.

Редакція Azure Edition призначена виключно для оцінки віртуальних машин у межах

Azure, дозволяючи організаціям тестувати та оцінювати можливості системи в хмарі, використовуючи анклави VBS для забезпечення безпечного середовища оцінювання.

А версія Annual Channel for Container Host фокусується на контейнерних робочих навантаженнях, забезпечуючи ефективне розгортання та керування контейнеризованими додатками, де анклави VBS підтримують безпечні та ізольовані контейнерні середовища.

Ці чотири редакції чітко окреслюють варіанти, доступні в межах Windows Server 2025, кожна з яких задовольняє різні потреби та випадки використання.

Основні відмінності між Windows Server 2025 і Windows Server 2022

У сучасному технологічному середовищі, що стрімко розвивається, нові продукти часто спочатку сприймаються лише як поступові оновлення своїх попередників. Таке твердження на перший погляд може стосуватися і Windows Server 2025, натякаючи лише на поверхневі покращення порівняно з Windows Server 2022. Проте, при детальному розгляді Windows Server 2025 виявляються суттєві вдосконалення та нові функції. При порівнянні Windows Server 2025 з попередником, Windows Server 2022, стають очевидними кілька помітних досягнень і вдосконалень.

Стосовно вдосконалень доменних служб Active Directory (AD DS), у Windows Server 2025 запроваджується збільшений розмір сторінки бази даних – 32k для AD, що підвищує масштабованість. Нові оновлення схеми розширюють функціональність AD, а адміністратори підприємства отримують можливість відновлювати об’єкти з відсутніми основними атрибутами. Натомість у Windows Server 2022 основна увага приділялася покращенню керування AD та гнучкості схеми. У контексті протоколу SMB over QUIC, у Windows Server 2025 цей протокол тепер може бути налаштований у всіх редакціях з використанням QUIC, що підвищує продуктивність обміну файлами та безпеку, тоді як у Windows Server 2022 було впроваджено лише початкову підтримку SMB over QUIC [3].

Щодо покращень безпеки, Windows Server 2025 включає цілісність коду на основі гіпервізора, вдосконалений сервер із захищеним ядром та апаратний захист стеку. Стандартна підтримка TLS 1.3 покращує мережеву безпеку. Водночас Windows Server 2022 характеризувався покращеннями протоколів безпеки, включаючи Secured-core Server та розширену підтримку TLS. Розглядаючи підтримку гарячого виправлення, у Windows Server 2025 реалізовано можливості гарячого виправлення, що дозволяє здійснювати безперебійні оновлення без простоїв, на відміну від Windows Server 2022, де продовжувалася підтримка надійних інструментів керування оновленнями.

У сфері керування на основі штучного інтелекту Windows Server 2025 пропонує розширені можливості керування з оптимізаціями на основі ШІ, тоді як у Windows Server 2022 були представлені початкові інструменти керування на основі ШІ. Щодо гнучкості

платформи, Windows Server 2025 зосереджується на динамічній маршрутизації та покращеному керуванні обліковими записами служб. У Windows Server 2022 було впроваджено динамічну маршрутизацію джерела (DSR) та вдосконалення у віртуалізованих часових поясах.

Вдосконалення Windows Admin Center у Windows Server 2025 включають розширені можливості керування, зокрема автоматизоване керування життєвим циклом розширень та налаштовувані перегляди інформації про віртуальні машини, тоді як Windows Server 2022 підтримував вдосконалені інструменти Windows Admin Center. Підтримка Kubernetes у Windows Server 2025 покращується для середовищ Kubernetes завдяки досягненням у керуванні контейнерами, тоді як Windows Server 2022 забезпечував початкову підтримку Kubernetes та вдосконалення оркестрації контейнерів.

Варто зазначити, що гаряче виправлення вимагає підключення Azure Arc, яке забезпечує інтеграцію локальних серверів із сервісами Azure. До інших залежностей належать Azure Update Management для гарантування ефективного керування та розгортання оновлень, сумісність із конкретними ролями та функціями сервера (оскільки не всі ролі можуть підтримувати гаряче виправлення на початковому етапі, тому необхідно перевіряти сумісність), а також наявність достатніх системних ресурсів для забезпечення адекватності апаратних та мережевих ресурсів для обробки процесів гарячого виправлення [3].

Розуміння цих відмінностей між Windows Server 2025 та Windows Server 2022 допоможе визначити, яка версія найкраще відповідає наявним потребам при розгортанні мережевої серверної інфраструктури та адмініструванні серверів і комп’ютерних мереж.

Тема 2
Віртуалізація та серверні середовища

Концепція віртуалізації

Віртуалізація визначається як технологія, що може бути використана для створення віртуальних представлень серверів, сховищ, мереж та інших фізичних пристроїв. Віртуальне програмне забезпечення емулює функціональність фізичного обладнання для одночасного запуску віртуальних машин на одній фізичній машині. Підприємства використовують віртуалізацію для ефективного використання апаратних ресурсів та отримання додаткового прибутку від своїх інвестицій. Також ця технологія забезпечує надання послуг хмарних обчислень, що допомагають організаціям ефективно керувати своєю архітектурою.

Важливість віртуалізації зумовлена можливістю взаємодіяти з будь-яким апаратним ресурсом із більшою гнучкістю. Фізичні сервери споживають електроенергію, займають місце для зберігання та вимагають технічного обслуговування. Доступ до них часто обмежується фізичною близькістю та проектом мережі. Віртуалізація дозволяє усунути всі ці обмеження шляхом абстрагування функціональності фізичного обладнання у програмне забезпечення. Існує можливість здійснювати моніторинг, технічне обслуговування та використання апаратної інфраструктури як веб-додатка.

Для належного розуміння віртуальної машини на основі ядра (KVM) спочатку необхідно зрозуміти деякі базові поняття віртуалізації. Отож, віртуалізація – це процес, який дозволяє комп’ютеру спільно використовувати свої апаратні ресурси з кількома цифрове відокремленими середовищами. Кожне віртуалізоване середовище функціонує в межах виділених ресурсів, таких як пам’ять, обчислювальна потужність та сховище. Завдяки віртуалізації організації можуть перемикатися між різними операційними системами на одному сервері без перезавантаження [3].

Віртуальні машини та гіпервізори є двома важливими концепціями віртуалізації. Віртуальна машина визначається як програмно-визначений комп’ютер, що працює на фізичному комп’ютері з окремою операційною системою та обчислювальними ресурсами. Фізичний комп’ютер називається хост-машиною, а віртуальні машини називаються гостьовими машинами. На одній фізичній машині може працювати кілька віртуальних машин. Віртуальні машини абстрагуються від комп’ютерного обладнання за допомогою гіпервізора.

Огляд гіпервізорів

Гіпервізор – це програмний компонент, що здійснює керування декількома віртуальними машинами на комп’ютері. Цей механізм гарантує, що кожна віртуальна машина отримує виділені їй ресурси та не створює перешкод для функціонування інших віртуальних

машин. Гіпервізор являє собою програмне забезпечення для віртуалізації, яке інсталюється на обчислювальні системи. Він виступає як програмний шар, що виконує роль посередника між віртуальними машинами та базовим апаратним забезпеченням або операційною системою хоста. Гіпервізори координують доступ до фізичного середовища таким чином, щоб декілька віртуальних машин мали доступ до власної частки фізичних ресурсів. Для прикладу, якщо віртуальна машина потребує обчислювальних ресурсів, таких як процесорна потужність комп'ютера, запит спочатку надсилається до гіпервізора. Після цього гіпервізор перенаправляє запит до базового апаратного забезпечення, яке виконує поставлене завдання. Існує два основних типи гіпервізорів [3].

Гіпервізори першого типу, також відомі як гіпервізори без операційної системи (також «рідні» гіпервізори) є програмами-гіпервізорами, які встановлюються безпосередньо на апаратне забезпечення комп'ютера, а не на операційну систему (рис. 2.1). Внаслідок такої архітектури гіпервізори першого типу характеризуються вищою. Гіпервізор першого типу зазвичай використовується для віртуалізації сервера. Наприклад, вони використовуються в центрах обробки даних та хмарних обчисленнях. Він працює безпосередньо на апаратному забезпеченні хоста і керує розподілом системних ресурсів між віртуальними операційними системами. Приклади гіпервізорів типу 1 включають VMware vSphere/ESxi, Xen і Oracle VM Server.

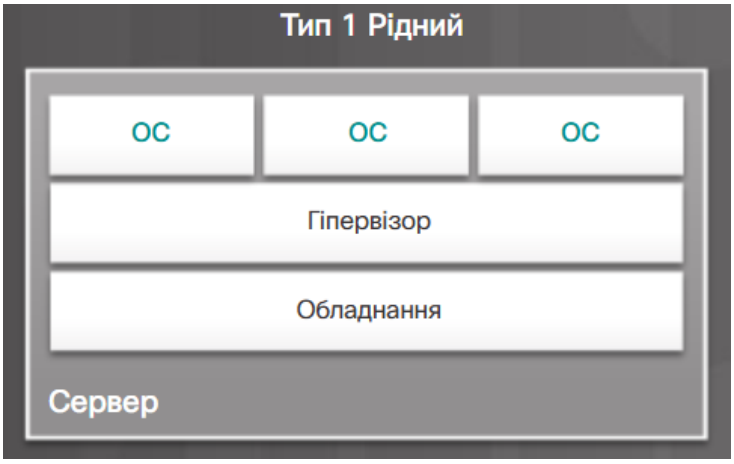

Рисунок 2.1 – Гіпервізор першого типу [16]

Гіпервізори другого типу функціонують як прикладне програмне забезпечення (додаток) на комп'ютерному обладнанні, що вже має встановлену операційну систему (рис. 2.2). Гіпервізори другого типу вважаються придатними для забезпечення обчислювальних потреб кінцевих користувачів. Гіпервізори другого типу, такі як VMware Workstation працюють з хост-комп'ютером для створення та використання кількох віртуальних машин. Гіпервізори типу 2 включають VMware Workstation, Windows Hyper-V, and Oracle VirtualBox.

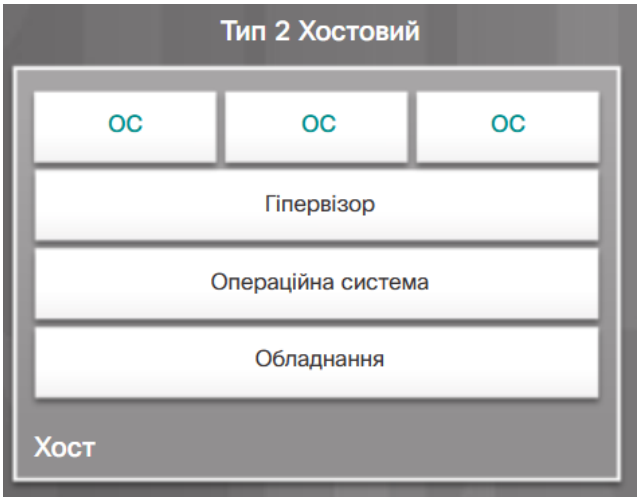

Рисунок 2.2 – Гіпервізор другого типу [16]

Створення віртуальних машин

Процес розгортання віртуалізації та створення віртаульних машин, з використанням гіпервізора другого типу Hyper-V, починається з активації відповідних компонентів операційної системи Windows. Для увімкнення Hyper-V у середовищі Windows використовуються такі інструменти, як PowerShell або інструмент обслуговування та керування образами розгортання (DISM). При використанні PowerShell необхідно ініціювати запуск оболонки з правами адміністратора, оскільки без цих привілеїв виконання команд буде неможливим. На робочому столі Windows здійснюється пошук Windows PowerShell через меню «Пуск», після чого через контекстне меню обирається опція «Запуск від імені адміністратора». Далі виконується команда Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V –All (рис. 2.3). Для завершення інсталяції та застосування змін необхідно ввести символ Y для перезавантаження комп’ютера [14].

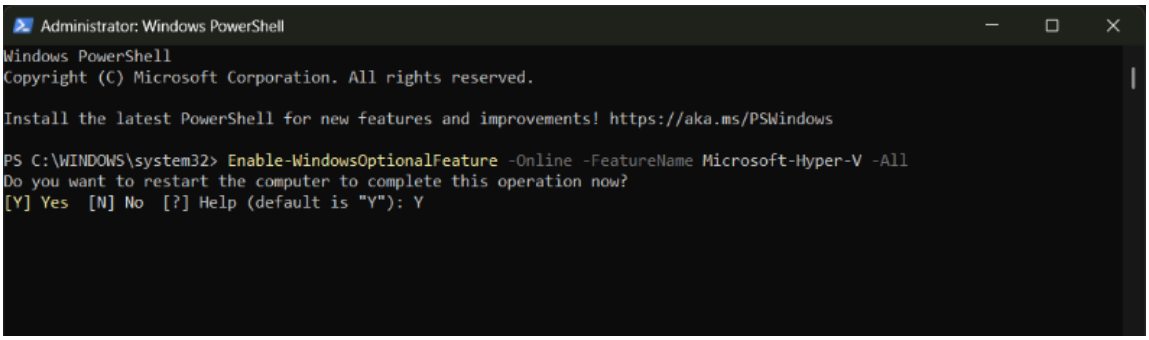

Рисунок 2.3 – Команда Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V –All [14]

Альтернативним методом є використання інструменту DISM, який дозволяє налаштовувати образи Windows та вмикати функції під час роботи операційної системи. Аналогічно до попереднього методу, запускається Windows PowerShell із правами

адміністратора, після чого вводиться команда DISM /Online /Enable-Feature /All /FeatureName:Microsoft-Hyper-V. Успішне виконання операції підтверджується відповідним повідомленням у консолі.

Перед початком процесу створення віртуальної машини необхідно переконатися у відповідності системи певним вимогам. Комп'ютер повинен працювати під керуванням Windows Server або клієнтської версії Windows із вже активованою роллю Hyper-V. Користувач повинен мати членство в групі локальних адміністраторів або спеціалізованій групі «Адміністратори Hyper-V». Крім того, хост-система повинна мати достатній обсяг фізичної оперативної пам'яті для виділення віртуальній машині, а також достатній простір на дисковому накопичувачі для розміщення файлів конфігурації та віртуальних жорстких дисків. До необов'язкових, але рекомендованих умов належать наявність налаштованого віртуального комутатора для забезпечення мережевого підключення, а також наявність інсталяційного носія операційної системи (файлу .iso) або існуючого віртуального жорсткого диска (.vhd або .vhdx) [14].

Створення віртуальної машини може бути реалізовано за допомогою Диспетчера Hyper-V (Hyper-V Manager) або PowerShell. При використанні графічного інтерфейсу Диспетчера Hyper-V, який можна знайти через меню «Пуск», необхідно переконатися, що роль Hyper-V встановлена. У лівій області інтерфейсу обирається цільовий сервер, після чого на панелі «Дії» обирається пункт «Створити», а потім – «Віртуальна машина», що ініціює запуск «Майстра створення віртуальної машини».

На етапі «Вказати ім'я та розташування» вводиться ідентифікатор віртуальної машини та, за необхідності, змінюється місце зберігання файлів конфігурації шляхом встановлення прапорця «Зберігати віртуальну машину в іншому місці» та вибору відповідної папки (рис. 2.4).

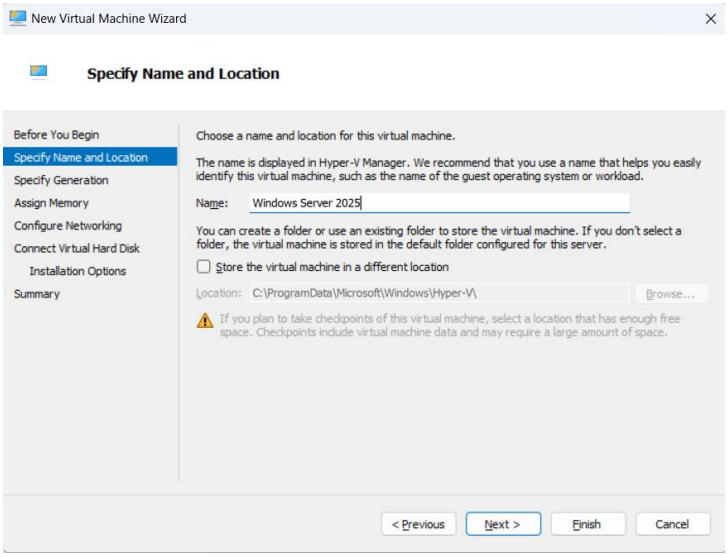

Рисунок 2.4 – Надання імені віртуальній машині та вибір місця зберігання [14]

Наступним кроком є вибір покоління віртуальної машини на сторінці «Вказати покоління». Рекомендується створення віртуальної машини покоління 2, якщо відсутні специфічні причини для використання покоління 1.

Процес конфігурації продовжується на сторінці «Призначити пам’ять», де визначається обсяг оперативної пам’яті, що виділяється при запуску. Існує можливість використання динамічної пам’яті, при цьому мінімальний обсяг становить 32 МБ, а максимальний обмежений ресурсами системи. На сторінці «Налаштування мережі» обирається віртуальний комутатор для інтеграції машини в мережу; цей крок можна пропустити та виконати налаштування пізніше.

На етапі «Підключення віртуального жорсткого диска» пропонуються варіанти: створення нового диска із зазначенням імені, розташування та розміру; використання існуючого диска (.vhd або .vhdx); або відкладення підключення диска на майбутнє (рис. 2.5).

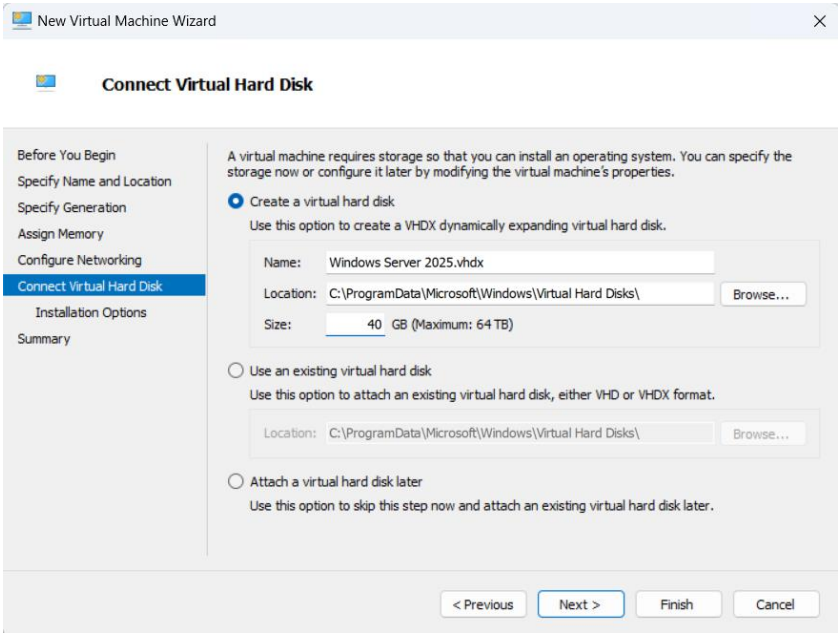

Рисунок 2.5 – Підключення віртуального жорсткого диска [14]

Завершальним етапом конфігурації є «Параметри інсталяції», де обирається джерело для встановлення операційної системи: інсталяція пізніше, використання файлу завантажувального образу (.iso), використання фізичного дисководу, або інсталяція з мережевого сервера. Після перевірки всіх параметрів на сторінці «Підсумок» процес завершується натисканням кнопки «Готово» (рис. 2.6).

Після завершення створення віртуальної машини виконується її запуск та підключення. У Диспетчері Hyper-V необхідно натиснути правою кнопкою миші на створену віртуальну машину та вибрати опцію «Підключитися...». У вікні підключення, що відкриється, для ініціалізації роботи системи обирається послідовність «Дія» та «Запустити».

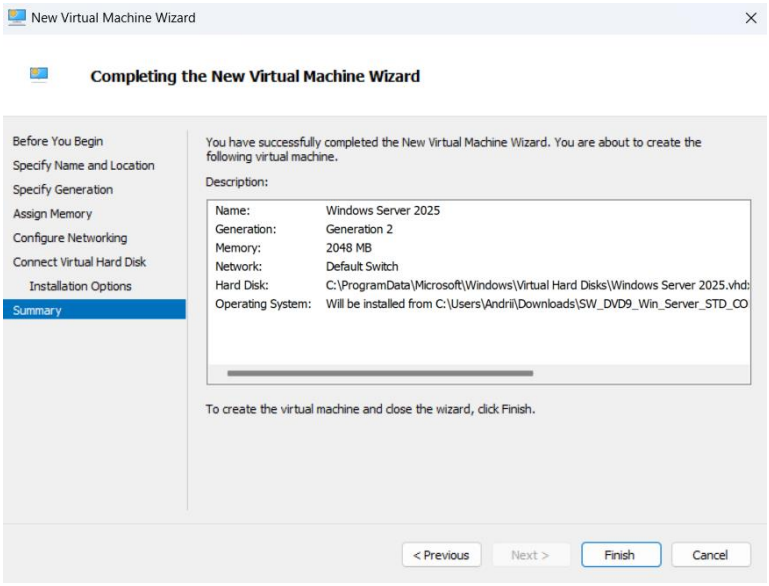

Рисунок 2.6 – Перевірка всіх параметрів на сторінці «Підсумок» [14]

Розуміння основ віртуалізації у Windows Server 2025

Віртуалізація у Windows Server 2025 визначається як трансформаційна технологія, що дозволяє створювати та експлуатувати декілька віртуальних машин (ВМ) на одному фізичному сервері або мережі взаємопов'язаних серверів, відомій як кластер. Кожна ВМ діє як незалежний комп'ютер, укомплектований власною операційною системою, додатками та виділеними ресурсами, функціонуючи ізольовано від інших ВМ. Ця технологія також поширюється на віртуалізацію пристроїв зберігання даних та мережевих ресурсів, що підвищує гнучкість та ефективність віртуалізованого середовища. Завдяки консолідації робочих навантажень на меншій кількості фізичних серверів, віртуалізація здатна суттєво зменшити витрати на обладнання, знизити енергоспоживання та мінімізувати фізичний простір, необхідний для дата-центрів [3].

Операційна система Windows Server 2025 включає Hyper-V – потужну функцію віртуалізації, яка забезпечує ефективне розгортання та керування ВМ як на клієнтських системах Windows, так і в серверних середовищах. Hyper-V, наступник раннього Windows Virtual PC, еволюціонував з моменту свого заснування у Windows Server 2008, ставши широко прийнятою та високо оціненою платформою серед системних адміністраторів. Його надійний набір служб та інструментів підтримує створення, конфігурацію та адміністрування ВМ, надаючи комплексне рішення для керування віртуальними середовищами [16].

Основа хмарної інфраструктури полягає в тому, що Hyper-V сприяє створенню та керуванню ВМ на фізичному сервері, забезпечуючи ефективне використання ресурсів. Ця здатність до віртуалізації є важливою для хмарних середовищ, де ресурси повинні динамічно розподілятися для задоволення змінних робочих навантажень. Опановуючи Hyper-V, IT-фахівці можуть використовувати цю технологію для створення масштабованих, гнучких хмарних інфраструктур.

Інтеграція з Microsoft Azure є ще одним ключовим аспектом, оскільки Microsoft Azure, одна з провідних хмарних платформ, значною мірою спирається на принципи віртуалізації, подібні до тих, що використовуються в Hyper-V. Розуміння Hyper-V дозволяє фахівцям безперешкодно переносити свої навички локальної віртуалізації в Azure, де вони можуть розгортати віртуальні машини Azure (Azure Virtual Machines) та використовувати такі функції, як Azure Site Recovery для аварійного відновлення. Ця обізнаність сприяє більш плавному процесу міграції та покращує загальні можливості керування хмарою [3].

Віртуалізація дозволяє забезпечити роботу декількох операційних систем (ОС) на одному фізичному сервері або в кластері серверів шляхом використання різних режимів. Кожен режим пропонує відмінні функції та переваги, адаптовані до різних потреб у віртуалізованих середовищах.

Режим повної віртуалізації (Fully Virtualized Mode) передбачає, що кожна ОС працює у власному ізольованому та безпечному віртуальному середовищі, ніби вона знаходиться на окремій фізичній машині. Шар віртуалізації, або гіпервізор, керує ресурсами хост-сервера та розподіляє їх для кожної ВМ. Цей підхід забезпечує надійну ізоляцію між ВМ, гарантуючи, що вони можуть працювати незалежно, не змінюючи своїх конфігурацій. Повністю віртуалізовані середовища ідеально підходять для сценаріїв, що вимагають надійної безпеки та розділення, оскільки гостьові ОС залишаються необізнаними про базову інфраструктуру віртуалізації. Рисунок 2.7 ілюструє, як Windows Server 2025 функціонує в такому ізольованому середовищі, підкреслюючи розділення ресурсів та процесів між різними ВМ.

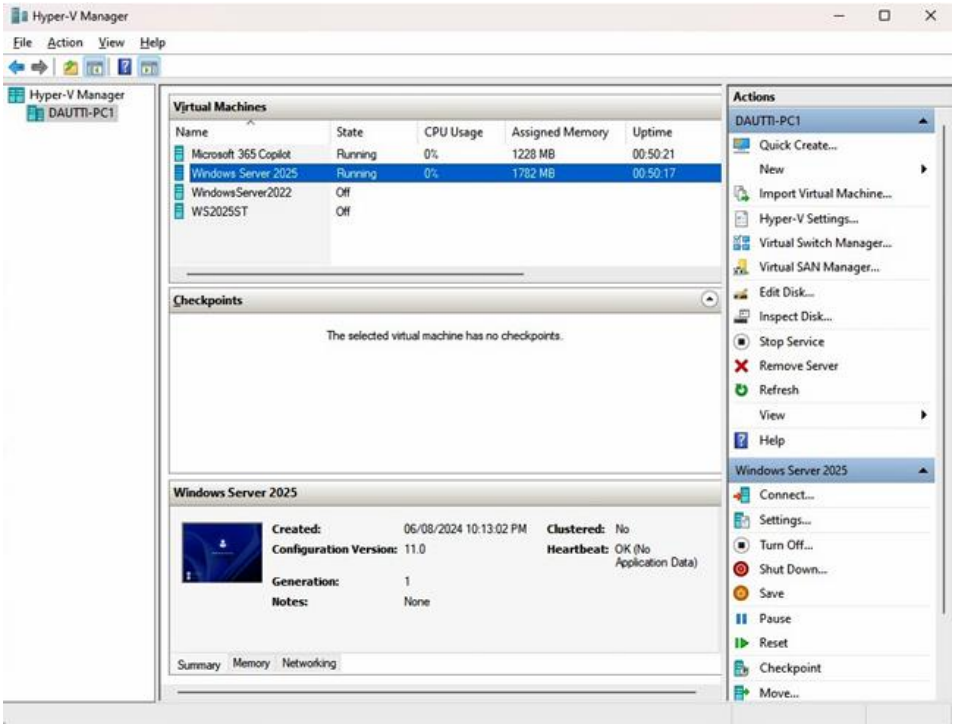

Рисунок 2.7 – Windows Server 2025, що працює в ізольованому та безпечному віртуальному середовищі [3]

Режим паравіртуалізації (Paravirtualized Mode) пропонує більш інтегрований підхід, дозволяючи гостьовій ОС безпосередньо спілкуватися з гіпервізором. На відміну від режиму повної віртуалізації, де гостьова ОС не знає про шар віртуалізації, паравіртуалізовані системи вимагають модифікації гостьової ОС для ефективної взаємодії з гіпервізором. Цей режим використовує інтерфейс прикладного програмування (API) для забезпечення прямого зв'язку, що зменшує накладні витрати, зазвичай пов'язані з емуляцією обладнання. Результатом є значне підвищення продуктивності та використання ресурсів, що робить його переконливим вибором для середовищ, де ефективність та швидкість мають першорядне значення [3].

Режим контейнеризації (Containerization Mode) фокусується на інкапсуляції додатків разом з їхніми середовищами виконання, системними інструментами та налаштуваннями в самодостатні одиниці, відомі як контейнери. На відміну від ВМ, які віртуалізують цілі операційні системи, контейнери віртуалізують на рівні додатків, забезпечуючи легке та портативне рішення. Кожен контейнер працює незалежно, але використовує спільне ядро хост-ОС, що робить його ефективним вибором для розгортання та керування додатками в різних середовищах. Контейнери підвищують масштабованість, оптимізують розгортання додатків та забезпечують узгодженість, упаковуючи всі необхідні компоненти разом. Цей підхід є особливо корисним для розробки, тестування та послідовного розгортання додатків на різних платформах [3].

Варто зазначити, що фізичний сервер працює з операційною системою, відомою як хост-ОС, яка керує апаратними ресурсами сервера. Натомість, ВМ запускає операційну систему, що називається гостьовою ОС, яка працює у віртуальному середовищі, створеному хост-ОС або гіпервізором. Наприклад, у певній конфігурації ноутбук може бути обладнаний Windows 11 Pro як хост-ОС, тоді як ВМ на тій самій машині запускає Windows Server 2025 Standard як гостьову ОС. Хост-ОС відіграє критичну роль у розподілі та контролі апаратних ресурсів, дозволяючи гостьовій ОС безперешкодно функціонувати у віртуалізованому середовищі.

У віртуалізації продуктивність є критичним фактором, який може суттєво впливати на ефективність розгорнутих ВМ. Розуміння впливу різних типів сховищ та конфігурацій інфраструктури є важливим для оптимізації продуктивності ВМ.

При проектуванні віртуалізованого середовища розуміння відмінностей між мережами зберігання даних (SAN) та локальними дисками є вирішальним, оскільки кожне рішення для зберігання представляє унікальні характеристики продуктивності та наслідки для операцій ВМ.

Мережі зберігання даних (SAN) забезпечують централізоване рішення для зберігання, яке дозволяє декільком серверам отримувати доступ до спільного пулу ресурсів зберігання. Хоча SAN пропонують такі переваги, як висока доступність та масштабованість, вони

можуть вносити затримку, що впливає на продуктивність. Ця затримка виникає через мережеві накладні витрати, оскільки дані повинні проходити через мережеву фабрику, щоб досягти масиву зберігання. У середовищах з високим попитом, де швидкий доступ до даних є критичним, ця затримка може призвести до повільнішої продуктивності ВМ, особливо для додатків з інтенсивним вводом-виводом.

Натомість, локальні диски безпосередньо підключені до фізичного сервера, що розміщує ВМ. Ця конфігурація зазвичай забезпечує меншу затримку, оскільки даним не потрібно проходити через мережу. Локальне сховище ідеально підходить для додатків, що вимагають швидкого доступу до даних та високої пропускної здатності, таких як бази даних та системи обробки транзакцій. Однак локальні диски обмежують надлишковість та масштабованість порівняно з SAN, що робить їх менш придатними для великих віртуалізованих середовищ.

Гіперконвергентна інфраструктура (HCI) інтегрує обчислення, зберігання та мережі в єдине програмно-кероване рішення, пропонуючи уніфікований підхід до віртуалізації. HCI може підвищити продуктивність кількома способами. По-перше, покращена локальність даних досягається шляхом використання локального сховища в кожному вузлі кластера HCI, що значно скорочує час доступу до даних. Ця локальність мінімізує затримку, забезпечуючи швидшу продуктивність ВМ, особливо для додатків з високими вимогами до вводу-виводу. По-друге, масштабованість та еластичність дозволяють організаціям безперешкодно масштабувати свої ресурси. Зі зростанням попиту до кластера можна додавати додаткові вузли, ефективно розподіляючи робочі навантаження та підвищуючи продуктивність без шкоди для цілісності системи зберігання. По-третє, інтелектуальне керування ресурсами реалізується у багатьох рішеннях HCI, які включають передову аналітику та функції керування ресурсами, що оптимізують розміщення робочих навантажень на основі метрик продуктивності. Ця здатність гарантує, що ВМ розподіляються на найбільш відповідні ресурси, додатково підвищуючи загальну продуктивність [3].

Вибір типу сховища – чи то SAN, чи локальні диски – безпосередньо впливає на продуктивність віртуалізованих середовищ. Крім того, використання HCI може надати значні переваги в ефективному керуванні ресурсами та забезпеченні оптимальної продуктивності для ВМ. Розуміння цих режимів віртуалізації дозволяє обрати найбільш відповідний метод для інфраструктури залежно від вимог до продуктивності, безпеки та масштабованості.

Додавання та налаштування ролі Hyper-V у Windows Server 2025

Значною перевагою серверної віртуалізації є здатність запускати декілька віртуальних машин на одному фізичному сервері, максимізуючи при цьому продуктивність та ефективність використання ресурсів. Hyper-V дозволяє безперешкодно створювати, керувати

та експлуатувати ВМ у середовищі Windows Server 2025.

Для повного розуміння архітектури Hyper-V доцільно представити її як деревоподібну структуру, де гіпервізор діє як корінь і глибоко інтегрований у фундамент апаратного забезпечення, що слугує ґрунтом. Гіпервізор є фундаментальним компонентом віртуальної платформи Hyper-V, маючи прямий доступ до апаратних ресурсів фізичного сервера, включаючи центральний процесор, пам’ять, сховище та мережеві ресурси. Цей прямий контроль дозволяє гіпервізору ефективно керувати цими ресурсами та розподіляти їх між декількома ВМ [13].

З гіпервізора розгалужуються окремі середовища виконання, відомі як розділи. Кожен розділ є ізольованим, що означає його незалежне функціонування без втручання з боку інших. Така ізоляція є критично важливою для безпеки та стабільності, оскільки вона гарантує, що проблема в одному розділі не вплине на інші. Самі розділи не мають прямого доступу до фізичного обладнання; натомість вони взаємодіють із віртуалізованим шаром, що надається гіпервізором або кореневим розділом. Цей віртуалізований шар абстрагує апаратне забезпечення, надаючи гостьовим операційним системам узгоджене та кероване середовище для роботи.

Кореневий розділ (root) є першим і найбільш привілейованим розділом, у якому працюють як хост-операційна система, так і роль Hyper-V. Він діє як центральний вузол, керуючи взаємодією з апаратним забезпеченням та наглядаючи за створенням і роботою інших розділів, відомих як дочірні розділи. Ці дочірні розділи розміщують гостьові операційні системи, які можуть включати різні версії Windows або Linux, забезпечуючи різноманітне та гнучке обчислювальне середовище. Зв’язок між кореневим і дочірніми розділами забезпечується спеціалізованими компонентами, відомими як Постачальник послуг віртуалізації (Virtualization Service Provider – VSP) та Споживач послуг віртуалізації (Virtualization Service Consumer – VSC), як проілюстровано на рисунку 2.8.

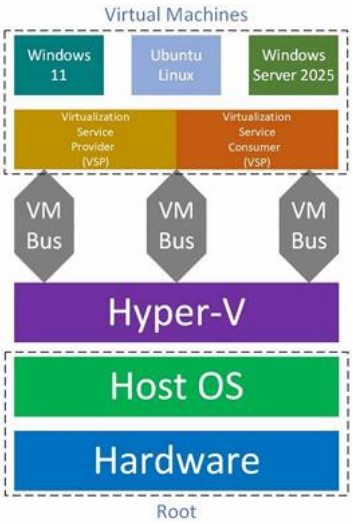

Рисунок 2.8 – Архітектура Hyper-V [13]

Ці компоненти використовують логічний канал зв'язку, що називається Шиною віртуальної машини (Virtual Machine Bus – VMBus), для ефективного обміну даними та командами. Така схема гарантує, що гостьові операційні системи в дочірніх розділах можуть виконувати необхідні операції, такі як доступ до сховища або мережевих ресурсів, без прямого доступу до апаратного забезпечення. Розуміння цієї архітектури є ключовим для оцінки того, як Hyper-V підтримує різні типи віртуалізації, включаючи повну віртуалізацію, де гостьова операційна система працює без змін у віртуальному середовищі. Ця можливість є критичною для сценаріїв, що вимагають сумісності та мінімальної модифікації існуючого програмного забезпечення. Однак перед розгортанням Hyper-V необхідно ознайомитися зі специфічними апаратними та програмними вимогами, а також передумовами для забезпечення успішної реалізації та оптимальної продуктивності [13].

Перед інсталяцією та використанням Hyper-V критично важливо переконатися, що сервер відповідає специфічним передумовам, необхідним для активації гіпервізора. Основною вимогою є підтримка сервером віртуалізації на апаратному рівні, що є основою функціональності Hyper-V. Це передбачає наявність процесора з увімкненою технологією віртуалізації, такою як Intel VT-x або AMD-V [3].

Ці технології є важливими, оскільки дозволяють процесору ефективно керувати декількома ВМ, динамічно та безпечно розподіляючи ресурси без значних накладних витрат. Окрім підтримки віртуалізації, сервер також повинен мати увімкнені інші функції, такі як запобігання виконанню даних (Data Execution Prevention – DEP), що забезпечує додатковий рівень безпеки, запобігаючи виконанню шкідливого коду в захищених областях пам'яті. Крім того, прошивка BIOS або UEFI сервера повинна бути налаштована коректно для підтримки цих технологій, з увімкненими опціями віртуалізації.

Ще одним важливим фактором є вкладена віртуалізація, особливо в середовищах, де планується запуск Hyper-V всередині ВМ. Ця розширена функція дозволяє створювати віртуальні середовища всередині ВМ, забезпечуючи гнучкість для тестування, розробки та навчальних сценаріїв без потреби в додатковому фізичному обладнанні. Окрім цих апаратних вимог, також важливо переконатися, що операційна система є сумісною з Hyper-V. Наприклад, Hyper-V доступний лише в певних редакціях Windows Server та клієнтських операційних систем Windows, таких як Windows 11 Pro або Enterprise. Забезпечення відповідності сервера цим умовам є ключовим для досягнення плавного та ефективного розгортання Hyper-V, що дозволяє повною мірою використовувати переваги віртуалізації в IT-середовищі [3].

Вкладена віртуалізація визначається як розширена функція, що дозволяє запускати ВМ всередині іншої ВМ. По суті, це означає, що апаратне забезпечення хост-машини здатне запускати Hyper-V всередині гостьової операційної системи, дозволяючи гостьовій ОС

створювати та керувати додатковими ВМ так само, якби вона працювала безпосередньо на фізичному обладнанні. Ця можливість, хоча спочатку може здаватися теоретичною, підтримується компанією Microsoft починаючи з Windows Server 2016 і стала неоціненним інструментом у різних сценаріях, таких як тестування складних конфігурацій, навчальні середовища або запуск віртуальних лабораторій, де потрібні кілька рівнів віртуалізації. Простіше кажучи, вкладена віртуалізація дозволяє розглядати гостьову операційну систему так, ніби вона є хост-операційною системою, запускаючи Hyper-V і створюючи віртуалізоване середовище всередині вже віртуалізованого середовища. Таке вкладене налаштування може бути особливо корисним для сценаріїв, що вимагають декількох ізольованих середовищ, або для розробників та IT-фахівців, яким необхідно тестувати розгортання та конфігурації безпечним і контрольованим чином.

Налаштування вкладеної віртуалізації у Windows Server 2025 виконується безпосередньо за допомогою Windows PowerShell. Спочатку через контекстне меню кнопки «Пуск» обирається Windows PowerShell (з правами адмінічтратора). У вікні PowerShell виконується така команда: Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true. Ця команда дозволяє гостьовій ВМ надавати необхідні розширення віртуалізації, дозволяючи їй запускати Hyper-V. Наступна команда: Get-VMNetworkAdapter -VMName <VMName> | Set-VMNetworkAdapter -MacAddressSpoofing On вмикає підміну MAC-адреси (MAC address spoofing) на мережевому адаптері ВМ, що є необхідним для функціонування мережі в сценарії вкладеної віртуалізації. Після виконання цих конфігурацій можна переходити до інсталяції Hyper-V всередині гостьової ВМ, дотримуючись інструкцій, які розглядають інсталяцію Hyper-V на Windows Server 2025 [13].

Ознайомлення з диспетчером Hyper-V для адміністрування віртуальних машин

Диспетчер Hyper-V (Hyper-V Manager) – це універсальний та важливий інструмент для адміністрування віртуальних машин у середовищі Windows Server 2025. Він забезпечує централізований інтерфейс для керування різноманітними завданнями, пов’язаними з ВМ, оптимізуючи адміністрування віртуалізованих ресурсів [3].

За допомогою Диспетчера Hyper-V виконується ефективне створення нових ВМ, імпорт існуючих та видалення тих, що більше не потрібні, що забезпечує гнучкість у керуванні віртуальною інфраструктурою. Інструмент також дозволяє налаштовувати та керувати віртуальними комутаторами, які є критично важливими для підключення ВМ до мережі та забезпечення їх ефективної взаємодії з іншими мережевими ресурсами. Додатково Диспетчер Hyper-V сприяє створенню менеджера мережі зберігання даних (SAN), що дозволяє ВМ підключатися до рішень спільного зберігання. Ця можливість є життєво важливою для підтримання високої доступності та продуктивності у віртуальному

середовищі. Крім того, Диспетчер Hyper-V включає функції для інспекції та оптимізації віртуальних дисків, дозволяючи регулювати розподіл дискового простору та покращувати продуктивність відповідно до вимог. Також здійснюється керування станом ВМ шляхом їх зупинки або вимкнення, що є корисним для цілей обслуговування та усунення несправностей.

Інтерфейс Диспетчера Hyper-V у Windows Server 2025 організований у п’ять основних секцій: панель серверів, що відображає список серверів; панель ВМ, що показує ВМ на вибраному сервері; панель контрольних точок, яка надає доступ до контрольних точок ВМ для відновлення станів; деталі вибраної ВМ, що пропонують інформацію та налаштування для поточної вибраної ВМ; та панель дій, яка надає доступ до різних управлінських дій (рис. 2.9). Кожен із цих компонентів відіграє вирішальну роль у ефективному керуванні та конфігурації віртуального середовища.

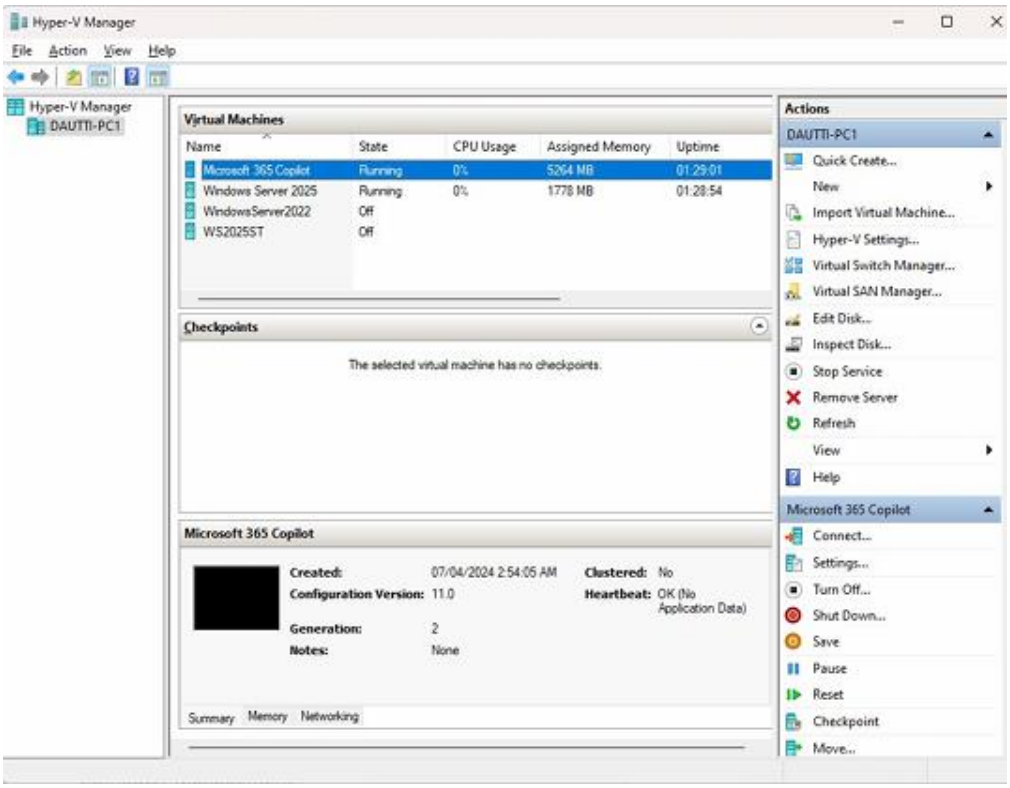

Рисунок 2.9 – Інтерфейс Диспетчера Hyper-V у Windows Server 2025 (основні панелі) [3]

Під час навігації Диспетчером Hyper-V необхідно ознайомитися зі специфічними елементами інтерфейсу користувача, які відіграють критичну роль у керуванні віртуальними середовищами. Колонка «Стан реплікації» (Replication Health) у вікні віртуальних машин надає цінну інформацію про статус реплікації ВМ. Ця функція є вирішальною для підтримки цілісності даних та доступності, особливо у сценаріях аварійного відновлення. Реплікація дозволяє дублювати ВМ на вторинний хост, гарантуючи наявність резервної копії у разі збою. Статус реплікації може відображати такі індикатори, як «Нормальний», «Попередження» або

«Критичний», кожен з яких представляє поточний стан процесу реплікації. Регулярний моніторинг стану реплікації допомагає проактивно виявляти та вирішувати потенційні проблеми; статус «Нормальний» вказує на коректне функціонування, тоді як попередження або критичні сповіщення вимагають негайного розслідування для захисту доступності даних у ситуаціях відмови [3].

Іншою важливою функцією, доступною в Диспетчері Hyper-V, є можливість експорту віртуальної машини на інший хост. Ця функція є необхідною для керування ресурсами та операційної безперервності. Експорт ВМ передбачає створення повної копії, включаючи налаштування конфігурації, віртуальні жорсткі диски та будь-які пов'язані знімки. Ця функціональність дозволяє безперешкодно мігрувати ВМ між різними хостами Hyper-V. Розуміння процесу експорту ВМ озброює IT-фахівців навичками, необхідними для адаптації віртуальних середовищ до змінних потреб організації, забезпечуючи мінімальні збої під час обслуговування або балансування робочих навантажень між хостами.

Перед початком створення та керування віртуальними машинами необхідно ефективно налаштувати параметри Hyper-V на сервері. Ці налаштування доступні через опцію «Параметри Hyper-V...» (Hyper-V Settings...), що знаходиться на панелі дій Диспетчера Hyper-V (рис. 2.10). Кілька ключових областей конфігурації можуть бути адаптовані для оптимізації віртуального середовища, як показано нижче.

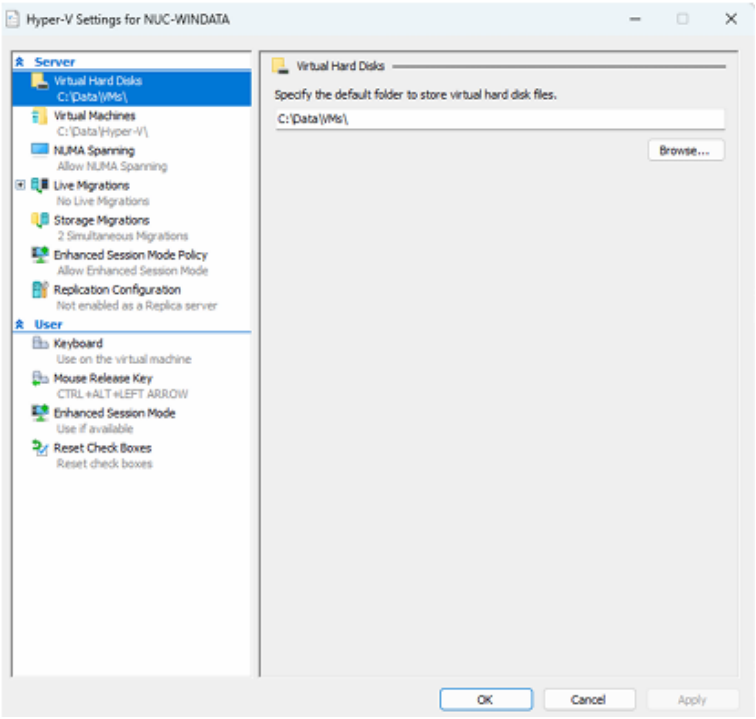

Рисунок 2.10 – Параметри Hyper-V (Hyper-V Settings) у Windows Server 2025 [3]

Налаштування «Віртуальні жорсткі диски» дозволяє вказати каталог за замовчуванням для зберігання файлів віртуальних дисків; належна конфігурація тут є життєво важливою для

підтримки організованого зберігання та ефективного використання дискового простору. Опція «Віртуальні машини» дозволяє визначити розташування за замовчуванням для файлів конфігурації ВМ, забезпечуючи централізоване керування всіма налаштуваннями та метаданими. Розділ «Фізичні графічні процесори» (Physical GPUs) дозволяє призначити графічний процесор, який буде використовуватися ВМ, що є особливо важливим для робочих навантажень, які вимагають високої графічної продуктивності. Налаштування «NUMA Spanning» контролює, чи можуть ВМ охоплювати кілька вузлів неоднорідного доступу до пам'яті (NUMA), що може підвищити продуктивність ВМ шляхом доступу до ширшого діапазону обчислювальних ресурсів. Конфігурація «Міграції сховища» дозволяє встановити максимальну кількість одночасних міграцій сховища, які може обробляти сервер, що є критичним для підтримки продуктивності під час переміщення даних. Політика розширеного режиму сеансу (Enhanced Session Mode Policy) вмикає або вимикає можливість перенаправлення локальних пристроїв та ресурсів з хост-машини до підключення віртуальної машини. Додатково важливо відзначити функції конфігурації реплікації (Replication Configuration) для налаштування Hyper-V Replica та опцію живих міграцій (Live Migrations), що полегшує безперешкодне переміщення запущених ВМ без простою.

Для створення та керування віртуальним жорстким диском (VHD) на Windows Server 2025 за допомогою Диспетчера Hyper-V виконується певна послідовність дій. Спочатку запускається Диспетчер Hyper-V через меню «Засоби Windows». На панелі дій обирається «Створити» (New), а потім «Жорсткий диск...», що ініціює запуск Майстра створення нового віртуального жорсткого диска (рис. 2.11).

Рисунок 2.11 – Процес створення віртуального жорсткого диска [3]

У майстрі обирається формат VHD: VHDX для підвищеної продуктивності та більшої

ємності або VHD для сумісності зі старими системами. Далі визначається тип диска: фіксованого розміру (розмір встановлюється і залишається постійним), динамічно розширюваний (розмір зростає в міру додавання даних до максимуму) або диференціальний (відстежує зміни від базового VHD). Вказується ім’я та розташування файлу VHD, після чого приймається рішення про створення порожнього диска або імпорт даних з існуючого фізичного диска. Після перевірки вибору натискається кнопка «Готово» для створення VHD.

Налаштування розподілу оперативної пам’яті для ВМ є критичним для оптимізації продуктивності. Процес починається з переконання, що ВМ вимкнена. У Диспетчері Hyper-V натискається права кнопка миші на вибраній ВМ і обирається пункт «Параметри...» (Settings...) (рис. 2.12).

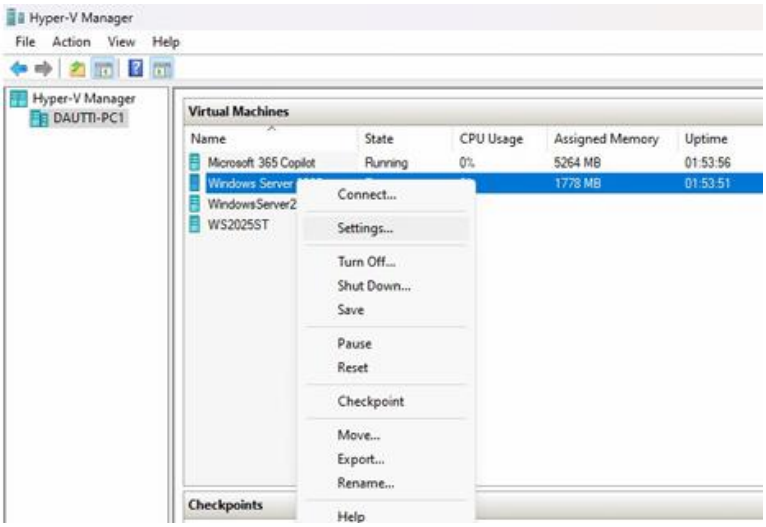

Рисунок 2.12 – Налаштування віртуальної машини [3]

У вікні налаштувань у розділі «Апаратне забезпечення» обирається «Пам’ять», де доступні відповідні інструменти керування (рис. 2.13).

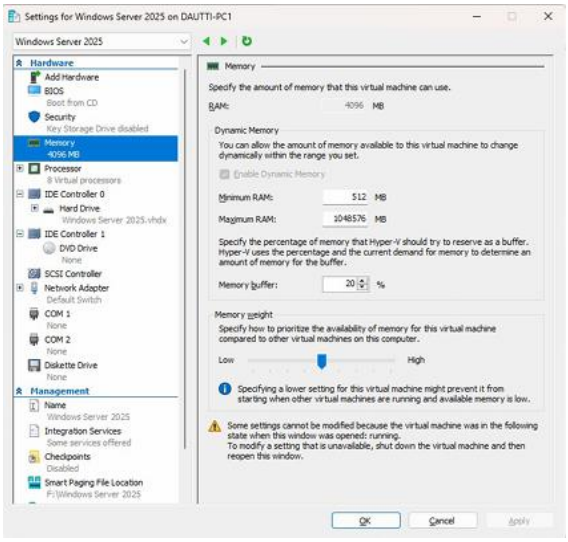

Рисунок 2.13 – Керування віртуальною пам’яттю [3]

Існує дві опції конфігурації: виділення фіксованого обсягу пам’яті шляхом введення бажаного розміру в мегабайтах, або використання динамічної пам’яті шляхом встановлення прапорця «Увімкнути динамічну пам’ять». Остання функція дозволяє Hyper-V розподіляти пам’ять на основі попиту ВМ, встановлюючи мінімальне та максимальне значення RAM. Варто також згадати концепцію надлишкового виділення ресурсів, яка стосується практики виділення більшої кількості віртуальних ресурсів, ніж може підтримати фізичне обладнання. Хоча це може підвищити гнучкість, це також несе ризики зниження продуктивності, тому балансування розподілу ресурсів є критично важливим [4].

Налаштування віртуальної мережі є необхідним для забезпечення зв’язку між ВМ та із зовнішньою мережею. У Hyper-V це досягається шляхом конфігурації віртуального комутатора. Розрізняють три основні типи: зовнішній комутатор (підключає ВМ до фізичного мережевого адаптера хоста, дозволяючи доступ до зовнішньої мережі), внутрішній комутатор (підключає ВМ до хоста, але не надає доступу до зовнішньої мережі) та приватний комутатор (дозволяє зв’язок виключно між ВМ на одному хості). Для налаштування використовується «Диспетчер віртуальних комутаторів...» (Virtual Switch Manager...) на панелі дій (рис. 2.14).

Рисунок 2.14 – Створення віртуального комутатора (Virtual Switch Manager) [3]

Обирається тип комутатора, натискається «Створити віртуальний комутатор», після чого налаштовуються його параметри (рис. 2.15).

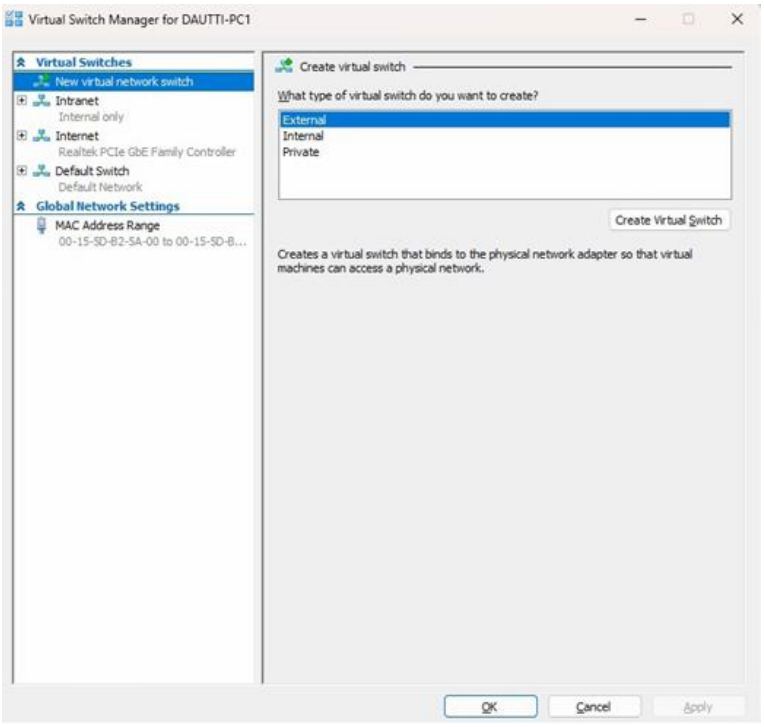

Рисунок 2.15 – Властивості віртуального комутатора [3]

Вказується ім’я та тип підключення. За необхідності вмикається ідентифікація віртуальної локальної мережі (VLAN) для керування трафіком та підвищення безпеки.

Контрольні точки в Hyper-V є ключовою функцією, що дозволяє захопити та зберегти стан ВМ у певний момент часу. Це є неоціненним для підтримки стабільності системи під час критичних операцій. Для створення контрольної точки необхідно натиснути правою кнопкою миші на ВМ і вибрати «Контрольна точка» (Checkpoint) (рис. 2.16).

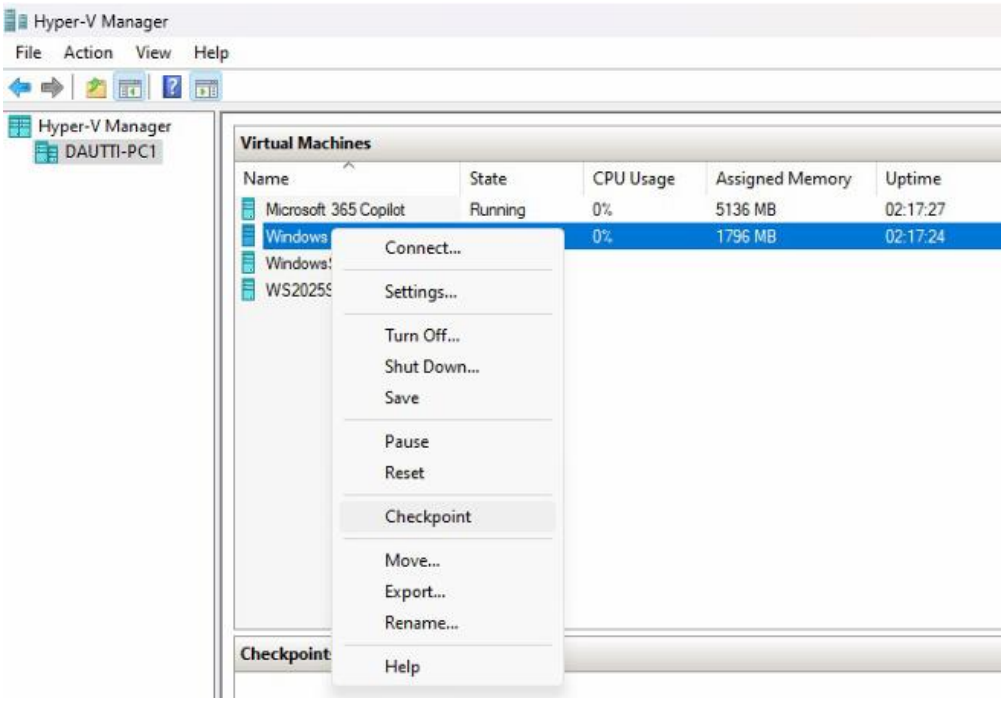

Рисунок 2.16 – Створення контрольної точки (Checkpoint) [3]

Після ініціювання процесу система може відобразити підтвердження успішного виконання операції (рис. 2.17).

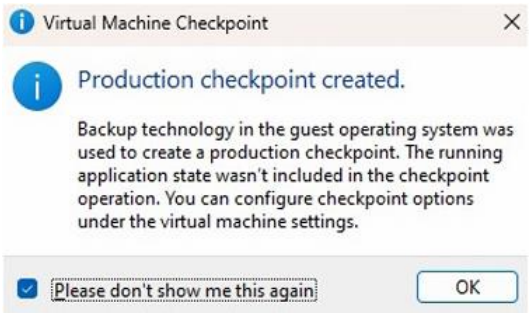

Рисунок 2.17 – Підтвердження створення контрольної точки [3]

Hyper-V пропонує два типи контрольних точок: виробнича контрольна точка (Production Checkpoint), яка фокусується на захопленні стану ВМ з точки зору операційної системи без включення стану запущених додатків, та стандартна контрольна точка (Standard Checkpoint), яка захоплює повний стан ВМ, включаючи всі запущені додатки (рис. 2.18).

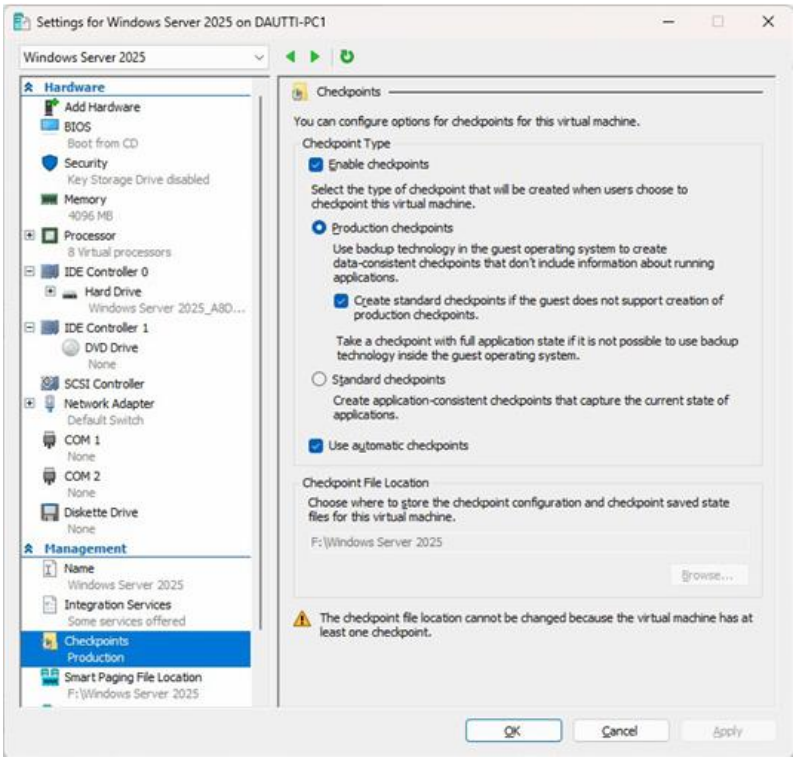

Рисунок 2.18 – Типи контрольних точок (Production та Standard) [3]

З моменту дебюту у Windows Server 2008 можливості віртуального дискового сховища Hyper-V значно еволюціонували. Спочатку використовувався формат VHD з обмеженням розміру до 2 ТБ. З введенням Windows Server 2012 було представлено формат VHDX, який збільшив ліміт до 64 ТБ, покращив стійкість до збоїв живлення та продуктивність.

Незважаючи на ці досягнення, формат VHD залишається підтримуваним у Windows Server 2025 для сумісності [3].

Конвертація фізичних серверів у віртуальні машини (P2V) реалізується за допомогою інструменту Disk2vhd від Microsoft, який перетворює фізичні дискові приводи у файли VHD (рис. 2.19).

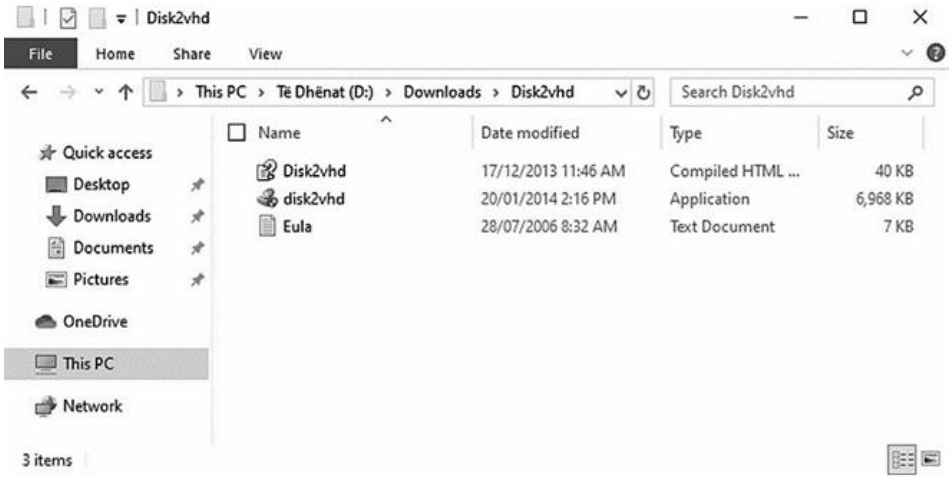

Рисунок 2.19 – Додаток Disk2vhd для конвертації фізичного диска у VHD [3]

Після генерації VHD можна використовувати Диспетчер Hyper-V для налаштування нової ВМ. Зворотний процес, відомий як конвертація з віртуального у фізичне середовище (V2P), є менш підтримуваним і часто вимагає сторонніх рішень або ручної міграції. Для виконання V2P конвертації можна використовувати програмне забезпечення для клонування, таке як EZ Gig IV.

Перехід від VMware до Hyper-V вимагає ретельного планування. Ключові міркування включають оцінку поточного середовища, перевірку сумісності та ліцензування, а також резервне копіювання даних. Microsoft надає інструменти для полегшення міграції, такі як Microsoft Virtual Machine Converter (MVMC) та Disk2VHD. Процес міграції включає підготовку середовища Hyper-V, конвертацію ВМ, тестування та фіналізацію налаштувань мережі [3].

Для ефективного керування ВМ у Hyper-V доступ до її налаштувань здійснюється через контекстне меню «Параметри» (рис. 2.20).

Вікно конфігурації дозволяє налаштувати такі аспекти: додавання обладнання (Add Hardware), прошивка (Firmware), BIOS (порядок завантаження), безпека (Security) для шифрування, пам’ять (Memory), процесор (Processor), контролери IDE та SCSI для керування накопичувачами, мережевий адаптер (Network Adapter), порти COM та дисковод для гнучких дисків. Ретельне налаштування цих параметрів дозволяє оптимізувати продуктивність ВМ та адаптувати її до специфічних операційних вимог.

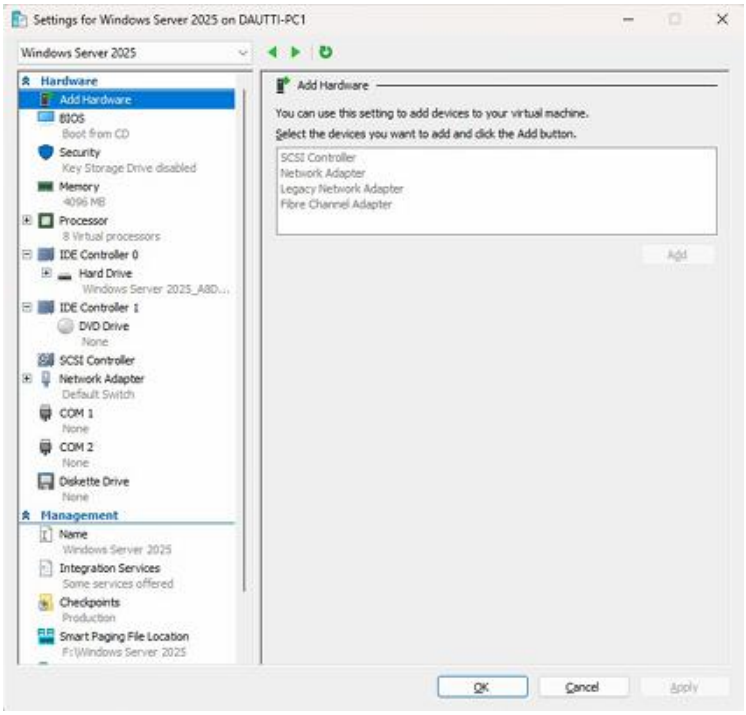

Рисунок 2.20 – Встановлення параметрів ВМ [3]

Під час керування віртуальними машинами у Hyper-V використання як панелі дій, так і контекстного меню ВМ дозволяє суттєво оптимізувати адміністративні завдання. Панель дій, зображена на рисунку 2.21, є важливим компонентом Диспетчера Hyper-V, що полегшує комплексне керування ВМ. Вона надає опції для створення нових віртуальних машин, конфігурації параметрів Hyper-V, налаштування віртуальних комутаторів та створення віртуальних мереж зберігання даних (SAN). Ця панель також дозволяє здійснювати модифікацію та перевірку віртуальних дисків, зупинку та запуск служб, видалення ВМ та оновлення списку доступних ВМ. Її роль як центрального інструменту керування гарантує, що адміністратори можуть виконувати широкий спектр завдань з єдиного інтерфейсу, підвищуючи ефективність та зручність використання.

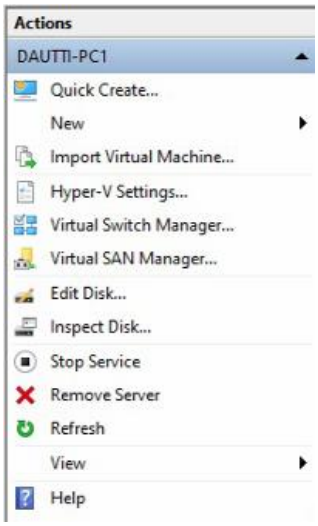

Рисунок 2.21 – Панель дій у Диспетчері Hyper-V [3]

Контекстне меню ВМ, проілюстроване на рисунку 2.22, доповнює панель дій, пропонуючи опції, специфічні для вибраної ВМ. Це меню включає такі важливі функції, як «Підключити...» (Connect...) для доступу до консолі ВМ, «Перейменувати...» (Rename...) для оновлення імені ВМ, а також різні інші опції керування, адаптовані до окремої ВМ. Наприклад, можна керувати налаштуваннями ВМ, контрольними точками та знімками або навіть контролювати стан її живлення (наприклад, запуск, зупинка, пазу) безпосередньо з цього меню. Специфічність контекстного меню дозволяє здійснювати точне, сфокусоване керування окремими ВМ, що робить його цінним інструментом для виконання завдань, специфічних для ВМ. Розуміння того, як використовувати як панель дій, так і контекстне меню, озброює адміністратора надійним набором інструментів для ефективного керування ВМ у Hyper-V.

Рисунок 2.22 – Контекстне меню в Диспетчері Hyper-V [3]

Налаштування параметрів запуску та відновлення ВМ є важливим для забезпечення безперебійної роботи та стійкості системи, особливо після перезавантаження хоста. Ці налаштування дозволяють адміністраторам контролювати поведінку ВМ у відповідь на перезапуск хоста, мінімізуючи потенційний час простою та оптимізуючи розподіл ресурсів. Рекомендується конфігурувати «Дію при запуску» (Startup Action) на основі операційних потреб. Опція «Нічого не робити» (Do Nothing) ідеально підходить для некритичних ВМ, що може допомогти зберегти ресурси хоста після перезапуску. Опція «Автоматично запускати, якщо вона працювала» (Automatically Start if Running) призначена для важливих ВМ, забезпечуючи відновлення їхнього попереднього стану без необхідності ручного втручання, що є корисним для послідовної безперервності надання послуг. Опція «Завжди запускати» (Always Start) підходить для критичних систем, які повинні бути оперативними негайно після перезапуску хоста, незалежно від їхнього попереднього стану [3].

Важливим параметром є також «Затримка автоматичного запуску» (Automatic Start

Delay). Поетапний запуск ВМ може запобігти вузьким місцям у продуктивності шляхом зменшення миттєвого навантаження на центральний процесор та пам'ять. Ця функція є корисною в середовищах з декількома ВМ на одному хості. Окрім того, налаштування «Дії при автоматичній зупинці» (Automatic Stop Action) для коректного завершення роботи ВМ при вимкненні або перезавантаженні хоста допомагає запобігти втраті даних та підтримує цілісність ВМ. Hyper-V надає опції в налаштуваннях автоматичної дії при запуску та зупинці для кожної віртуальної машини, дозволяючи адміністраторам конфігурувати поведінку ВМ при запуску або вимкненні хоста Hyper-V. Ці налаштування є важливими в середовищах Hyper-V для забезпечення часу безвідмовної роботи для критичних робочих навантажень шляхом автоматичного перезапуску важливих ВМ, керування розподілом ресурсів під час перезавантаження хоста шляхом встановлення затримок для некритичних ВМ, що допомагає запобігти вузьким місцям у продуктивності, а також збереження цілісності даних ВМ шляхом налаштування дії завершення роботи для вимкнення ВМ перед коректним вимкненням хоста. Ці конфігурації запуску та відновлення є невід'ємною частиною опцій керування Hyper-V та відіграють ключову роль у підтримці надійних, стійких операцій ВМ. Дотримання цих практик забезпечує добре організоване середовище ВМ з мінімізованим впливом від несподіваних перезавантажень та оптимізованою продуктивністю робочих навантажень.

Для покращення розуміння та надання практичних висновків у цьому розділі висвітлюються реальні сценарії, де Hyper-V відіграє вирішальну роль у сучасних IT-операціях. Ці приклади не лише демонструють універсальність Hyper-V, але й пропонують дієві кроки для загальних галузевих практик, таких як міграція, аварійне відновлення, автоматизація та резервне копіювання.

Для багатьох організацій міграція з VMware на Hyper-V представляє стратегічний зсув у напрямку консолідації IT-ресурсів в екосистемі Microsoft. Ця міграція вимагає продуманого планування, починаючи з комплексної оцінки сумісності існуючих ВМ. Використання таких інструментів, як Microsoft Virtual Machine Converter (MVMC) або System Center Virtual Machine Manager (SCVMM), може оптимізувати процес міграції шляхом автоматизації певних етапів, таких як конвертація дисків ВМ та конфігурація мережі. Тестування кожної ВМ у проміжному середовищі перед реальним розгортанням забезпечує оптимальну функціональність та зменшує ризик потенційних проблем. Завдяки ретельній підготовці організації можуть перейти на Hyper-V, підтримуючи високу продуктивність та мінімізуючи перебої в обслуговуванні.

Hyper-V Replica є потужною функцією для аварійного відновлення, що дозволяє організаціям реплікувати ВМ на вторинний майданчик, як локально, так і в хмарі. Це налаштування забезпечує критичну мережу безпеки, гарантуючи швидке відновлення та мінімальну втрату даних у разі збою основного майданчика. Конфігурація Hyper-V Replica

передбачає налаштування реплікації на рівні ВМ, визначення частоти реплікації на основі цільових точок відновлення (Recovery Point Objectives – RPO) та конфігурацію мережевих з'єднань між основним та реплікаційним майданчиками. Регулярно реплікуючи ВМ на резервний майданчик, бізнес може захистити свої дані та зменшити час простою, підтримуючи стійку інфраструктуру [3].

Рутинне технічне обслуговування, таке як оновлення системи, може вносити зміни, що впливають на стабільність ВМ. Автоматизація контрольних точок ВМ за допомогою PowerShell перед кожним оновленням є найкращою практикою для полегшення відкату у разі виникнення проблем. Наступний скрипт PowerShell створює контрольну точку для кожної запущеної ВМ, позначаючи кожен знімок міткою часу для легкої ідентифікації.

Цей скрипт допомагає адміністраторам економити час, впроваджуючи механізм безпеки для декількох ВМ, сприяючи операційній узгодженості та мінімізуючи ризик, пов'язаний з оновленнями.

Регулярне резервне копіювання ВМ Hyper-V є необхідним для безперервності бізнесу, дотримання нормативних вимог та захисту даних. Windows Server 2025 надає такі інструменти, як Windows Server Backup та System Center Data Protection Manager (DPM), для планування автоматизованого резервного копіювання або створення знімків за вимогою. Налаштування рутинного резервного копіювання гарантує, що стан ВМ, конфігурація та дані надійно зберігаються, підтримуючи швидке відновлення у разі випадкової втрати даних або кіберінцидентів. Впроваджуючи регулярне резервне копіювання, організації не лише захищають критичні дані, але й будують стійку та відповідну вимогам IT-інфраструктуру, здатну задовольнити сучасні вимоги бізнесу. Ці реальні приклади підкреслюють можливості Hyper-V у досягненні надійних та ефективних віртуалізованих середовищ, допомагаючи IT-фахівцям застосовувати ці найкращі практики безпосередньо у своїх організаціях. З цим фундаментом здійснюється підготовка до переходу до практичних вправ, таких як інсталяція ролі Hyper-V у Windows Server 2025, для подальшого вдосконалення навичок та застосування знань у реальних сценаріях [4].

Технічні вимоги

Впровадження платформи віртуалізації Hyper-V вимагає дотримання чітко визначених специфікацій обладнання, причому для окремих функціональних можливостей можуть висуватися додаткові умови. Наведена нижче інформація призначена для аналізу відповідності системи встановленим критеріям, що є необхідним для планованої експлуатації середовища.

Незалежно від обраного набору функцій Hyper-V, базові вимоги до апаратної платформи є обов'язковими для виконання. Ключовою умовою є наявність 64-розрядного

процесора з підтримкою технології трансляції адрес другого рівня (SLAT). Наявність SLAT є критичною для інсталяції компонентів віртуалізації, таких як гіпервізор Windows. Водночас, для встановлення засобів керування Hyper-V, до яких належать «Підключення до віртуальної машини» (Virtual Machine Connection або VMConnect), Диспетчер Hyper-V та командлети Hyper-V для Windows PowerShell, наявність SLAT на процесорі не вимагається. Окрім цього, необхідною є підтримка розширень режиму моніторингу віртуальної машини. Окремої уваги потребує підсистема оперативної пам'яті. Планування ресурсів має виходити з мінімального обсягу у 4 ГБ, при цьому більший обсяг пам'яті забезпечує кращу продуктивність. Системі має бути доступний достатній обсяг пам'яті як для функціонування хоста, так і для одночасної роботи всіх запланованих віртуальних машин [17].

На рівні базової системи вводу-виводу (BIOS) або інтерфейсу UEFI повинна бути активована підтримка віртуалізації. Це передбачає наявність апаратної віртуалізації, що реалізується у процесорах з відповідними опціями, зокрема Intel Virtualization Technology (Intel VT) або AMD Virtualization (AMD-V).

Також обов'язковою вимогою є доступність та активація апаратного запобігання виконанню даних (DEP). Для архітектури Intel ця технологія позначається як біт XD (Execute Disable Bit), а для систем AMD – як біт NX (No Execute Bit) [17].

Для верифікації відповідності апаратного забезпечення вимогам Hyper-V застосовуються інструменти командного рядка. Процедура передбачає відкриття Windows PowerShell або командного рядка та введення команди Systeminfo.exe (рис. 2.23).

У згенерованому звіті необхідно прокрутити вміст до розділу вимог Hyper-V. Якщо всі перелічені параметри мають значення «Так», система придатна для запуску ролі Hyper-V. У разі, якщо будь-який з елементів повертає значення «Ні», вимагається перегляд вимог, наведених у документації, та внесення відповідних апаратних або конфігураційних коректив.

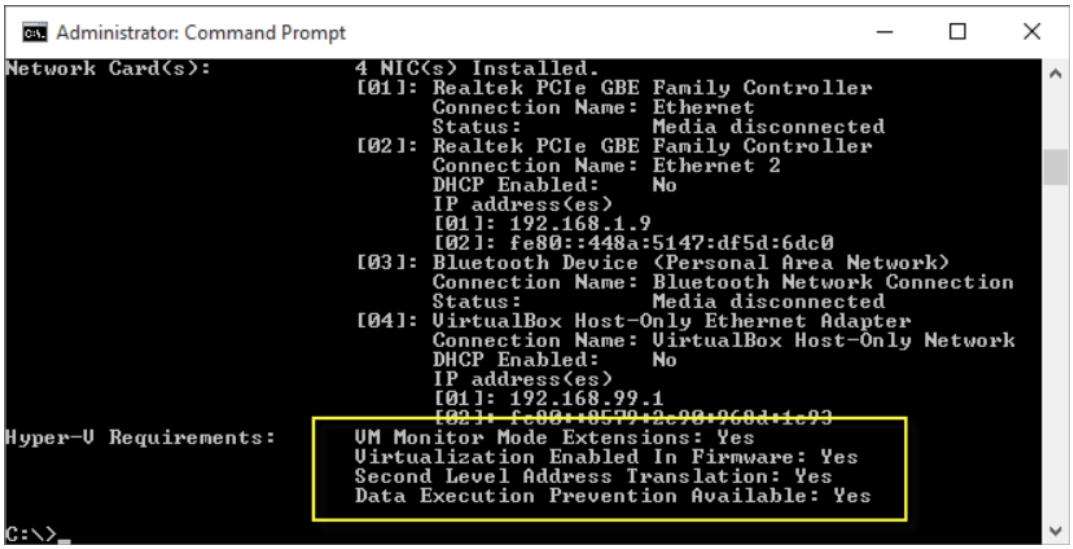

Рисунок 2.23 – Звіт команди Systeminfo.exe [17]

Окремий набір вимог висувається до таких функцій, як призначення дискретних пристроїв та використання екранованих віртуальних машин. Стосовно призначення дискретних пристроїв (Discrete Device Assignment), вимоги до хоста аналогічні тим, що встановлені для функції SR-IOV у Hyper-V. Процесор повинен підтримувати роботу з розширеною таблицею сторінок (EPT) для архітектури Intel або вкладеною таблицею сторінок (NPT) для архітектури AMD. Системна логіка (чіпсет) повинна забезпечувати перепризначення переривань, що реалізується через Intel VT-d з можливістю перепризначення переривань (VT-d2) або будь-яку версію блоку керування пам'яттю вводу/виводу AMD (I/O MMU). Також необхідна підтримка перепризначення прямого доступу до пам'яті (DMA), що забезпечується Intel VT-d з черговими інвалідаціями або I/O MMU AMD. Обов'язковою є наявність служб контролю доступу (ACS) на кореневих портах PCI Express [17].

Таблиці прошивки системи повинні бути сконфігуровані таким чином, щоб надавати гіпервізору Windows доступ до I/O MMU. Зазначена функція може бути деактивована в налаштуваннях UEFI або BIOS, тому для її активації рекомендується звернутися до документації обладнання або виробника. Стосовно пристроїв, що призначаються, вимагається наявність графічного процесора або енергонезалежної пам'яті Express (NVMe). Слід зауважити, що лише певні моделі графічних пристроїв підтримують призначення дискретних пристроїв, що потребує перевірки через технічну документацію. Деталізовану інформацію про використання цієї функції та важливі аспекти налаштування можна знайти у спеціалізованих джерелах, присвячених опису та довідці щодо призначення дискретних пристроїв.

У випадку успішного виконання всіх вимог до операційної системи, апаратного забезпечення та сумісності, у відповідному інтерфейсі керування стає доступним розділ Hyper-V.

Тема 3
Встановлення та основи адміністрування Windows Server

Розуміння розподілу дисків і параметрів зберігання даних

Встановлення нових операційних систем класифікується як рутинне завдання в межах системного адміністрування. Цей процес охоплює низку критичних етапів, зокрема підготовку інсталяційного носія, безпосереднє виконання інсталяції ОС, перевірку результатів розгортання та налаштування початкової конфігурації сервера. Зазначені кроки є фундаментальними для формування бази подальших операцій. Хоча певні сервери можуть постачатися з попередньо встановленими операційними системами, експертиза системного адміністратора часто є необхідною для забезпечення відповідності встановленої ОС специфічним потребам інфраструктури. Перед початком процесу інсталяції розглядається важливість схем розподілу для організації дискових розділів [6].

Розподіл диска визначається як процес поділу фізичного носія на логічні секції, відомі як розділи. Кожен розділ може функціонувати під управлінням окремої файлової системи, наприклад, файлової системи нової технології (NTFS) або стійкої файлової системи (ReFS), і використовуватися для зберігання різноманітних типів даних. Розділи також можуть застосовуватися для створення окремих томів – логічних одиниць зберігання, що можуть охоплювати кілька фізичних дисків [3].

Схема розподілу є технікою, що детермінує спосіб створення та керування цими розділами на дисках. Виділяють дві основні схеми розподілу: Головний завантажувальний запис (MBR) та Таблицю розділів GUID (GPT). MBR – це старіша схема розподілу, яка наразі вважається застарілою і не рекомендується для сучасних систем. MBR оперує дисковими секторами розміром 512 байт і підтримує лише 4 основні розділи або 1 розширений розділ, що містить до 26 логічних розділів. Для керування дисками використовується логічна адресація блоків (LBA) з максимальним обмеженням обсягу в 2 ТБ. Хоча MBR свого часу була корисною для систем із кількома варіантами завантаження, вона має низку обмежень, що робить її несумісною із сучасними технологіями: обмеження розміру в 2 ТБ є недостатнім для багатьох сучасних пристроїв, а лімітована кількість розділів може стати вузьким місцем для складних конфігурацій [3].

Додатково MBR позбавлена розширених функцій надлишковості та відновлення, властивих новішим схемам. Ці недоліки зумовили розробку Таблиці розділів GUID (GPT) – сучасної схеми, що долає недоліки MBR. GPT використовує 128-бітний глобальний унікальний ідентифікатор (GUID) для ідентифікації ресурсів. Підтримуються розміри блоків від 512 байт і вище, із загальноприйнятим стандартом у 4096 байт, де кожен запис розділу займає 128 байт. GPT є частиною стандарту єдиного розширюваного інтерфейсу прошивки (UEFI), який замінює застарілий BIOS. Ця схема характеризується стійкістю, здатністю

обробляти до 9,4 зетабайт (ZB) дискового простору та підтримувати до 128 розділів на диск. Також GPT забезпечує кращі функції надійності та безпеки, такі як захисний MBR та контрольна сума CRC32. Важливо розуміти сутність CRC32 – алгоритму контрольної суми, що використовується для виявлення помилок при передачі або зберіганні даних. CRC32 генерує унікальне значення, похідне від вмісту даних, яке порівнюється з оригінальною сумою для перевірки цілісності. Невідповідність значень свідчить про можливе пошкодження даних під час передачі чи зберігання.

Для інсталяції Windows Server 2025 використання схеми розділів GPT є обов'язковим. Ця необхідність випливає з вимоги використання UEFI, який замінює традиційний BIOS і здійснює завантаження виключно з дисків GPT. UEFI не лише забезпечує швидші та безпечніші процеси завантаження, але й підтримує розширені функціональні можливості, такі як безпечне завантаження (Secure Boot) та BitLocker. Secure Boot захищає процес завантаження, дозволяючи запуск лише авторизованого ПЗ та блокуючи шкідливий код, наприклад руткіти. BitLocker доповнює це повним шифруванням диска, гарантуючи безпеку даних навіть у разі фізичного вилучення пристрою [7].

У Windows Server 2025 створення та керування розділами здійснюється через інструмент «Керування дисками» або утиліту Diskpart. Альтернативно використовується майстер налаштування Windows під час інсталяції. При необхідності конвертації MBR у GPT попередньо видаляються всі розділи, тому критично важливо виконати резервне копіювання даних. Окрім вибору схеми розділів, налаштовуються параметри завантаження (Boot settings) в BIOS або UEFI для визначення джерела запуску ОС (DVD, USB, мережа). Для створення завантажувального USB-накопичувача можна використовувати інструмент Windows 7 USB/DVD Download Tool, доступний на офіційному сайті Microsoft [7].

Окрім розподілу дисків, Windows Server 2025 пропонує різноманітні варіанти зберігання для підвищення продуктивності, доступності та масштабованості. До ключових функцій належать Storage Spaces, Storage Spaces Direct та Storage Replica. Функція Storage Spaces дозволяє створювати віртуальні диски з пулу фізичних дисків, пропонуючи різні рівні стійкості (простий, дзеркальний, з парністю) та підтримує багаторівневе зберігання для автоматичного переміщення даних між SSD та HDD.

Storage Spaces Direct уможливлює формування спільного пулу зберігання з локальних дисків у межах кластера, сприяючи створенню рішень гіперконвергентної інфраструктури (HCI) або програмно-визначеного сховища (SDS). HCI представляє структуру, що об'єднує обчислення, зберігання та мережу в єдину систему, керовану програмним забезпеченням, що оптимізує керування та масштабованість. SDS, у свою чергу, відокремлює обладнання для зберігання від програмного забезпечення керування, дозволяючи динамічно розподіляти ресурси.

Функція Storage Replica забезпечує реплікацію даних між серверами або кластерами (синхронну або асинхронну), уможливлюючи створення розтягнутих кластерів або реплікацію між сайтами. Розтягнуті кластери розподіляють єдиний кластер між кількома локаціями для забезпечення безперебійної роботи, тоді як реплікація між сайтами синхронізує дані між [3].

Після завершення інсталяції важливим є розуміння розширених параметрів запуску. У Windows Server 2025 відсутня опція використання клавіші F8 для відновлення ОС. Натомість доступ до розширених опцій здійснюється через меню налаштувань. Процес ініціюється натисканням кнопки «Пуск», вибором піктограми «Налаштування» (Settings), переходом до розділу «Система» (System) та вибором опції «Відновлення» (Recovery). У правій частині екрана, у розділі параметрів відновлення, натискається кнопка «Перезавантажити зараз» (Restart now), як показано на рисунку 3.1.

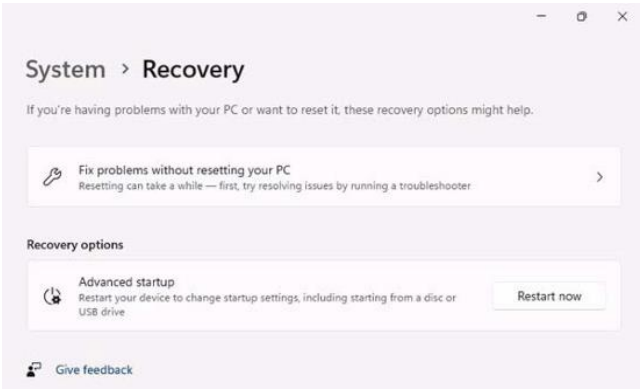

Рисунок 3.1 – Перехід до розширеного запуску в Windows Server 2025 [3]

Після цього з’являється діалогове вікно попередження про збереження роботи, де необхідно повторно натиснути «Перезавантажити зараз» та обрати причину дії. Після перезавантаження системи на екрані вибору опцій обирається пункт «Виправлення неполадок» (Troubleshoot). На екрані розширених опцій, як показано на рисунку 3.2, стає можливим вибір різноманітних інструментів для відновлення або ремонту серверної операційної системи.

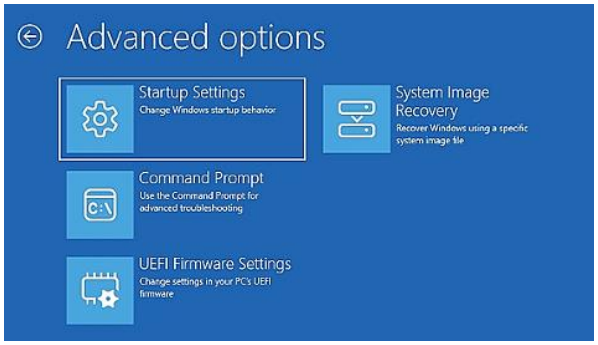

Рисунок 3.2 – Розширені параметри (Advanced Options) у Windows Server 2025 [3]

Квоти

У контексті адміністрування серверів під керуванням Windows Server 2025 критично важливим завданням є контроль використання дискового простору користувачами та додатками. Для вирішення цієї задачі застосовується механізм дискових квот, який дозволяє обмежувати обсяг даних, що зберігаються, та запобігати переповненню фізичних носіїв, що могло б призвести до відмови в обслуговуванні критичних сервісів.

У сучасній версії Windows Server 2025 розрізняють два основні підходи до реалізації квотування: стандартні квоти NTFS та розширені квоти диспетчера ресурсів файлового сервера (File Server Resource Manager – FSRM). Стандартні квоти NTFS функціонують на рівні логічного тому і прив'язуються до облікового запису користувача, який є власником файлів. Цей метод є базовим і дозволяє встановити ліміт дискового простору для конкретного користувача на всьому диску, незалежно від розташування файлів у папках. Хоча цей підхід забезпечує загальний контроль, він характеризується недостатньою гнучкістю для складних корпоративних сценаріїв, де необхідно обмежувати розмір конкретних спільних папок, а не загальний простір користувача [3].

Для більш гранулярного та ефективного керування в Windows Server 2025 рекомендується використання Диспетчера ресурсів файлового сервера (FSRM). На відміну від квот NTFS, квоти FSRM застосовуються безпосередньо до папок або томів, що дозволяє адміністраторам контролювати розмір директорій спільного доступу, незалежно від того, хто є власником файлів у них.

Система FSRM підтримує два типи квот: жорсткі та м'які. Жорстка квота фізично забороняє запис даних на диск після досягнення встановленого ліміту, генеруючи помилку про недостатність місця для користувача. Цей тип використовується для суворого дотримання політик зберігання. М'яка квота, навпаки, не блокує запис даних при перевищенні ліміту, а використовується виключно для моніторингу та сповіщення. Вона дозволяє адміністраторам відстежувати тенденції зростання даних та отримувати повідомлення про порушення політик використання простору, не перериваючи робочий процес користувачів [3].

Процес налаштування квот у FSRM оптимізується за допомогою використання шаблонів квот. Шаблони визначають набір стандартних параметрів, таких як ліміт простору, тип квоти (жорстка чи м'яка) та порогові значення сповіщень.

Використання шаблонів дозволяє централізовано керувати політиками: при зміні параметрів у шаблоні зміни можуть автоматично поширюватися на всі квоти, що базуються на ньому. Важливим елементом конфігурації є налаштування порогових значень, які ініціюють дії при заповненні квоти на певний відсоток (наприклад, 85%, 95% або 100%). Дії можуть включати надсилання електронних листів адміністратору або користувачу, запис події

в журнал Windows, виконання скриптів або формування звітів. Такий підхід забезпечує проактивне керування інфраструктурою зберігання даних, дозволяючи виявляти та вирішувати проблеми з нестачею вільного місця до настання критичних ситуацій.

Дослідження конфігурацій завантаження та параметрів запуску

Перед завантаженням операційної системи комп'ютер повинен пройти процес ініціалізації, який охоплює перевірку апаратних компонентів та завантаження системного програмного забезпечення. Цей процес керується мікропрограмним забезпеченням – BIOS або UEFI, залежно від архітектури материнської плати та апаратного забезпечення. Як BIOS, так і UEFI відповідають за конфігурацію параметрів завантаження, включаючи порядок завантаження, режим завантаження та вибір пріоритетного пристрою. Параметри завантаження мають суттєвий вплив на продуктивність сервера та його взаємодію з іншими пристроями й мережами. Розуміння відмінностей між BIOS та UEFI, а також їхніх відповідних переваг і недоліків, є критично важливим для системного адміністрування. У цьому розділі розглядаються опції завантаження, доступні в BIOS та UEFI, а також методологія їх налаштування в середовищі Windows Server 2025.

Для коректного запуску системи необхідно розуміти опції завантаження в UEFI (Unified Extensible Firmware Interface), який значною мірою витіснив застарілий BIOS у сучасних системах. UEFI визначається як інтерфейс мікропрограми, що ініціалізує обладнання та ефективно завантажує операційну систему. Доступ до налаштувань UEFI здійснюється під час запуску шляхом натискання певних клавіш (F2, F10, Delete або Esc), які варіюються залежно від виробника. На відміну від старіших систем, UEFI пропонує розширені функції, такі як безпечне завантаження, прискорений час завантаження та підтримку жорстких дисків великого обсягу з використанням GPT [11].

Для забезпечення безперебійного процесу інсталяції Windows Server 2025 критично важливо налаштувати порядок завантаження, встановивши інсталяційний носій (USB або DVD) як основний пристрій завантаження. Додатково настійно рекомендується активація безпечного режиму для підвищення рівня безпеки. Ця функція дозволяє завантажувати лише довірене програмне забезпечення, запобігаючи змінам з боку шкідливого ПЗ. Оскільки Secure Boot часто вимагається стандартами безпеки, необхідно використовувати диск із розміткою GPT, адже ця функція не підтримує розділи MBR. Попередня перевірка цих конфігурацій дозволяє мінімізувати ймовірність збоїв інсталяції через невідповідність налаштувань [5].

При вході в інтерфейс BIOS стають доступними різні варіанти завантаження. Одним із поширених типів інсталяційного носія є завантажувальний DVD. Для його використання необхідно налаштувати комп'ютер на завантаження з DVD-приводу, змінивши порядок завантаження в налаштуваннях BIOS та встановивши оптичний привід як пріоритетний

пристрій. Іншим методом є використання завантажувального USB-накопичувача, який повинен мати обсяг не менше 8 ГБ. Процедура вимагає підключення накопичувача та вибору його як першої опції у послідовності завантаження в BIOS. Також існує метод мережевого завантаження (PXE Boot), що дозволяє завантажувати інсталяційні файли з віддаленого сервера через локальну мережу (LAN). Для цього в налаштуваннях BIOS активується опція мережевого завантаження та встановлюється відповідний пріоритет. Вибір методу залежить від уподобань адміністратора та наявності ресурсів [4].

Розуміння роботи апаратних компонентів та процесу запуску дозволяє технічним спеціалістам швидко вирішувати проблеми та скорочувати час простою сервера. Коли сервер вмикається, початкова активність пов’язана з чіпом на материнській платі, відомим як ПЗУ (ROM), який активує програму BIOS. BIOS відіграє ключову роль у керуванні функціональністю обладнання, виявляючи та конфігуруючи такі компоненти, як центральний процесор (CPU), пам’ять та диски. Крім того, BIOS ідентифікує завантажувальні пристрої, визначаючи джерела ініціації процесу завантаження. Цей процес проілюстровано на рисунку 3.3.

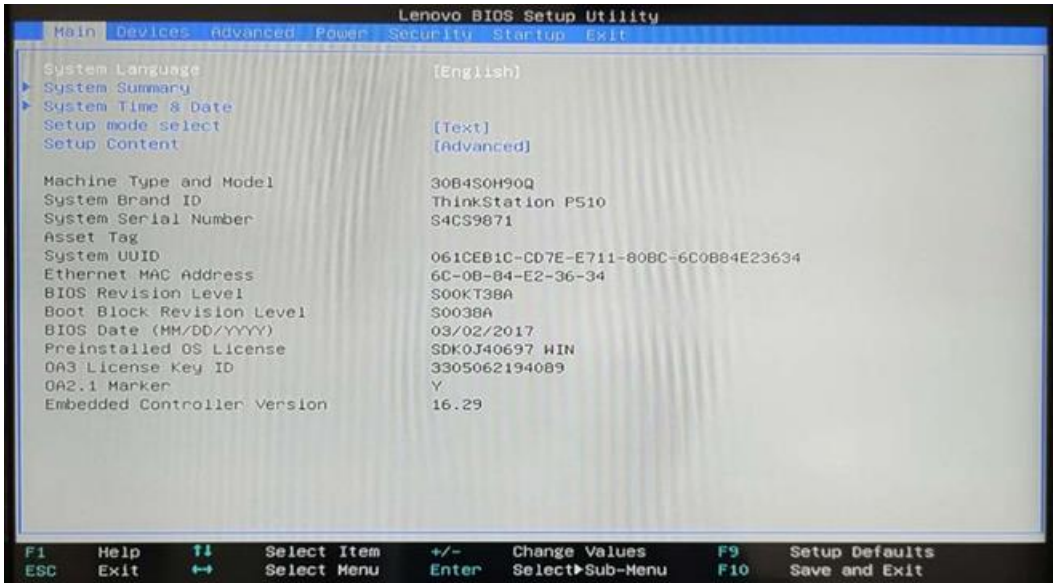

Рисунок 3.3 – Екран конфігурації BIOS [3]

Однак BIOS має обмеження, що робить його недостатнім для сучасних серверів. Для вирішення цих проблем було розроблено UEFI, який забезпечує швидше та безпечніше завантаження, підтримку більших дисків та покращений графічний інтерфейс [9].

Сучасні обчислювальні системи використовують UEFI, розроблений консорціумом UEFI для подолання обмежень BIOS. UEFI може працювати в 32-розрядних та 64-розрядних режимах процесора, маючи доступ до всього обсягу системної пам’яті. Він використовує схему розділів GPT, підтримуючи диски обсягом понад 2 ТБ, та може легко оновлюватися через завантаження мікропрограми з сайту виробника. Доступ до UEFI здійснюється під час

перезавантаження або увімкнення живлення натисканням відповідних клавіш. Меню UEFI дозволяє конфігурувати порядок завантаження, параметри безпеки та налаштування обладнання (рис. 3.4) [9].

Рисунок 3.4 – Утиліта налаштування UEFI [3]

Довірений платформний модуль (TPM) – це чіп безпеки, вбудований у материнську плату сервера, призначений для захищеного зберігання ключів шифрування, сертифікатів та паролів. TPM відіграє вирішальну роль у вимірюванні цілісності процесу завантаження, гарантуючи відсутність несанкціонованих змін у мікропрограмі, завантажувачі або операційній системі. Він працює в поєднанні з BitLocker, який шифрує диски сервера, використовуючи TPM для зберігання ключа шифрування та розблокування його лише після успішної перевірки цілісності (рис. 3.5). Це забезпечує надійний захист даних від крадіжки та втручання [3].

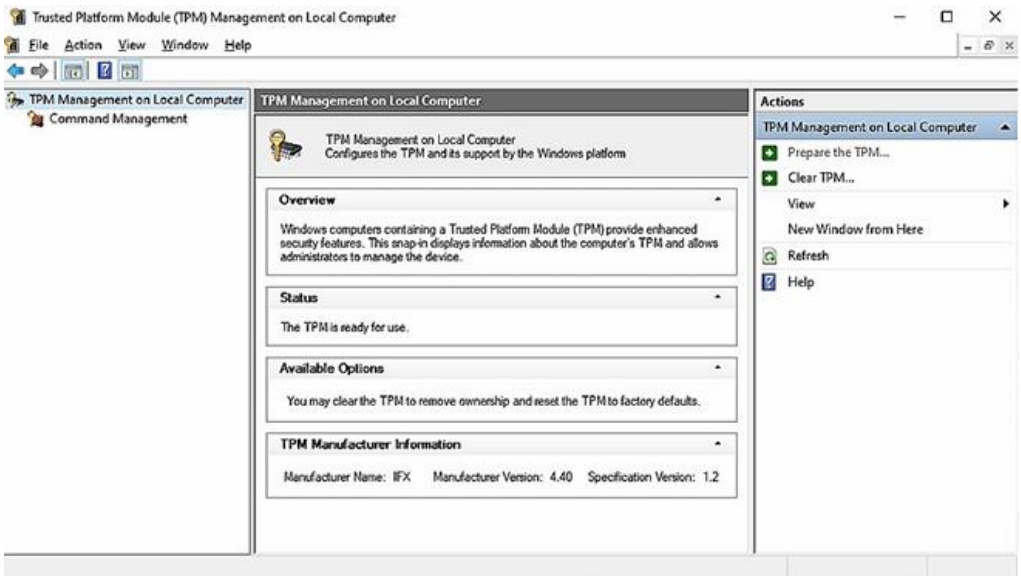

Рисунок 3.5 – Консоль керування TPM [3]

Для коректного запуску сервера проводиться автоматичний діагностичний тест POST (Power-On Self-Test). POST перевіряє процесор, пам’ять, диски та інші пристрої на наявність

помилок, повідомляючи про проблеми через звукові коди або повідомлення на екрані. Особлива увага приділяється таким компонентам, як процесори та відеокарти, оскільки у разі їх несправності сервер не завантажиться. Оскільки різні виробники BIOS/UEFI використовують різні звукові коди, ознайомлення з ними є корисним для діагностики апаратних збоїв [12].

Після проходження POST керування передається першому завантажувальному пристрою. BIOS/UEFI сканує пристрій на наявність таблиці розділів (MBR або GPT), яка вказує розташування ОС. GPT є сучасним стандартом, що підтримує більші диски та підвищує надійність завдяки дублюванню таблиці розділів. UEFI використовує завантажувач, здатний читати розділи GPT. Залежно від версії Windows, завантажувачем може бути NTLDR (для старих версій) або BOOTMGR (від Windows Vista до Windows Server 2025).

Дані конфігурації завантаження (BCD) – це база даних, що зберігає налаштування завантаження ОС. BCD керується за допомогою інструменту командного рядка bcdedit.exe або графічних засобів (рис. 3.6). Вона містить записи для кожного завантажувача та ОС, а також параметри налагодження та відновлення. BCD забезпечує стандартизований інтерфейс опцій завантаження, підвищуючи безпеку порівняно з попередньою системою boot.ini [3].

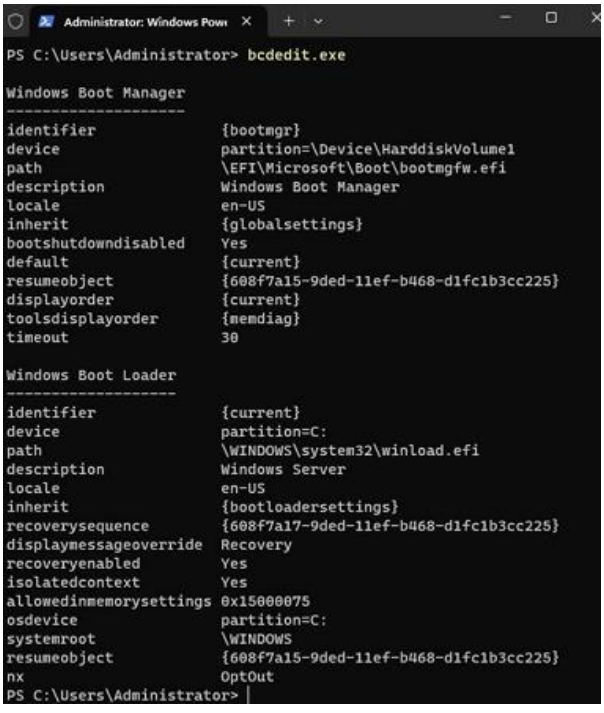

Рисунок 3.6 – Запуск bcdedit.exe у Windows Server 2025 [3]

У сценаріях із кількома завантаженнями (multiboot) можуть бути присутні як NTLDR, так і BOOTMGR. Проблеми з розбиттям дисків та сумісністю драйверів є поширеними під час інсталяції і вирішуються шляхом перевірки режиму завантаження, використання сумісних стилів розділів та завантаження актуальних драйверів.

Завантажувач (bootloader) – це програма, що ініціює запуск системи після POST, завантажуючи ядро ОС у пам’ять [8].

Завантажувальний сектор – це критична область на диску, що містить MBR або GPT. У системах BIOS із MBR сектор містить головний код завантаження та таблицю розділів. Системи UEFI з GPT використовують системний розділ EFI (ESP). Для сумісності UEFI може використовувати модуль підтримки сумісності (CSM) для імітації BIOS. Меню завантаження дозволяє вибирати між кількома встановленими ОС. У старіших версіях це керувалося файлом boot.ini, тоді як нові версії використовують базу даних BCD [8].

Безпечний режим (Safe Mode) є діагностичним інструментом, що запускає Windows лише з основними драйверами та службами. Доступ до нього у старіших версіях здійснювався через клавішу F8 [8].

У нових версіях, включаючи Windows Server 2025, використовуються розширені параметри запуску (Advanced startup options), доступні через утримання клавіші Shift під час перезавантаження. Після перезапуску з’являється екран розширених параметрів завантаження, де можна обрати безпечний режим (рис. 3.7).

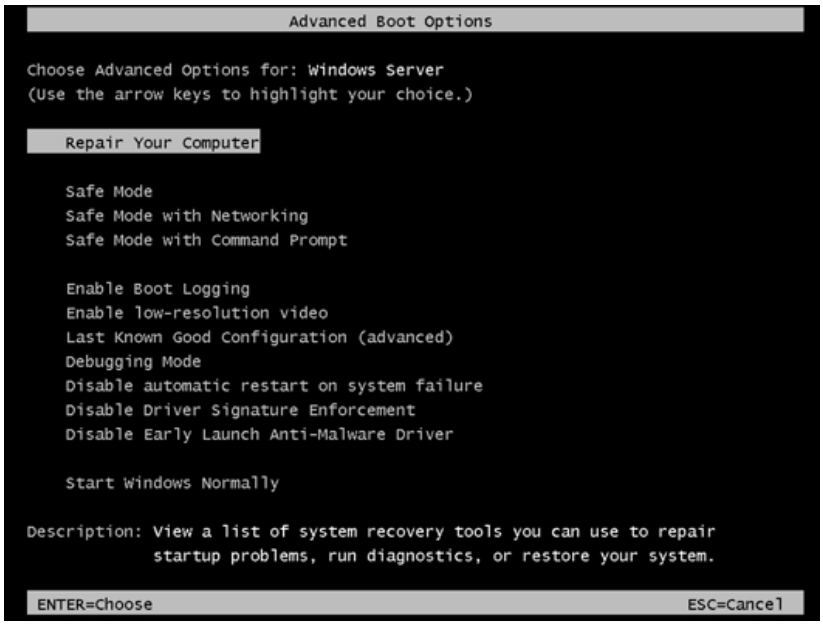

Рисунок 3.7 – Розширені параметри завантаження [3]

Під час підготовки до інсталяції Windows Server 2025 необхідно враховувати вимоги до файлової системи. Системні диски повинні бути відформатовані в NTFS. Для керування розділами використовується утиліта «Керування дисками» (Disk Management), яка дозволяє форматувати диски, змінювати розмір томів (стискати або розширювати) та перевіряти сумісність. Забезпечення правильної конфігурації дисків та формату NTFS мінімізує помилки під час інсталяції.

У цьому розділі було досліджено елементи процесу завантаження Windows,

включаючи BIOS, UEFI, TPM, POST, MBR, BCD, завантажувачі та безпечний режим. Наступний розділ зосередиться на безперервності бізнесу та стратегії її підтримки.

Варіанти встановлення Windows Server 2025

При розгортанні Windows Server вибір відповідного варіанта встановлення є критично важливим етапом для задоволення специфічних потреб інфраструктури. Windows Server надає різноманітні варіанти інсталяції, кожен з яких відповідає різним вимогам щодо дискового простору, використання пам'яті, функціональних можливостей та графічних інтерфейсів. Ці опції також безпосередньо впливають на безпеку, продуктивність, керування та сумісність системи.

Під час інсталяції Windows Server 2025 важливо враховувати специфічні ролі та обов'язки, які виконуватиме сервер. Це передбачення може суттєво вплинути на вибір конфігурації під час інсталяції, включаючи специфікації апаратного забезпечення та вибір служб. Оцінка робочих навантажень передбачає визначення того, чи буде сервер переважно обробляти операції читання, запису або збалансоване поєднання обох. Наприклад, файловий сервер, який переважно надає файли кільком клієнтам, може виграти від вищих швидкостей диска та більшого обсягу оперативної пам'яті для задоволення високих вимог до читання. Натомість сервер баз даних, що обробляє інтенсивні операції запису, може потребувати оптимізованих рішень для зберігання даних та потенційно потужніших обчислювальних ресурсів [10].

Вимоги до пам'яті також варіюються залежно від ролі сервера. Сервери віртуалізації зазвичай потребують більше RAM для ефективного керування кількома віртуальними машинами. Забезпечення адекватного обсягу пам'яті сприяє підтримці продуктивності та швидкодії під навантаженням. Вибір компонентів та служб є критичним: для веб-сервера пріоритетом можуть бути мережеві інтерфейсні карти (NIC) для високошвидкісного з'єднання, тоді як для сервера баз даних акцент робиться на швидких дисках великої ємності для ефективної обробки транзакцій даних. Також важливим є планування майбутнього зростання, що передбачає врахування необхідності обслуговування більшої кількості користувачів або обробки збільшених обсягів даних. Ці фактори слід враховувати при виборі апаратного забезпечення для уникнення потенційних вузьких місць у міру зростання вимог. Інтеграція цих міркувань у планування інсталяції дозволяє адаптувати середовище Windows Server 2025 для ефективного задоволення організаційних потреб.

Перед початком інсталяції Windows Server 2025 необхідно виконати ретельну перевірку сумісності ресурсів для забезпечення відповідності апаратного забезпечення необхідним вимогам для оптимальної продуктивності. Цей крок дозволяє заощадити час та запобігти проблемам під час та після процесу інсталяції. Ключові пункти включають

перевірку системних вимог: процесор повинен бути сумісним з Windows Server 2025 (зазвичай мінімум 1,4 ГГц, 64-бітний процесор), при цьому рекомендується багатоядерний процесор для кращої продуктивності. Мінімальна вимога до ОЗП становить 2 ГБ, проте для кращої продуктивності та обробки важчих навантажень рекомендується 4 ГБ або більше [15].

Також перевіряється доступність ресурсів, зокрема дискового простору. Необхідно забезпечити достатньо місця для інсталяції, а також для майбутніх оновлень та програм (рекомендується мінімум 32 ГБ вільного простору). Оцінюються мережеві ресурси, зокрема пропускна здатність та з'єднання, особливо при розгортанні у хмарному або гібридному середовищі. Встановлення Windows Server на обладнання з недостатньою потужністю може призвести до проблем із продуктивністю, що вплине на роботу сервера та запущених на ньому програм. Додатково перевіряється сумісність існуючих програм з новою версією операційної системи. Проведення цих перевірок перед інсталяцією створює основу для успішного розгортання Windows Server 2025 [15].

При встановленні Windows Server 2025 пропонуються три різні варіанти, кожен з яких має унікальні переваги та обмеження.

Опція Desktop Experience надає повний графічний інтерфейс користувача (GUI) разом з усіма інструментами та функціональними можливостями Windows Server 2025. Хоча це забезпечує комплексний користувацький досвід, цей варіант вимагає більше апаратних ресурсів і може становити вищий ризик безпеки порівняно з іншими [18].

Опція Server Core, рекомендована Microsoft за свою ефективність, є варіантом мінімальної інсталяції, який виключає GUI, зосереджуючись на основних функціях сервера. Вона споживає менше ресурсів та має зменшену площу атаки. Керування здійснюється локально через Windows PowerShell або віддалено за допомогою Server Manager [18].

Третім варіантом є Nano Server – вдосконалена версія Server Core, розроблена для ще більшої легкості та ефективності. Вона підтримує лише 64-бітні додатки та не має можливості локального входу, вимагаючи керування через віддалені інструменти, такі як Windows Admin Center або Windows PowerShell. Nano Server особливо підходить для хмарних середовищ або контейнеризованих додатків [18].

При розгортанні Windows Server 2025 забезпечення надійного мережевого підключення є критичним для успішного приєднання до домену. Процедура усунення несправностей включає перевірку конфігурації IP (підтвердження коректності статичної адреси або отримання адреси від DHCP) та налаштувань DNS, оскільки DNS є життєво важливим для пошуку контролерів домену.

Необхідно перевірити конфігурації брандмауера, щоб переконатися, що відповідні порти відкриті (53 для DNS, 88 для Kerberos, 389 для LDAP). Використання команди ping дозволяє перевірити зв'язок з контролером домену. Також здійснюється огляд налаштувань

мережевого адаптера та аналіз журналів подій на предмет помилок, пов’язаних з мережею.

Питання активації та ліцензування є важливими при інсталяції Windows Server 2025, особливо в Azure або гібридних середовищах. Належна активація гарантує автентичність ОС та можливість отримання оновлень. Поширеною проблемою є збій активації через проблеми зі з’єднанням. У хмарних налаштуваннях необхідно забезпечити стабільне інтернет-з’єднання з серверами активації Microsoft. Якщо активація не вдається, доцільним є використання інструменту командного рядка slmgr, наприклад, виконання команди slmgr /ato для спроби ручної активації [3].

Проблеми ліцензування також можуть виникати при використанні ключів корпоративного ліцензування. Для гібридних розгортань слід розглянути перевагу гібридного використання Azure (Azure Hybrid Benefit), яка дозволяє застосовувати існуючі ліцензії Windows Server до віртуальних машин Azure. Вирішення цих питань на ранніх етапах є життєво важливим для безперебійного розгортання та відповідності вимогам. Далі будуть розглянуті різні методи розгортання Windows Server 2025 [3].

Загалом, існує кілька методологічних підходів до інсталяції Windows Server 2025, кожен з яких адаптований до конкретних сценаріїв експлуатації.

Основним методом є «чиста» установка (Clean install), яка передбачає розгортання нового екземпляра операційної системи з повним видаленням попередніх даних та конфігурацій. Цей підхід є оптимальним для нових розгортань або у випадках, коли необхідно розпочати роботу з «чистого аркуша» на новому чи існуючому жорсткому диску. Процес ініціюється завантаженням сервера із зовнішнього носія (DVD, USB) або через мережу, після чого інсталяційні файли завантажуються в оперативну пам’ять. У ході налаштування здійснюється вибір мовних параметрів, прийняття ліцензійних умов та вибір редакції операційної системи, наприклад, Windows Server 2025 Datacenter (Desktop Experience), як показано на рисунку 3.8.

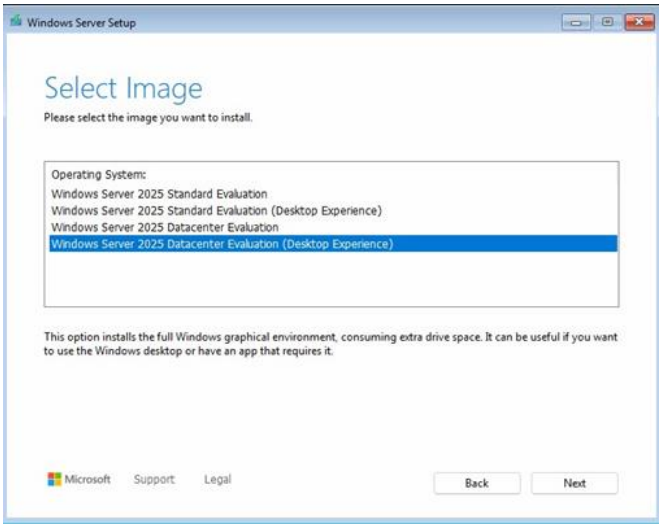

Рисунок 3.8 – Вибір образу операційної системи для інсталяції [3]

Критичним етапом є вибір цільового диска або розділу для інсталяції, де підтверджується видалення існуючих даних, що ілюструється на рисунку 3.9. Після завершення копіювання файлів та налаштування компонентів система перезавантажується для встановлення пароля адміністратора та початкового входу в систему. Важливим аспектом архітектури є використання Windows Installer – інтерфейсу прикладного програмування (API) для керування встановленням та обслуговуванням програмного забезпечення.

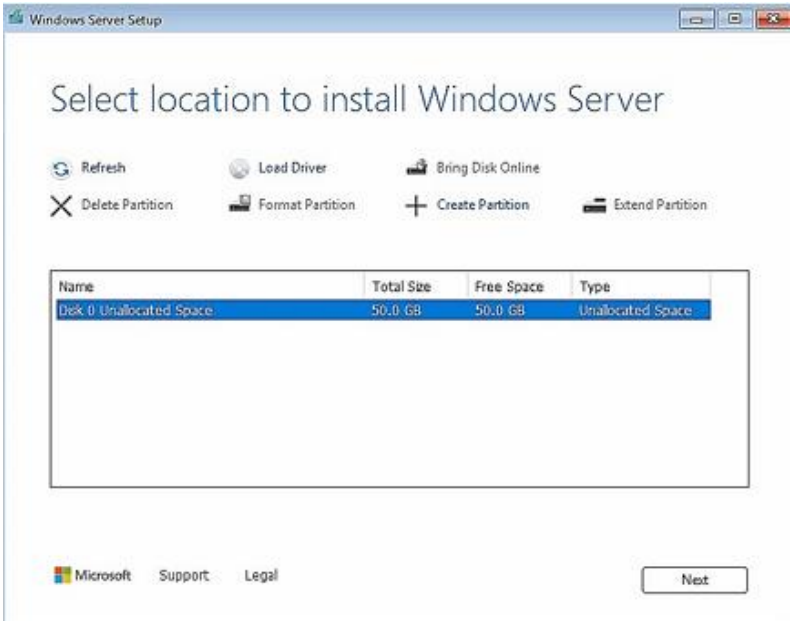

Рисунок 3.9 – Вибір диска або розділу для встановлення Windows Server 2025 [3]

Для оптимізації процесів у корпоративних середовищах застосовується розгортання за допомогою Microsoft Deployment Toolkit (MDT). Цей метод дозволяє автоматизувати інсталяцію, мінімізуючи необхідність ручного втручання, що є критично важливим при масовому розгортанні серверів. Незважаючи на те, що службу розгортання Windows (WDS) визнано застарілою, використання комплекту оцінки та розгортання Windows (Windows ADK) у поєднанні з MDT залишається актуальним стандартом. Ключовим елементом автоматичної установки є файл відповідей у форматі XML, який містить попередньо визначені параметри конфігурації [3].

Створення такого файлу здійснюється за допомогою диспетчера системних образів Windows (Windows SIM) або безпосередньо в середовищі MDT. Процедура передбачає інсталяцію Windows ADK та середовища попереднього встановлення (Windows PE), після чого налаштовується спільний ресурс розгортання через майстер налаштування, як зображено на рисунку 3.10. Після імпорту файлів операційної системи створюється послідовність завдань, яка визначає логіку інсталяції. Сервер завантажується за допомогою образу Windows PE, підключається до спільного ресурсу та виконує розгортання згідно з визначеним сценарієм, що демонструється на рисунку 3.11.

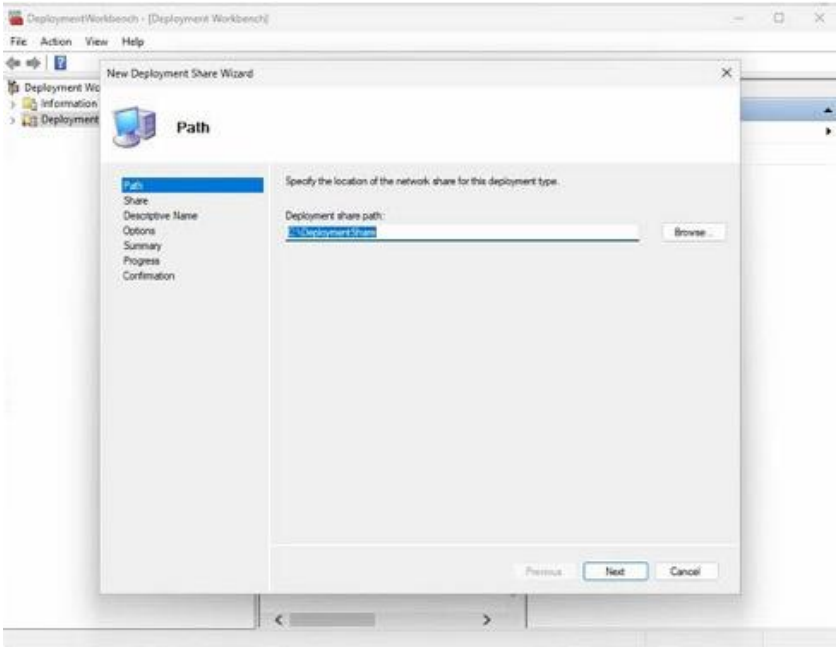

Рисунок 3.10 – Майстер створення нового спільного ресурсу розгортання [3]

Рисунок 3.11 – Розгортання Windows Server 2025 через MDT [3]

Альтернативним підходом є оновлення на місці (In-place upgrade), яке дозволяє модернізувати існуючу операційну систему до версії Windows Server 2025 зі збереженням налаштувань користувача, встановлених додатків та даних. Цей метод підтримується для переходу з версій Windows Server 2012 R2, 2016, 2019 або 2022. Перед початком процедури обов'язковим є виконання резервного копіювання стану системи. Процес оновлення ініціюється із середовища працюючої ОС шляхом запуску файлу налаштування з інсталяційного носія. Після вибору опції збереження файлів та налаштувань система проводить перевірку сумісності та наявності вільного дискового простору. Запуск процесу оновлення, показаний на рисунку 3.12, призводить до заміни системних файлів на нові версії з подальшим перезавантаженням сервера.

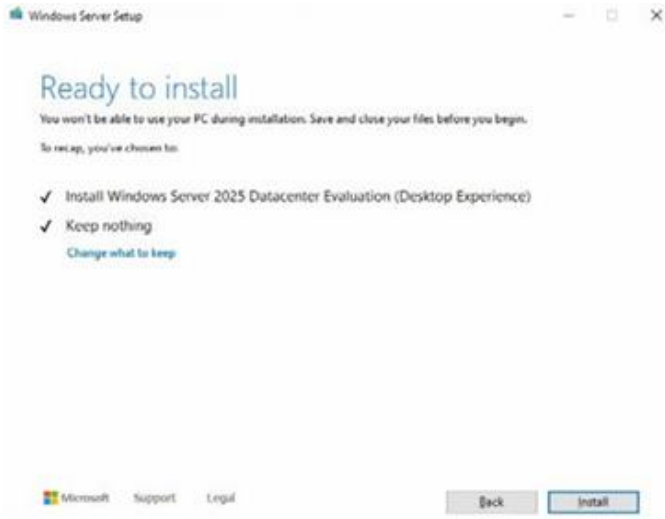

Рисунок 3.12 – Готовність до виконання оновлення на місці [3]

Окремим важливим процесом є міграція сервера, яка передбачає перенесення ролей, функцій, програм та мережевих служб зі старого сервера на новий, що працює під управлінням Windows Server 2025. Цей процес відрізняється від оновлення тим, що виконується між різними фізичними або віртуальними машинами. Для реалізації міграції використовуються інструменти міграції Windows Server (WSMT) та командлети PowerShell. Прикладом може слугувати міграція DHCP-сервера, де на вихідному сервері виконується експорт конфігурації у XML-файл за допомогою команди Export-DhcpServer. Після встановлення ролі DHCP на новому сервері здійснюється імпорт налаштувань за допомогою командлета Import-DhcpServer, як проілюстровано на рисунку 3.13. Це забезпечує безперервність надання мережевих послуг при зміні апаратної або програмної платформи.

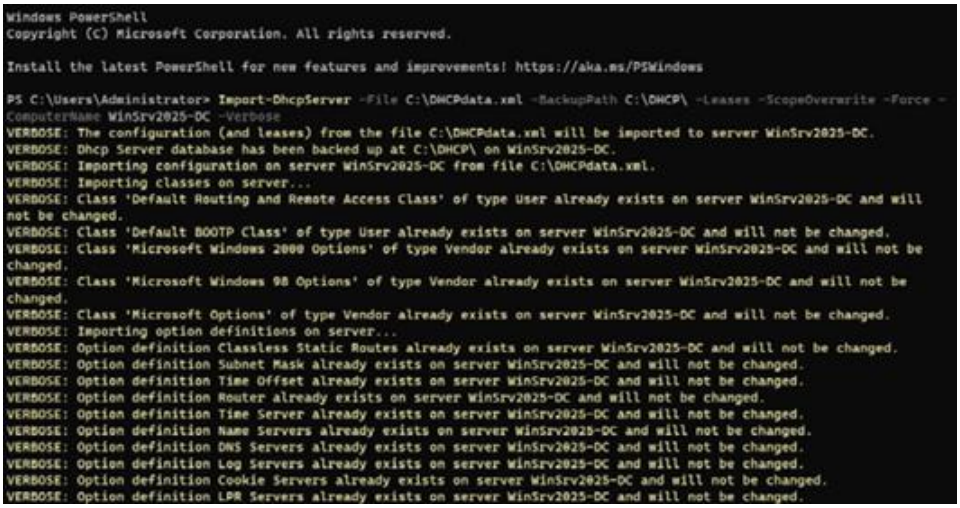

Рисунок 3.13 – Імпорт конфігурації DHCP-сервера на новий сервер [3]

В умовах сучасної цифровізації набуває поширення розгортання в хмарному середовищі Microsoft Azure. Цей метод дозволяє використовувати Windows Server 2025 як

віртуальну машину, забезпечуючи масштабованість та надійність без необхідності у фізичному обладнанні. Процес передбачає створення облікового запису Azure та налаштування віртуальної машини через веб-портал. Під час конфігурації визначаються група ресурсів, регіон розташування та образ операційної системи, зокрема Windows Server 2025 Datacenter – Gen2, що показано на рисунку 3.14. Після задання параметрів дисків та мережі ініціюється розгортання, по завершенні якого доступ до сервера здійснюється через протокол віддаленого робочого столу (RDP). Цей підхід є оптимальним для гібридних інфраструктур та тестування нових можливостей ОС [3].

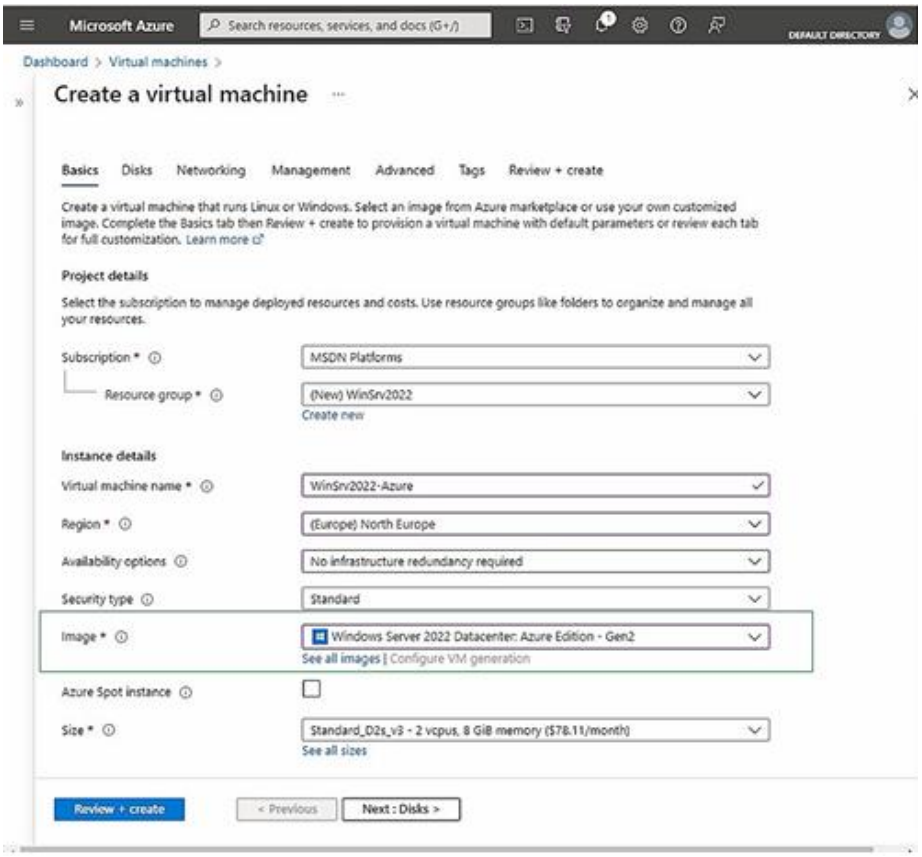

Рисунок 3.14 – Налаштування віртуальної машини з Windows Server 2025 в Azure [3]

Ролі та компоненти ОС

Перед призначенням ролей серверу необхідно чітко визначити його передбачувану функцію в IT-інфраструктурі організації. Цей розділ забезпечує всебічний огляд різноманітних ролей, служб ролей та компонентів, доступних у Windows Server 2025, що сприяє прийняттю обґрунтованих рішень щодо конфігурації сервера.

Роль сервера визначає основну функцію, яку сервер виконує в мережі. Наприклад, якщо основною метою сервера є зберігання та керування спільними файлами, для виконання цього завдання інсталюється роль «Файлові служби та служби зберігання» (File and Storage Services). Аналогічно, сервер, призначений для розміщення веб-додатків, використовуватиме роль «Веб-сервер (IIS)» для безпечної обробки запитів HTTP, забезпечуючи важливу

платформу для інтернет- та інтранет-сервісів. Сервери, що уможливлюють безпечний віддалений доступ, реалізують роль «Віддалений доступ» (Remote Access), яка полегшує рішення для підключення, такі як віртуальні приватні мережі (VPN) та DirectAccess, дозволяючи користувачам безпечно отримувати доступ до мережевих ресурсів з віддалених локацій. У більшості випадків призначення однієї ролі кожному серверу є оптимальним, оскільки це забезпечує оптимізовану продуктивність та спрощує керування сервером. Однак існують сценарії, коли на одному сервері може бути розгорнуто кілька ролей. У таких випадках необхідне ретельне планування для збалансування апаратних ресурсів відповідно до вимог конкретних ролей, забезпечення сумісності та запобігання потенційним конфліктам або вузьким місцям у продуктивності. Такий модульний підхід дозволяє Windows Server 2025 служити для низки цілей в організації, де кожна роль робить внесок у надійну, чуйну та безпечну мережеву інфраструктуру [3].

Окрім базових ролей, Windows Server 2025 пропонує служби ролей – додаткові компоненти, що покращують або розширюють функціональність ролі сервера. Ці служби дозволяють адміністраторам адаптувати можливості сервера до конкретних потреб. Наприклад, увімкнення віддаленого друку через Інтернет вимагає не лише встановлення ролі служб друку та документів (Print and Document Services), але й додавання служби ролі «Інтернет-друк». Такий багаторівневий підхід дозволяє налаштувати функціональність сервера для відповідності точним операційним вимогам, забезпечуючи гнучкість у тому, як сервер підтримує потреби організації [3].

Windows Server 2025 включає ряд вбудованих ролей та компонентів, розроблених для підтримки критичних потреб інфраструктури без покладання на додаткові додатки. Вибір для висвітлення трьох конкретних ролей – служб сертифікації Active Directory (AD CS), служб керування правами (RMS) та сервера політик мережі (NPS) – ґрунтується на їхній актуальності для фундаментальних аспектів керування Windows Server: безпеки, контролю доступу та захисту даних. Ці ролі забезпечують суттєві інфраструктурні можливості, на які покладаються багато організацій, незалежно від додаткових додатків, таких як Exchange або SQL Server [18].

Служби сертифікації Active Directory (AD CS) забезпечують масштабований, безпечний метод видачі та керування цифровими сертифікатами в організації. Це є фундаментальним для підтримки безпечної комунікації, цілісності даних та автентифікації користувачів. Роль відіграє вирішальне значення в середовищах, що пріоритезують безпеку, уможливлюючи виконання таких завдань, як SSL/TLS для веб-сайтів та автентифікація користувачів і пристроїв.

Служби керування правами (RMS) є життєво важливими для захисту інформації та убезпечення конфіденційних документів і комунікацій шляхом забезпечення дотримання

обмежень доступу та використання. Це гарантує, що лише авторизовані користувачі можуть взаємодіяти із захищеним вмістом, що є особливо критичним у галузях, які працюють з чутливими або регульованими даними.

Сервер політик мережі (NPS) функціонує як сервер RADIUS, підтримуючи централізовану автентифікацію доступу до мережі, авторизацію та облік. Ця можливість є безцінною для керування безпечним доступом до мережі, особливо в середовищах, де важлива інтеграція кількох сайтів та хмари, полегшуючи безпечні з'єднання для VPN, бездротових мереж та інших рішень віддаленого доступу.

Хоча ці ролі є критичними, Windows Server 2025 також включає кілька інших цінних вбудованих функцій, які потребують дослідження. До них належать «Файлові служби та служби зберігання», які є невід'ємною частиною централізованого спільного доступу до файлів, керування зберіганням та дедуплікації даних, вирішуючи основні потреби в мережевих середовищах. Роль Hyper-V є важливою для організацій, що використовують віртуалізацію, оптимізуючи використання серверів та забезпечуючи ізольовані віртуальні середовища для різних додатків.

Ролі DNS та DHCP є фундаментальними для мережевої інфраструктури, забезпечуючи розпізнавання доменних імен та керування IP-адресами (IPAM). Служби оновлення Windows Server (WSUS) є критичними для керування виправленнями, гарантуючи, що сервери та підключені пристрої отримують своєчасні оновлення для підтримання безпеки та відповідності вимогам. Розширення огляду на ширший вибір цих ролей забезпечує більш повне уявлення про вбудовані можливості Windows Server, оснащуючи адміністраторів міцною основою для керування безпекою мережі, відповідністю та доступністю. Це розуміння закладає підґрунтя для розширення функціональних можливостей сервера за допомогою додаткових додатків, підкреслюючи важливість вбудованих функцій у середовищах Windows Server [3].

На додаток до ролей та служб ролей, компоненти сервера є допоміжними елементами, що підтримують або покращують конкретні функції в серверному середовищі. Наприклад, встановлення компонента .NET Framework 3.5 може бути необхідним для запуску певних програм або служб. Натомість компонент IPAM надає розширені можливості керування для ролей DHCP та DNS. Такі компоненти, як WINS, можуть бути вирішальними в середовищах, де необхідне розпізнавання імен NetBIOS у кількох підмережах. Шляхом ретельного вибору та встановлення відповідних компонентів забезпечується повна оснащеність сервера для ефективного виконання призначених завдань, що сприяє загальній стабільності та продуктивності IT-інфраструктури. Підсумовуючи, розуміння та стратегічне налаштування ролей, служб ролей та компонентів у Windows Server 2025 є ключовим для оптимізації продуктивності сервера та задоволення унікальних потреб IT-середовища організації.

Диспетчер серверів (Server Manager) є основним інструментом для додавання, налаштування та керування ролями серверів у Windows Server 2025. Вперше представлений у Windows Server 2008, цей інструмент постійно вдосконалювався, пропонуючи оптимізований та інтуїтивно зрозумілий інтерфейс, що спрощує адміністрування сервера. Незалежно від того, чи виконується робота з локальним сервером, чи здійснюється керування віддаленими серверами, Server Manager дозволяє ефективно встановлювати та контролювати ролі серверів. Інтерфейс розділено на дві основні секції: панель області, яка відображає всі встановлені ролі, та панель деталей, яка надає вичерпну інформацію та опції керування для кожної обраної ролі. Ця центральна консоль не лише допомагає у моніторингу стану та продуктивності сервера, але й дозволяє легко отримувати доступ до інструментів та налаштувань, специфічних для ролі (рис. 3.15).

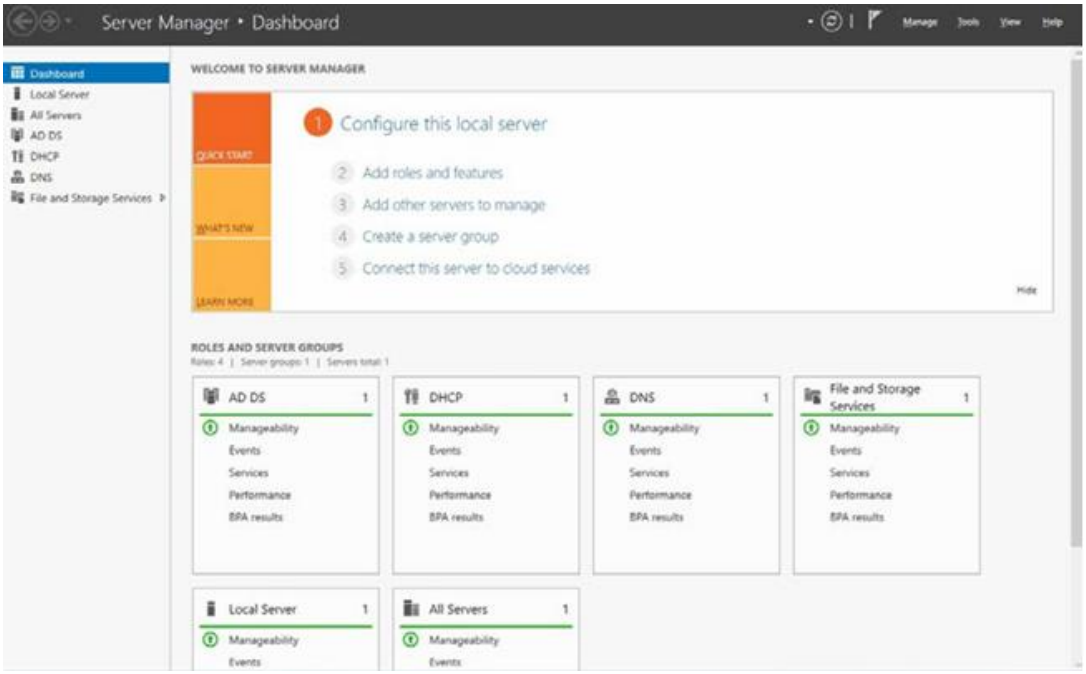

Рисунок 3.15 – Інтерфейс Диспетчера серверів у Windows Server 2025 [3]

Налаштування різних видів доступу

Ефективне адміністрування серверної інфраструктури неможливе без розуміння та правильної конфігурації механізмів доступу. У середовищі Windows Server 2025 реалізовано багаторівневу модель керування, яка передбачає перехід від локальної взаємодії до віддалених, автоматизованих та веб-орієнтованих інтерфейсів. Вибір методу доступу визначається політикою безпеки, архітектурою мережі (локальна, гібридна, хмарна) та специфікою розгорнутих ролей.

Найпоширенішим методом графічного керування сервером є використання протоколу RDP (Remote Desktop Protocol). В операційних системах сімейства Windows Server за замовчуванням дозволяється два одночасні адміністративні сеанси без необхідності

розгортання ролі сервера терміналів та придбання клієнтських ліцензій (CAL). Доступ здійснюється через порт TCP 3389 [4].

Налаштування здійснюється через властивості системи або за допомогою командлетів PowerShell (Set-ItemProperty), де модифікується реєстр для дозволу підключень. Слід зауважити, що використання RDP для адміністрування контролерів домену вимагає підвищених заходів безпеки, зокрема використання виділених адміністративних робочих станцій (PAW – Privileged Access Workstations) [4].

Сучасним стандартом керування Windows Server 2025 є Windows Admin Center – інструмент, що розгортається локально або на шлюзовому сервері. Архітектурно WAC працює через веб-браузер, використовуючи протокол HTTPS (порт 443 за замовчуванням) для зв'язку з керуючим вузлом, який, у свою чергу, комунікує з керованими серверами через PowerShell Remoting та WMI (Windows Management Instrumentation) поверх WinRM [3].

WAC консолідує більшість адміністративних завдань (керування сертифікатами, моніторинг подій, налаштування мережі, керування оновленнями) в єдиному інтерфейсі. Особливістю WAC є його здатність керувати як локальними серверами, так і віртуальними машинами в Azure, забезпечуючи «єдине вікно» для гібридних інфраструктур. Цей інструмент не вимагає встановлення агентів на цільові сервери, що спрощує його впровадження.

Основним інструментом автоматизації та віддаленого керування серверами, зокрема у конфігурації Server Core, є технологія PowerShell Remoting. Вона базується на протоколі WS-Management та службі WinRM, яка за замовчуванням використовує порти 5985 (HTTP) та 5986 (HTTPS) для забезпечення каналу зв'язку між керуючою станцією та серверами.

Взаємодія реалізується двома методами: через інтерактивні сесії за допомогою командлета Enter-PSSession для керування окремим сервером у реальному часі, або шляхом масового виконання команд через Invoke-Command для одночасної обробки скриптів на групі вузлів. Активація функціоналу здійснюється командою Enable-PSRemoting з можливістю додаткового налаштування безпеки через шифрування та обмеження списків довірених хостів.

RSAT (Remote Server Administration Tools) представляє собою набір класичних оснасток MMC (Microsoft Management Console) та інструментів командного рядка, які встановлюються на клієнтську робочу станцію адміністратора (наприклад, Windows 11). Цей підхід дозволяє керувати ролями сервера (DNS, DHCP, Active Directory) без необхідності прямого входу на консоль сервера через RDP [3].

В контексті адміністрування Windows Server 2025 важливим аспектом є реалізація принципу найменших привілеїв. Технологія JEA (Just Enough Administration) є надбудовою над PowerShell Remoting, яка дозволяє делегувати права адміністрування без надання повних

прав локального адміністратора.

JEA функціонує шляхом створення віртуальних облікових записів та файлів конфігурації сесій, де чітко визначено, які командлети, параметри та модулі доступні конкретному користувачеві. Це дозволяє, наприклад, надати операторам служби підтримки право лише перезапускати службу DNS, забороняючи будь-які інші дії в системі. Впровадження JEA є критичним кроком для захисту від внутрішніх загроз та мінімізації наслідків компрометації облікових записів [3].

Механізми віддаленого управління

Роль «Віддалений доступ» у Windows Server 2025 є комплексним рішенням, що інтегрує технології для забезпечення безпечного підключення до корпоративних ресурсів. До її складу входять DirectAccess, який гарантує безперебійне з'єднання через тунелювання IPv6 поверх IPv4 та шифрування IPsec без необхідності використання традиційного VPN; служба маршрутизації та віддаленого доступу (RRAS), що підтримує маршрутизацію трафіку та створення захищених каналів між підмережами; а також Web Application Proxy, що діє як зворотний проксі-сервер для публікації внутрішніх веб-додатків із використанням автентифікації AD FS. Налаштування цих компонентів розпочинається з додавання відповідної ролі до сервера (рис. 3.16).

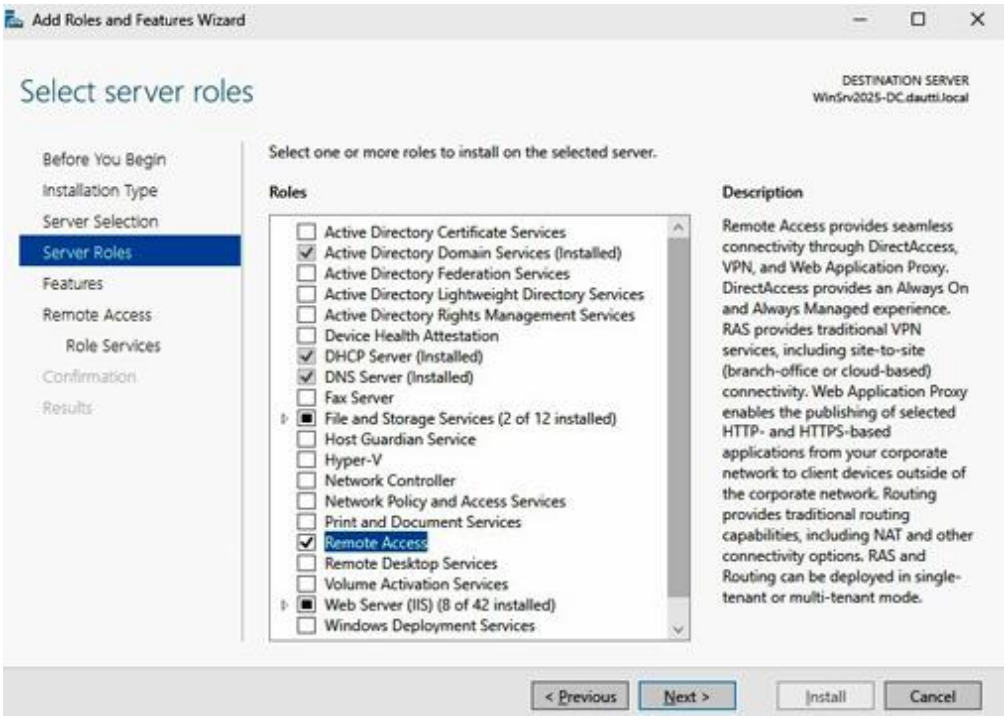

Рисунок 3.16 – Додавання ролі віддаленого доступу в Windows Server 2025 [3]

Механізм «Віддалений помічник» спроектовано для надання технічної підтримки в режимі реального часу, дозволяючи адміністратору (ініціатору) переглядати та керувати

робочим столом користувача (запрошеного). Процес взаємодії регламентується суворими протоколами безпеки: сеанс ініціюється запитом користувача, який надає дозвіл на доступ, що забезпечує контроль над процедурою діагностики та усунення несправностей без фізичної присутності фахівця. Активація функції здійснюється через майстер додавання ролей та компонентів.

Інструменти віддаленого адміністрування сервера (RSAT) дозволяють здійснювати централізоване керування ролями та компонентами серверів Windows Server 2025 із клієнтських робочих станцій під управлінням Windows 10 або 11. Цей набір інструментів включає як графічні інтерфейси, так і засоби командного рядка, забезпечуючи гнучкість адміністрування без необхідності прямого входу на консоль сервера. На відміну від сучасного веб-орієнтованого Windows Admin Center, RSAT представляє класичний підхід до керування інфраструктурою (рис. 3.17).

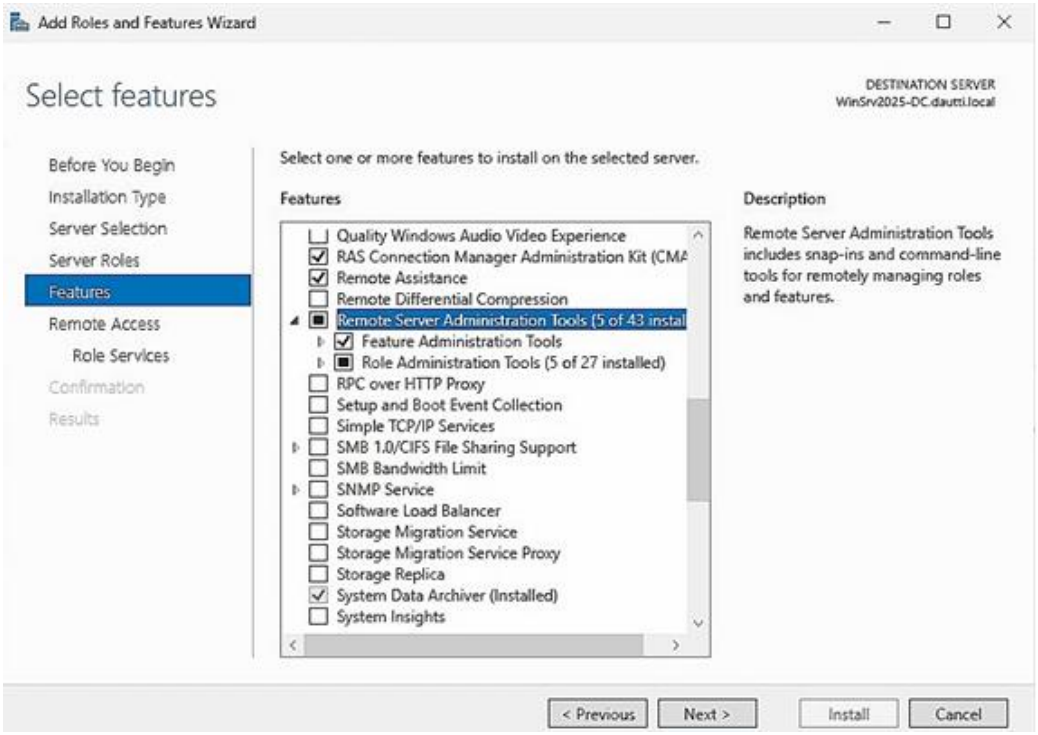

Рисунок 3.17 – Додавання компонента RSAT у Windows Server 2025 [3]

Служби віддалених робочих столів (RDS) забезпечують віртуалізацію сесій та додатків, дозволяючи користувачам працювати з графічним інтерфейсом сервера віддалено. Для функціонування розширеної інфраструктури (понад дві адміністративні сесії) вимагається розгортання сервера ліцензування для керування клієнтськими ліцензіями (RDS CALs) та налаштування шлюзу віддалених робочих столів (RDG). Шлюз виступає посередником, що інкапсулює RDP-трафік у HTTPS-пакети, забезпечуючи захищений доступ до внутрішніх ресурсів через Інтернет без прямого експонування серверів [3].

Технологія VPN реалізує захищений тунель для передачі даних через публічні мережі,

використовуючи протоколи шифрування. У Windows Server 2025 підтримуються конфігурації віддаленого доступу (Remote-Access VPN) для підключення окремих клієнтів та з'єднання типу «сайт-сайт» для об'єднання географічно розподілених мереж. На відміну від DirectAccess, який забезпечує постійне автоматичне з'єднання для доменних комп'ютерів, класичний VPN є більш універсальним рішенням для різнорідних клієнтських пристроїв (рис. 3.18).

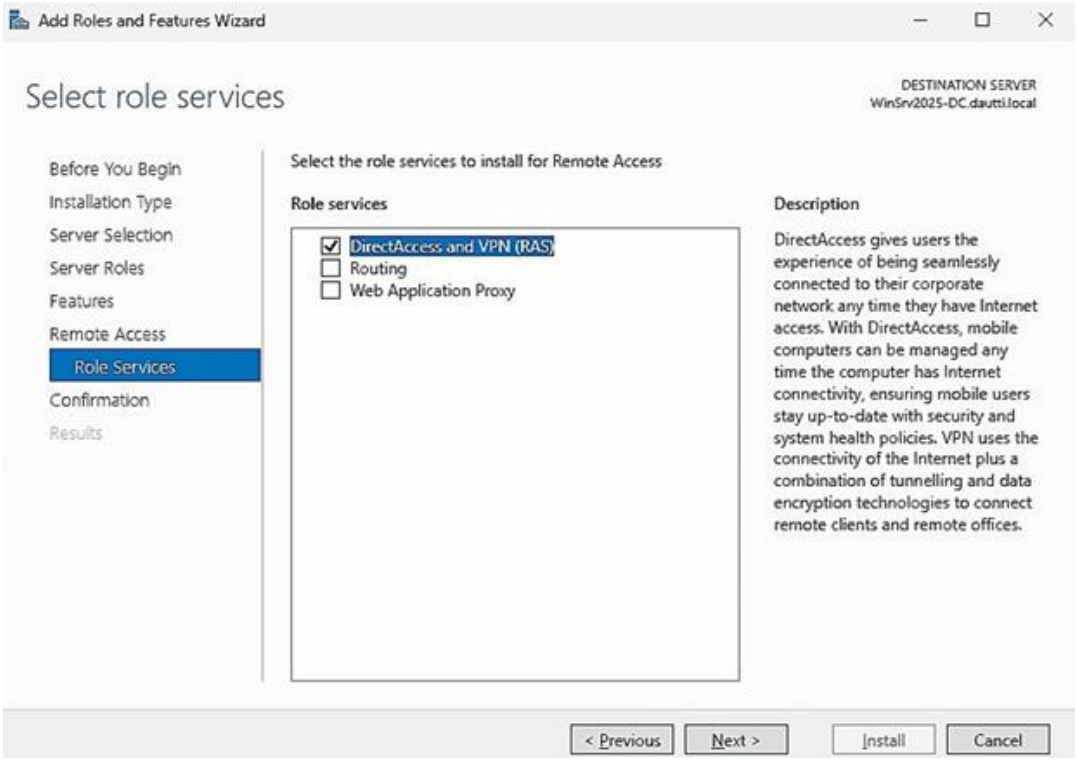

Рисунок 3.18 – Налаштування служб DirectAccess та VPN (RAS) [3]

Система Microsoft App-V дозволяє виконувати додатки без їх локальної інсталяції на кінцевих пристроях, використовуючи технологію потокової передачі з сервера. Це рішення ізолює додатки від операційної системи клієнта, мінімізуючи конфлікти сумісності (DLL hell) та спрощуючи процес оновлення програмного забезпечення. У сучасних сценаріях App-V часто інтегрується у хмарні середовища для підвищення масштабованості, а його впровадження вимагає використання пакету MDOP.

Для коректної маршрутизації трафіку в системах віддаленого доступу використовується механізм IP-сокетів, що поєднує IP-адресу вузла та номер порту (наприклад, 192.168.1.10:3389). Стандартний порт для RDP – 3389, проте для забезпечення одночасної роботи кількох сервісів або перенаправлення портів використовуються альтернативні значення (3390 і далі). Розуміння адресації на рівні сокетів є необхідним для налаштування правил брандмауера та коректної роботи служб RDS і App-V.

Резервне копіювання та архівація

Однією з першочергових відповідальностей в адмініструванні серверів є захист даних від втрати або пошкодження. Для реалізації цього завдання критично важливим є резервне копіювання, яке уможливлює дублювання даних на альтернативні локації або пристрої. Проте ефективність резервного копіювання безпосередньо залежить від здатності відновити дані у разі необхідності. Процес відновлення передбачає вилучення даних із резервних копій та їх розгортання на сервері.

Існує кілька типів резервного копіювання, що задовольняють різні потреби залежно від частоти та обсягу робіт. Повне резервне копіювання створює повну копію всіх даних сервера; для відновлення потрібна лише остання повна копія, що забезпечує найпростіший процес реставрації.

Інкрементальне резервне копіювання зберігає лише дані, змінені з моменту останнього резервного копіювання будь-якого типу. Зазвичай воно виконується щодня, крім дня повного копіювання (часто п’ятниці), що пришвидшує процес бекапу, але вимагає наявності останньої повної копії та всіх наступних інкрементальних копій для відновлення, роблячи цей процес більш тривалим [4].

Диференційне резервне копіювання зберігає дані, модифіковані з моменту останнього повного копіювання. Для відновлення потрібні остання повна та найсвіжіша диференційна копії, що прискорює відновлення порівняно з інкрементальним методом, але може уповільнити процес створення копії [4].

Вибір носіїв для резервного копіювання залежить від важливості та обсягу даних. Доступні опції включають CD, DVD, знімні жорсткі диски, стрічкові накопичувачі, мережеві сховища (NAS) та мережі зберігання даних (SAN). Останнім часом організації все частіше впроваджують онлайн-сервіси резервного копіювання через їхню зручність, безпеку та економічну ефективність. Додатково широко застосовується схема ротації резервних копій «Дід-Батько-Син» (Grandfather-Father-Son, GFS), яка забезпечує структуровану та надійну стратегію: щоденні копії позначаються як «син», щотижневі – як «батько», а щомісячні – як «дід» [4].

У середовищі Windows Server 2025 ключовим інструментом захисту даних є компонент Windows Server Backup, активація якого здійснюється через консоль Server Manager. Процедура налаштування розпочинається з натискання комбінації клавіш Windows + R, введення команди servermanager.exe та підтвердження вводу. У консолі диспетчера серверів необхідно обрати пункт «Додати ролі та компоненти». Після проходження вступної сторінки та вибору типу встановлення «На основі ролей або компонентів» (Role-based or Feature-based Installation), обирається цільовий сервер із пулу. Оскільки додавання нових ролей не вимагається, цей крок пропускається. На сторінці вибору компонентів (Features)

слід знайти у списку та відмітити пункт Windows Server Backup (рис. 3.19).

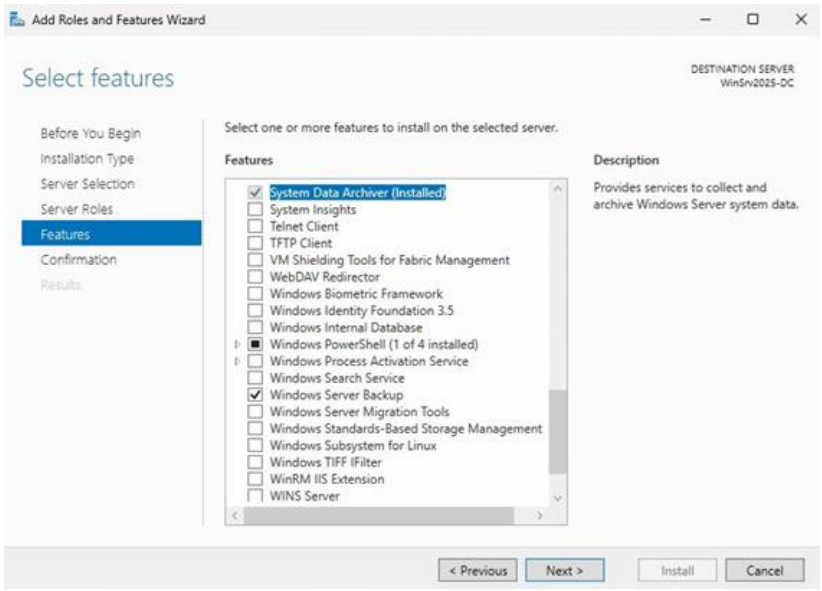

Рисунок 3.19 – Встановлення компонента Windows Server Backup [3]

Після підтвердження вибору натисканням кнопки «Install» на сторінці підтвердження розпочинається процес інсталяції, по завершенні якого роботу майстра слід завершити кнопкою «Close». Після встановлення Windows Server Backup система готова до виконання подальших завдань, зокрема відновлення Active Directory.

Традиційні методи, такі як носії з одноразовим записом (WORM), цифрова аудіострічка (DAT) та технологія Travan (TDLT), стають менш поширеними через обмеження у масштабованості, швидкості та доступності за межами майданчика. Натомість сучасні рішення, такі як аварійне відновлення як послуга (DRaaS) та резервне копіювання як послуга (BaaS), набувають популярності завдяки можливостям безпечного, масштабованого та ефективного захисту даних у віддаленому режимі. Ці сервіси дозволяють організаціям зберігати копії у хмарних сховищах, гарантуючи збереження та доступність критичних даних навіть у разі катастроф. Використання DRaaS та BaaS дозволяє бізнесу вдосконалити стратегії бекапу, покращуючи можливості відновлення та загальну безперервність бізнес-процесів, а також масштабувати ресурси відповідно до зростання потреб без ускладнення локальної інфраструктури [3].

Аналіз системних журналів

Засіб перегляду подій (Event Viewer) є важливим інструментом для системних адміністраторів, спроектованим для сприяння усуненню несправностей в операційних системах Windows шляхом надання комплексного огляду подій, що відбуваються на серверах. Ця утиліта реєструє та відображає записи критичних дій та модифікацій, які впливають на

програмне забезпечення, апаратне забезпечення або мережеві компоненти сервера. За допомогою засобу перегляду подій адміністратори мають можливість ефективно здійснювати моніторинг продуктивності та безпеки сервера, а також точно визначати першопричини різноманітних проблем. Шляхом аналізу зареєстрованих подій можна отримати цінну інформацію про операції системи та оперативно вирішувати проблеми, забезпечуючи оптимальну функціональність та стабільність сервера.

Засіб перегляду подій, інтерфейс якого представлено на рисунку 3.20, розроблено для полегшення діагностики різноманітних проблем шляхом надання детального звіту про події. Він пропонує для моніторингу п’ять різних типів журналів, кожен з яких слугує певній меті. Журнали програм (Application logs) фіксують події, згенеровані додатками, що виконуються на сервері. Журнали безпеки (Security logs) відстежують події, пов’язані з безпекою, такі як невдалі спроби входу або доступ до обмежених папок, що вимагає попереднього увімкнення аудиту. Журнали інсталяції (Setup logs) записують події, пов’язані зі встановленням та налаштуванням додатків, тоді як системні журнали (System logs) документують події, що стосуються функціонування компонентів ОС Windows [3].

Окремо виділяють журнали пересланих подій (Forwarded events logs), які містять події, зібрані з віддалених комп’ютерів, що потребує налаштування підписки. Варто зауважити, що необхідно коректно налаштувати мінімальний час зберігання журналів, оскільки за замовчуванням вони перезаписуються при досягненні максимального розміру файлу, що може призвести до втрати критичної інформації. Параметри зберігання коригуються через групову політику або редактор реєстру.

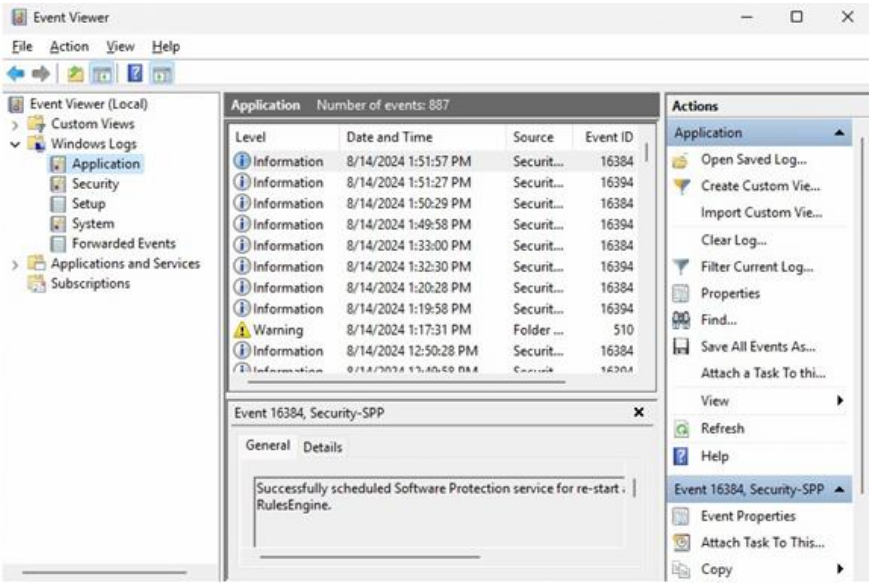

Рисунок 3.20 – Засіб перегляду подій (Event Viewer) [3]

Практичне застосування засобу перегляду подій передбачає виконання низки завдань, спрямованих на покращення нагляду за системою. Централізований моніторинг дозволяє

збирати та переглядати події з декількох серверів в одній локації за допомогою налаштування підписки на події через Windows PowerShell або консоль Event Viewer. Це значно спрощує аналіз активності серверів.

Паралельно з цим, важливим аспектом є фільтрація журналів, яка необхідна для зосередження уваги на конкретних подіях, релевантних для діагностики. Застосування фільтрів базується на таких критеріях, як ім'я журналу, рівень події, дата, джерело, ID події або ключові слова, з можливістю збереження налаштувань як настроюваних подань. Крім того, адміністратори можуть змінювати розташування журналів за замовчуванням для звільнення місця на системному диску або покращення продуктивності, використовуючи редактор реєстру або команду wevtutil.

Реалізація централізованого моніторингу в Windows Server 2025 вимагає послідовного виконання конфігураційних дій. Процес розпочинається із запуску командного рядка від імені адміністратора та введення команди winrm quickconfig для налаштування віддаленого керування. Далі через консоль «Керування комп'ютером» у розділі «Локальні користувачі та групи» до групи «Адміністратори» додається об'єкт Центрального сервера. Наступним кроком у командному рядку виконується команда wecutil qc з підтвердженням дії. Після запуску утиліти eventvwr.exe створюється нова підписка у розділі «Підписки», де вказуються її ім'я та опис. Цільовим журналом визначаються «Переслані події». Як показано на рисунку 3.21, через меню «Вибрати комп'ютер» додаються віддалені сервери для збору подій. Процес завершується визначенням критеріїв фільтрації через опцію «Вибрати події» та налаштуванням облікового запису комп'ютера у меню «Додатково» [3].

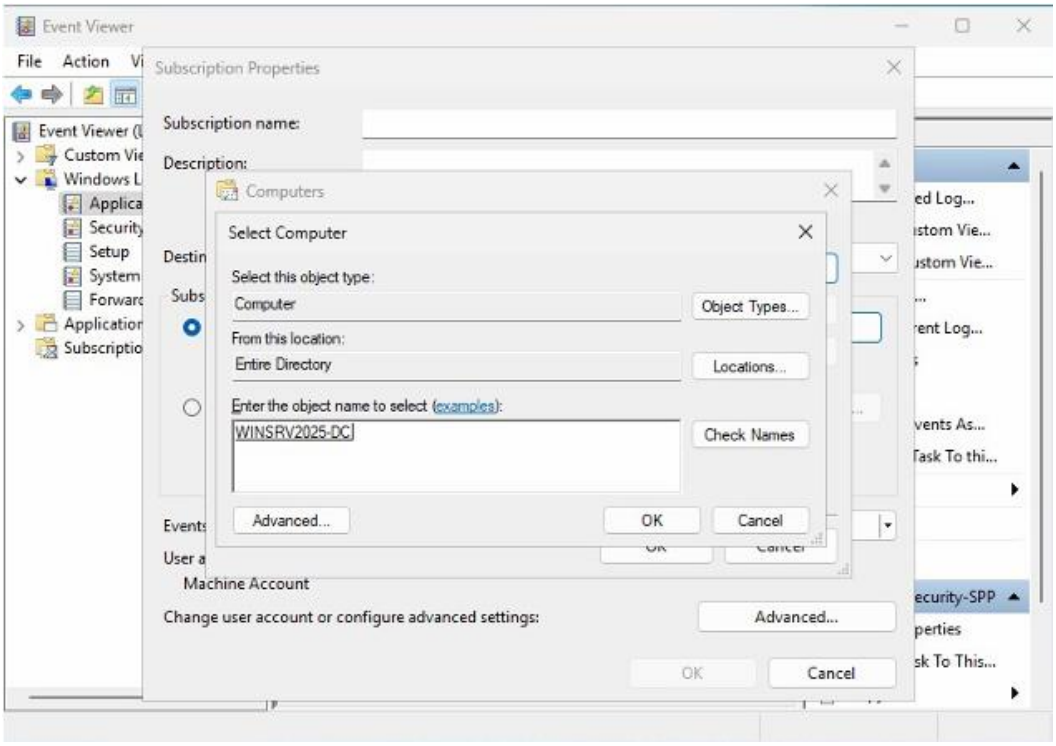

Рисунок 3.21 – Додавання віддаленого сервера для збору подій [3]

Для уточнення масиву даних у журналах використовується механізм фільтрації. Після запуску консолі eventvwr.msc здійснюється перехід до розділу «Журнали Windows», де обирається необхідна категорія (наприклад, Система або Безпека). На панелі дій активується функція «Фільтрувати поточний журнал», інтерфейс якої представлено на рисунку 3.22. У вікні налаштувань визначаються специфічні параметри, такі як рівень події, джерело або ключові слова, що дозволяє адаптувати відображення записів до поточних діагностичних потреб. Застосування фільтра відбувається після підтвердження налаштувань, що призводить до відображення уточненого списку подій.

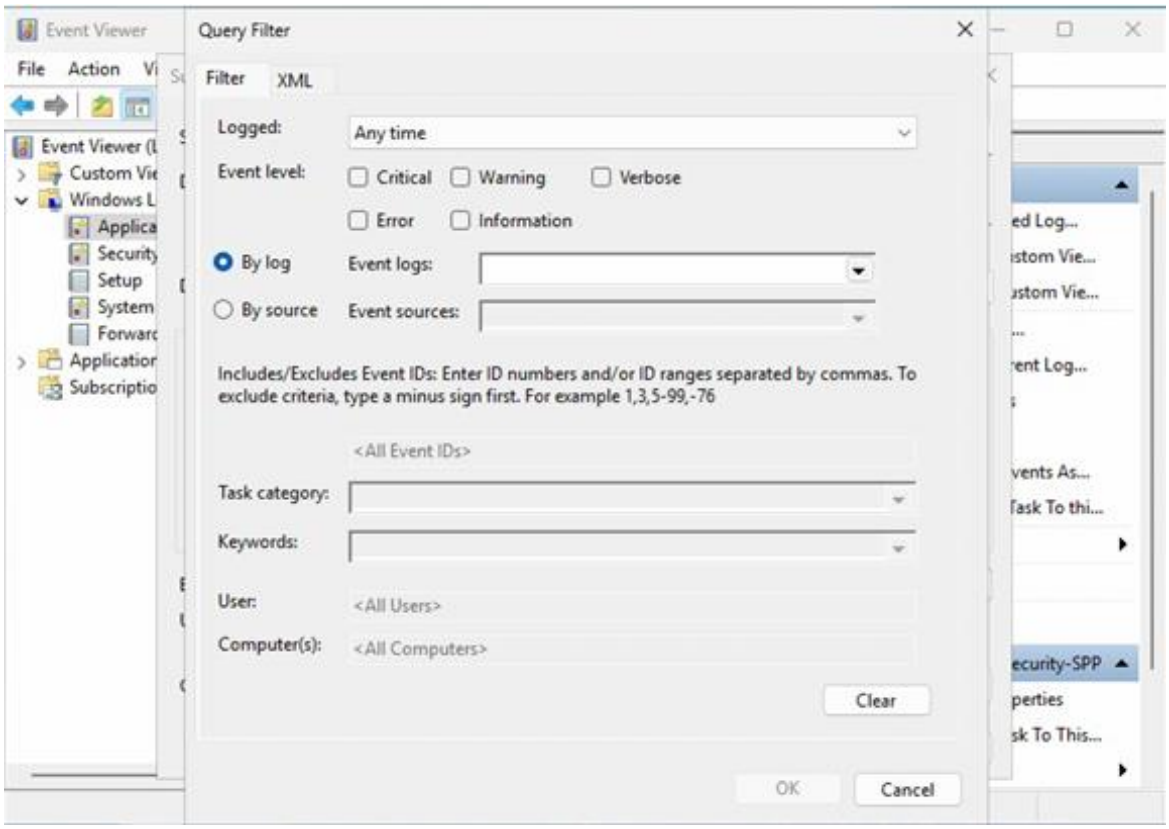

Рисунок 3.22 – Фільтрація журналів засобу перегляду подій [3]

Зміна стандартного розташування файлів журналів у Windows Server 2025 виконується шляхом редагування системного реєстру. Процедура ініціюється запуском редактора реєстру командою regedit. Для зміни шляху системного журналу необхідно перейти до гілки HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System. У даному розділі модифікується значення параметра File, де вказується новий шлях до файлу, як це продемонстровано на рисунку 3.23. Аналогічні дії виконуються у відповідних гілках для журналів програм (...EventLog\Application) та журналів безпеки (...EventLog\Security). Коректне виконання цих маніпуляцій дозволяє перенаправити потік запису подій на інші носії, що є важливою складовою стратегії керування дисковим простором сервера.

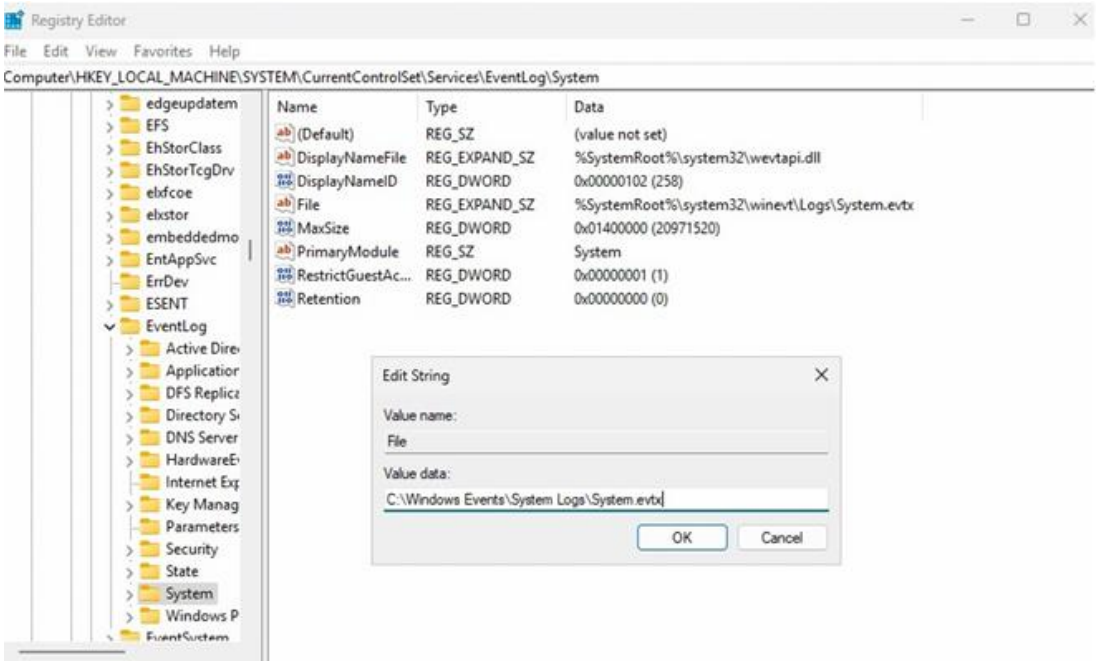

Рисунок 3.23 – Зміна розташування журналів за замовчуванням [3]

Тема 4
Active Directory

Вступ до служб доменів Active Directory

Технології Active Directory від корпорації Microsoft пройшли значний шлях розвитку з моменту їх первинного випуску у складі Windows Server 2000. Трансформувавшись із єдиного продукту, який позначався просто як Active Directory або AD, у середовищі Windows Server 2025 даний напрямок тепер охоплює загалом п’ять окремих технологій Active Directory. Кожна з цих технологій має подібну природу – всі вони існують для забезпечення функціонування служб каталогів та слугують платформою для майбутньої інтеграції технологій Microsoft. Чотирма додатковими ролями служб Active Directory у Windows Server 2025 є: полегшені служби каталогів Active Directory (Active Directory Lightweight Directory Services – AD LDS), служби федерації Active Directory (Active Directory Federation Services – AD FS), служби сертифікації Active Directory (Active Directory Certificate Services – AD CS) та служби управління правами Active Directory (Active Directory Rights Management Services – AD RMS) [3].

Проте, завжди основна увага зосереджується на традиційній службі Active Directory – доменних службах Active Directory (Active Directory Domain Services – AD DS). Розглядається інформація, необхідна для розуміння сутності AD DS та причин, через які ця технологія стала найбільш поширеною платформою корпоративних каталогів, що використовується на сьогоднішній день.

Проектування Active Directory

Процес проектування Active Directory визначається як етап, що передує будь-якому фізичному впровадженню серверного обладнання. Архітектура каталогу повинна розроблятися з урахуванням довгострокової перспективи, оскільки зміни в базовій структурі після розгортання є ресурсомісткими та технічно складними. Проектування традиційно розділяється на два взаємопов’язані рівні: логічне проектування, що визначає адміністративні межі та ієрархію безпеки, та фізичне проектування, яке відображає топологію мережі та розміщення контролерів домену. Головною метою проектування визначається створення масштабованої системи, що задовольняє вимоги безпеки та бізнес-потреби організації.

На етапі проектування логічної структури першочерговим завданням є визначення кількості лісів та доменів. Ліс розглядається як найвища межа безпеки, і згідно з сучасними рекомендаціями, модель єдиного лісу (Single Forest Model) визнається оптимальною для більшості підприємств. Такий підхід забезпечує спрощене управління, єдину схему та глобальний каталог, мінімізуючи адміністративні витрати на синхронізацію. Створення кількох лісів проектується лише за наявності специфічних вимог до ізоляції, які неможливо

вирішити засобами одного лісу. Стосовно структури доменів, тенденція проектування змістилася в бік спрощення: модель єдиного домену вважається найбільш доцільною, оскільки сучасні можливості AD DS дозволяють ефективно керувати мільйонами об’єктів без необхідності створення додаткових доменів виключно з технічних причин [22].

Важливим аспектом проектування є інтеграція з системою доменних імен (DNS), яка слугує основою для функціонування Active Directory. При виборі простору імен необхідно визначити стратегію, що запобігає конфліктам між внутрішніми та зовнішніми іменами. У сучасних реалізаціях рекомендується використання виділеного субдомену публічного простору (наприклад, corp.company.com) для внутрішньої інфраструктури AD. Використання немаршрутизованих суфіксів, таких як .local, більше не вважається кращою практикою через потенційні проблеми із сумісністю сертифікатів безпеки та інтеграцією з хмарними сервісами. Правильно спроектований простір імен забезпечує коректну реєстрацію службових записів та безперебійну роботу механізмів локалізації служб.

Проектування структури організаційних підрозділів (OU) виконується з метою забезпечення делегування адміністративних повноважень та ефективного застосування групових політик (GPO). Ієрархія OU не обов’язково повинна віддзеркалювати організаційну структуру підприємства; натомість вона проектується на основі адміністративної моделі. Розробляються схеми, що дозволяють застосовувати політики безпеки до конкретних типів об’єктів (користувачів, комп’ютерів, серверів) або географічних одиниць. Гнучкість структури OU дозволяє уникнути створення нових доменів для розмежування прав доступу, що значно спрощує загальну архітектуру [19].

Фізичне проектування зосереджується на оптимізації мережевого трафіку через конфігурацію сайтів та зв’язків між ними. Сайт в Active Directory визначається як сукупність підмереж з високошвидкісним з’єднанням. Правильне проектування топології сайтів є необхідним для контролю трафіку реплікації, який між сайтами піддається стисненню та плануванню, а також для локалізації трафіку автентифікації, щоб клієнтські комп'ютери зверталися до найближчих контролерів домену. Цей етап проектування є сполучною ланкою між логічними компонентами каталогу та реальною мережевою інфраструктурою.

Розуміння інфраструктури Active Directory у Windows Server 2025

Active Directory (AD) визначається як фундаментальна технологія від корпорації Microsoft, що виконує функцію розподіленої служби каталогів. Вона є необхідною для організації та управління мережевими ресурсами в ієрархічний та безпечний спосіб. Система діє як централізоване сховище, де зберігаються критично важливі об’єкти, такі як облікові записи користувачів, комп’ютери, принтери та мережеві служби, кожен з яких має власні унікальні налаштування безпеки. Унікальні атрибути кожного об’єкта в межах AD

уможливлюють гранулярний контроль над управлінням ресурсами, що дозволяє здійснювати точне адміністрування всією мережею. Наприклад, кожен об’єкт, будь то обліковий запис користувача, комп’ютер, принтер або мережева служба, володіє специфічними атрибутами, включаючи ідентифікатори безпеки (Security Identifiers – SIDs), членство в групах та списки контролю доступу (Access Control Lists – ACL). Наявність цих атрибутів надає адміністраторам повноваження визначати індивідуальні дозволи, ролі та політики доступу, гарантуючи, що заходи безпеки та функціональні можливості адаптовані до вимог кожного об’єкта.

Архітектура AD, як проілюстровано на рисунку 4.1, структурується навколо трьох фундаментальних рівнів: домену, який є базовою одиницею адміністрування, що забезпечує межу для політик та налаштувань безпеки; дерева, що являє собою колекцію доменів, пов’язаних безперервним простором імен, відображаючи ієрархічні відносини між ними; та лісу – найвищого рівня організації, який може охоплювати кілька дерев і слугує верхнім шаром, що інтегрує всю службу каталогів [3].

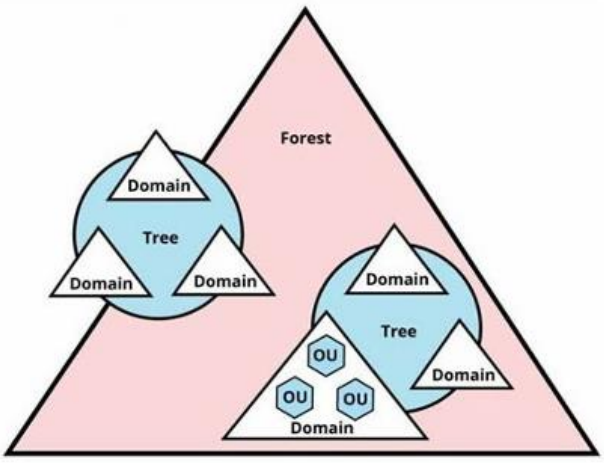

Рисунок 4.1 – Архітектура AD [3]

Такий багаторівневий підхід сприяє ефективному управлінню ресурсами та масштабованості, одночасно підтримуючи складні організаційні структури. Це дозволяє підприємствам налаштовувати свою мережеву інфраструктуру відповідно до специфічних операційних потреб, зберігаючи при цьому надійну безпеку та адміністративний нагляд. У подальшому викладі досліджуються специфічні функції та конфігурації AD, що забезпечує отримання знань та навичок, необхідних для ефективного впровадження та управління службами каталогів в організації.

Active Directory розглядається не просто як служба каталогів, а як основа сучасних IT-інфраструктур, що відіграє критичну роль в управлінні середовищами Windows. Для фахівців-початківців розуміння значущості AD є необхідним для усвідомлення її

функціональних можливостей та переваг.

По-перше, однією з головних переваг визначається здатність централізувати управління. IT-адміністратори можуть керувати користувачами, комп'ютерами та ресурсами з єдиного місця, що значно знижує складність та адміністративні витрати. Цей централізований підхід оптимізує процес надання та скасування доступу користувачів, полегшуючи підтримку організованої та ефективної мережі.

По-друге, AD підвищує рівень безпеки завдяки використанню SIDs та ACLs. Забезпечуючи доступ до конкретних ресурсів лише авторизованим користувачам, AD захищає конфіденційну інформацію та знижує ризик несанкціонованого доступу. Ця модель безпеки є критично важливою для захисту організаційних даних та дотримання нормативних стандартів.

По-третє, ієрархічна структура AD підтримує масштабованість організацій. У міру зростання бізнесу AD дозволяє безперешкодно інтегрувати нових користувачів та ресурси без шкоди для продуктивності або безпеки, що надає можливість адаптуватися до змінних потреб та ефективно розширювати IT-інфраструктуру.

Нарешті, AD сприяє застосуванню групових політик у всій мережі, що дозволяє організаціям уніфіковано впроваджувати налаштування безпеки та стандарти відповідності. Ця можливість гарантує дотримання політик організації всіма користувачами та пристроями, підвищуючи загальний стан безпеки та операційну ефективність. Розуміння цих основних принципів дозволяє оцінити ключову роль AD в управлінні та захисті мережевих ресурсів, що закладає фундамент для ефективного IT-адміністрування.

Функціонування Active Directory спирається на декілька критично важливих протоколів та служб, кожен з яких робить внесок у різні аспекти управління мережею та безпеки. Lightweight Directory Access Protocol (LDAP) є протоколом, який відіграє вирішальну роль у забезпеченні можливості запитів та взаємодії користувачів і додатків з даними каталогу. LDAP надає стандартизований метод доступу та управління інформацією, що зберігається в AD, що робить його ключовим елементом операцій служби каталогів [3].

Іншим важливим компонентом є Kerberos – складний механізм автентифікації, що лежить в основі інфраструктури безпеки AD. Kerberos використовує систему квитків для безпечної перевірки особистості користувачів і серверів у мережі, запобігаючи несанкціонованому доступу та гарантуючи належну автентифікацію всіх суб'єктів. Протокол DNS також є невід'ємною частиною функціональності AD. Він слугує каталогом для Інтернету та внутрішніх мереж, перетворюючи зручні для користувача доменні імена на цифрові IP-адреси. Цей процес трансляції є необхідним для ефективного пошуку та доступу до мережевих ресурсів. У середовищі AD DNS не лише перетворює доменні імена, але й підтримує специфічні функції, такі як визначення розташування контролерів домену та

забезпечення доступності служб у мережі. Разом ці протоколи та служби формують основу AD, дозволяючи надавати безпечну, масштабовану та ефективну службу каталогів [3].

Active Directory є потужною платформою, що надає комплексні послуги для забезпечення централізованого управління мережевими ресурсами, оптимізуючи роботу системних адміністраторів. Для ефективного управління різними аспектами служб AD корпорацією Microsoft пропонується набір адміністративних консолей у рамках Microsoft Management Console (MMC) (mmc.exe), кожна з яких адаптована до конкретних завдань. Центр адміністрування Active Directory (Active Directory Administrative Center – dsac.exe), зображений на рисунку 4.2, є ключовим інструментом в управлінні службами каталогів Windows Server.

Рисунок 4.2 – Центр адміністрування Active Directory у Windows Server 2025 [3]

Цей сучасний інтерфейс інтегрує кілька функцій управління, дозволяючи адміністраторам ефективно контролювати сервіси. Він включає оснастку «Active Directory – користувачі й комп'ютери» (dsa.msc), яка є необхідною для управління обліковими записами користувачів, об'єктами комп'ютерів, організаційними підрозділами та пов'язаними з ними властивостями. Цей інструмент є фундаментальним для повсякденних адміністративних завдань, таких як створення та управління користувачами, групами та пристроями, а також їх організація в структурі AD.

Консоль Active Directory Domains and Trusts (domain.msc) використовується для завдань, пов'язаних з управлінням доменами. Вона дозволяє налаштовувати та керувати довірою доменів, що є критично важливим для забезпечення безпечних комунікацій та спільного використання ресурсів між різними доменами, а також керує функціональними рівнями домену. Консоль Active Directory Sites and Services (dssite.msc) є критично важливим

інструментом для управління реплікацією між різними сайтами AD, що представляють фізичну структуру мережі. Інструмент дозволяє оптимізувати та контролювати реплікацію інформації каталогу між різними географічними локаціями. Окрім графічних інструментів, модуль AD для Windows PowerShell пропонує інтерфейс командного рядка для більш просунутих та автоматизованих завдань управління. Командлети PowerShell дозволяють створювати сценарії для складних операцій, автоматизувати повторювані завдання та керувати об’єктами AD у великих масштабах [20].

Для розгортання служб каталогів в організації необхідно встановити та налаштувати роль AD DS на сервері Windows. AD DS є основою середовища AD, забезпечуючи зберігання, організацію та управління інформацією про мережеві ресурси. Вона також підтримує розширені функції безпеки, такі як централізована автентифікація та авторизація. Варто зазначити, що доступ до великої кількості безкоштовних сценаріїв PowerShell можна отримати в Microsoft Script Center та PowerShell Gallery. Ці платформи слугують відомими репозиторіями, де IT-фахівці можуть знаходити та ділитися сценаріями для різних адміністративних завдань, включаючи ті, що стосуються AD та DNS [21].

Додавання та налаштування ролі AD DS (Active Directory Domain Services)

У середовищах Windows Server роль AD DS визначається як критично важлива для надання централізованих служб каталогів, що полегшують управління мережею та автентифікацію. Ппроцес додавання та налаштування ролі AD DS охоплює ключові завдання, такі як розгортання контролерів домену (DC), налаштування та управління доменами, а також створення ієрархічних структур, таких як дерева та дочірні домени (рис. 4.3).

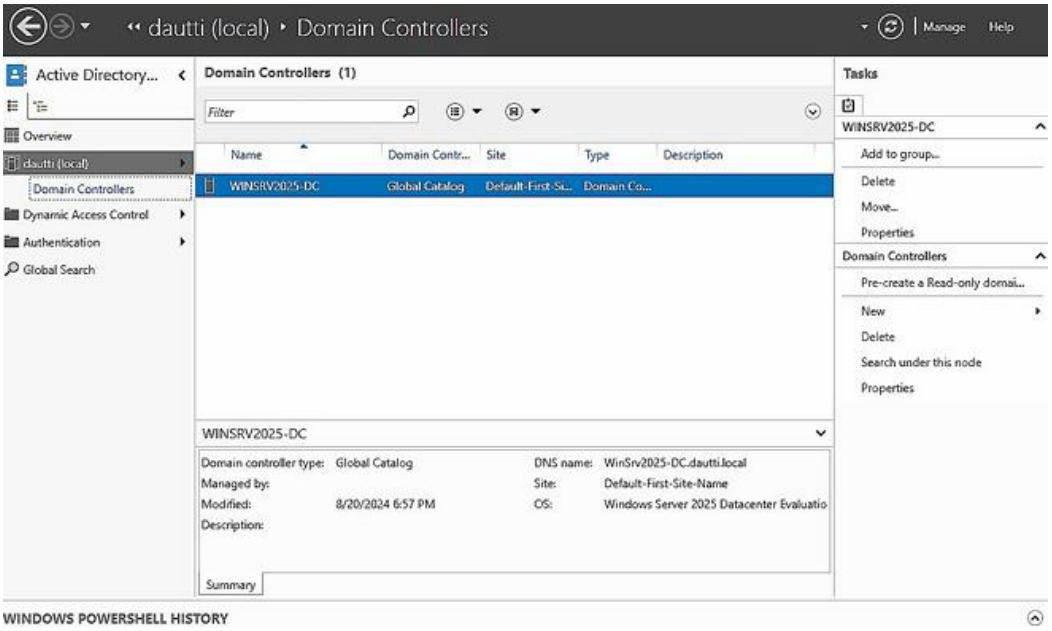

Рисунок 4.3 – Доступ до контролерів домену через Центр адміністрування Active Directory [3]

Контролер домену (DC), як зображено на рисунку 4.3, є сервером, що відіграє критичну роль в управлінні та перевірці ідентичності користувачів у мережі організації. Його основною функцією є автентифікація користувачів та авторизація доступу до мережевих ресурсів на основі політик безпеки, визначених у домені [20].

У ранніх середовищах Windows, зокрема Windows NT, управління доменом покладалося на первинний контролер домену (PDC) для виконання основних функцій та резервні контролери домену (BDC) для забезпечення надлишковості. Проте цю модель було замінено моделлю реплікації з багатьма майстрами (multi-master replication), впровадженою у Windows 2000, що дозволило кільком DC розподіляти відповідальність за управління функціями домену. Такий підхід підвищує надійність та доступність, оскільки всі DC можуть виконувати операції читання та запису, гарантуючи стійкість та доступність служб автентифікації та каталогів у всій мережі. Windows Server 2025 революціонізував підхід до DC, усунувши традиційні ролі первинного та резервного серверів. Натомість DC тепер ідентифікуються за послідовними номерами, наприклад DC1 та DC2, що вказує на їхню черговість, а не функцію. Цей сучасний підхід створює умови для більш гнучкого та масштабованого середовища управління доменом, де всі DC вважаються рівноправними партнерами, що поділяють відповідальність за автентифікацію та служби каталогів. Варто зазначити, що коли сервер приєднується до домену, але не бере на себе роль DC, він класифікується як рядовий сервер. Такі сервери працюють відповідно до політик домену та контролю доступу, але не обробляють запити на автентифікацію та не виконують завдань з управління доменом. Враховуючи, що DC є центральними елементами доступу до домену та автентифікації, розуміння концепції доменів є необхідним для усвідомлення повного обсягу інфраструктури AD [3].

Домени визначаються як фундаментальні компоненти управління мережею, що організовують та групують користувачів, комп’ютери, пристрої та мережеві служби в рамках єдиної адміністративної структури. Це логічне групування дозволяє здійснювати централізоване управління ресурсами та політиками безпеки. DC є критично важливим у цій конфігурації, а AD DS відіграє ключову роль у встановленні та підтримці функціональності домену. На рисунку 4.4 продемонстровано процес налаштування домену у вікні майстра конфігурації Active Directory Domain Services, що ілюструє створення та управління доменами.

Критично важливо розрізняти домен каталогу та доменне ім’я. У контексті служб каталогів домен стосується структурованої бази даних мережевих ресурсів, включаючи користувачів, сервери та пристрої, які керуються колективно відповідно до специфічних адміністративних політик. Цей домен сприяє ефективному управлінню та безпеці в IT-інфраструктурі організації. З іншого боку, доменне ім’я є частиною DNS – ієрархічної

системи імен, що використовується для ідентифікації та локалізації ресурсів в Інтернеті, таких як веб-сайти та сервери електронної пошти. Крім того, домени можуть бути організовані в дерево доменів, яке представляє ієрархічну структуру з кількох доменів. Ця структура дозволяє організувати домени у відносини «батько-дитина», де кожен домен у дереві може успадковувати політики та налаштування від свого батьківського домену, зберігаючи при цьому власну конфігурацію [3].

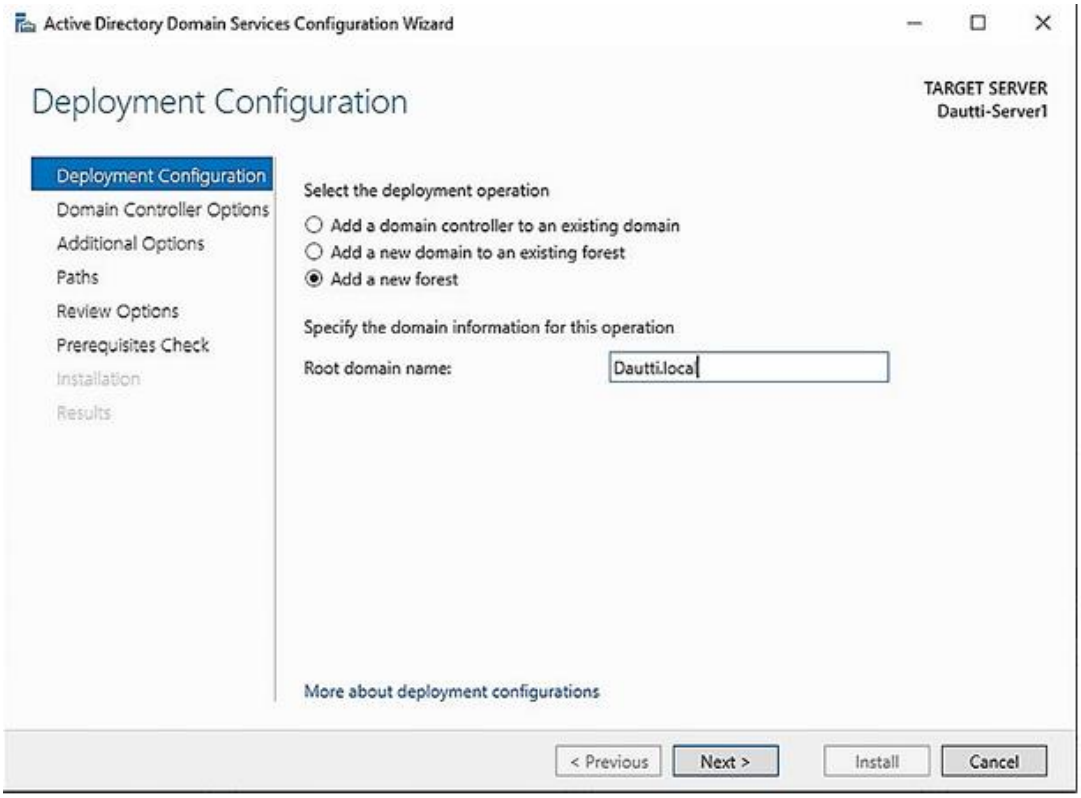

Рисунок 4.4 – Налаштування домену у вікні майстра конфігурації Active Directory Domain Services (налаштування кореневого домену) [3]

Для повного розуміння архітектури AD необхідно розглянути концепцію дерева доменів. Дерево доменів представляє логічну структуру в межах AD, що складається з одного або кількох доменів, які мають спільний простір імен і розташовані ієрархічно. Таке ієрархічне налаштування не лише організовує домени, але й забезпечує їхню взаємну довіру завдяки транзитивним довірчим відносинам. В AD довірчі відносини дозволяють користувачам в одному домені проходити автентифікацію та отримувати доступ до ресурсів в іншому домені без необхідності використання окремих облікових даних.

Транзитивна довіра означає, що якщо домен A довіряє домену B, а домен B довіряє домену C, то домен A автоматично довірятиме домену C. Ця вбудована довіра спрощує спільне використання ресурсів та автентифікацію між доменами в межах одного дерева. Процес впровадження нового домену в існуюче дерево передбачає вказання імені батьківського домену під час підвищення сервера для встановлення відповідної ієрархії. Це

додавання дозволяє новому домену успадковувати політики та налаштування від батьківського, встановлюючи власну унікальну ідентичність у дереві. Рисунок 4.5 надає візуальне представлення створення деревоподібного домену у Windows Server 2025 [3].

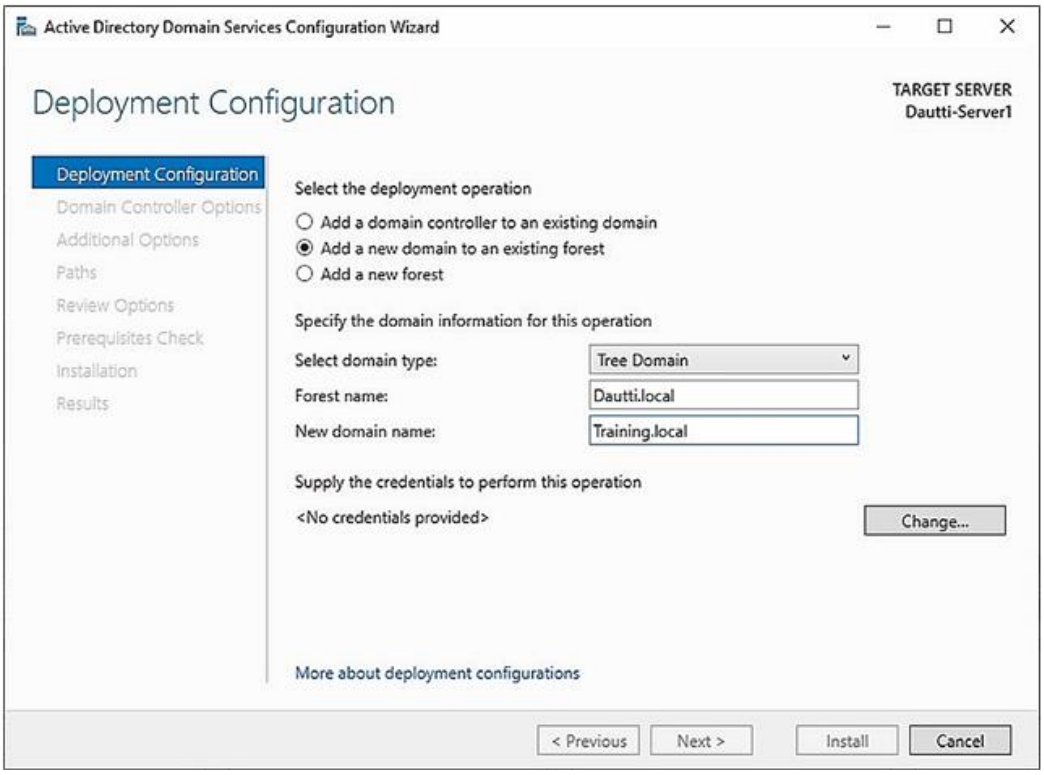

Рисунок 4.5 – Налаштування деревоподібного домену в Windows Server 2025 [3]

Концепція дерева доменів розширюється, коли кілька дерев доменів об’єднуються для формування лісу. Ліс представляє ширшу організаційну структуру, що групує всі дерева доменів підприємства, дозволяючи створити єдине середовище каталогів (рис. 4.6).

В AD концепція лісу аналогічна природному лісу, який складається з багатьох дерев. Ліс AD може складатися з одного дерева доменів або колекції взаємопов’язаних дерев. Кожне дерево доменів у лісі має спільну схему та глобальний каталог, але самі дерева не обов’язково повинні мати спільний простір імен.

Кореневий домен – це перший домен, створений у дереві доменів, що слугує основою для всієї структури. Він часто виконує критичні ролі, такі як майстер схеми та майстер іменування доменів. Дерево доменів, що діє як кореневий домен, може існувати незалежно в лісі, але за наявності кількох дерев ліс діє як всеосяжна структура, що інтегрує та керує цими деревами, створюючи цілісне та масштабоване середовище каталогів [3].

Ліс виступає як найвищий рівень структури AD, забезпечуючи єдину систему каталогів. Для створення та налаштування лісу у Windows Server 2025 використовується майстер конфігурації AD DS, який також застосовується для налаштування дерев доменів.

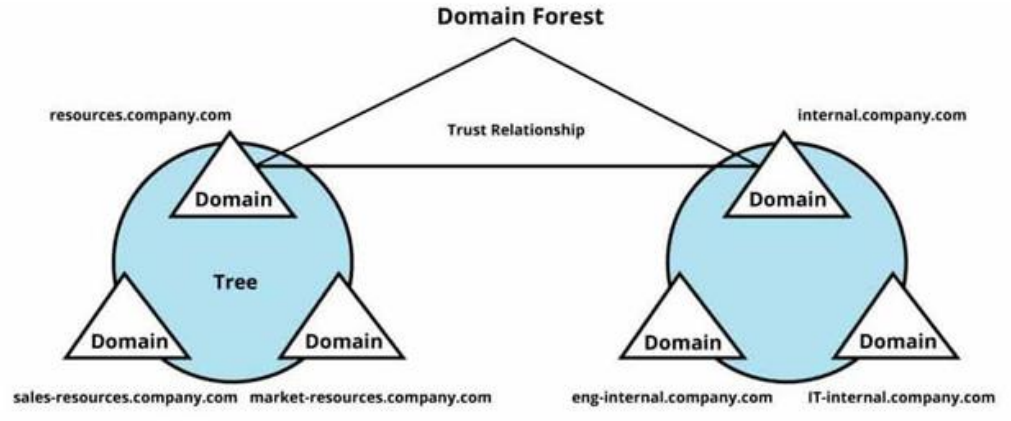

Рисунок 4.6 – Ієрархічна архітектура лісу доменів [3]

У рамках структури дерева доменів можуть бути створені додаткові субдомени, що називаються дочірніми доменами. Вони функціонують як підрозділи батьківського дерева доменів, дозволяючи більш гранулярну організацію та управління ресурсами. Дочірній домен є підпорядкованим доменом у структурі дерева AD. Наприклад, якщо Dautti.local слугує кореневим доменом лісу, встановлюючи базовий простір імен, то Administration.Dautti.local може бути створений як дочірній домен. Він є розширенням простору імен батьківського домену, забезпечуючи цілісну ієрархію каталогів. Створення дочірнього домену у Windows Server 2025 виконується за допомогою майстра конфігурації AD DS, як проілюстровано на рисунку 4.7.

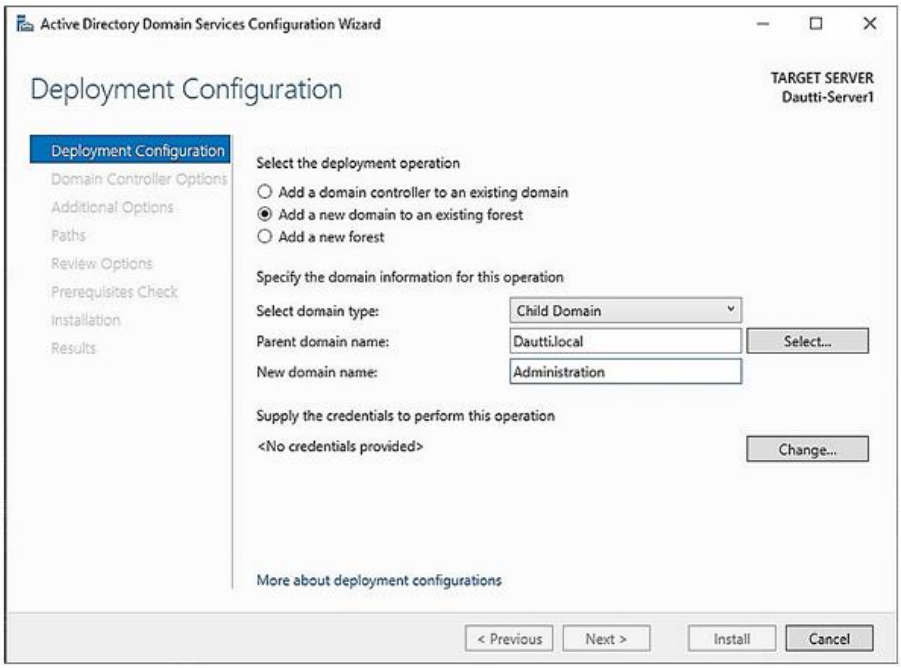

Рисунок 4.7 – Налаштування дочірнього домену в Windows Server 2025 [3]

AD DS є надійною системою, що вимагає ретельного планування. Ключовим компонентом AD DS є ролі майстрів операцій (Operations Master Roles), необхідні для

ефективного управління службами каталогів. При встановленні ролі AD DS та підвищенні сервера до DC автоматично призначаються п’ять критичних ролей майстрів операцій, розділених на дві категорії [3].

Ролі рівня лісу (Forest-wide roles) включають майстра схеми (Schema Master), який контролює схему каталогу, та майстра іменування доменів (Domain Naming Master), що керує простором імен та гарантує унікальність імен доменів у лісі.

Ролі рівня домену (Domain-wide roles) включають RID-майстра (RID Master), що виділяє ідентифікатори безпеки (SIDs), емулятора PDC (PDC Emulator), який обробляє зміни паролів та синхронізацію часу, та майстра інфраструктури (Infrastructure Master), відповідального за оновлення посилань на об’єкти в інших доменах. На рисунку 4.8 проілюстровано структуру AD DS, де кореневий домен утримує ролі рівня лісу, а кожен домен має власні ролі рівня домену.

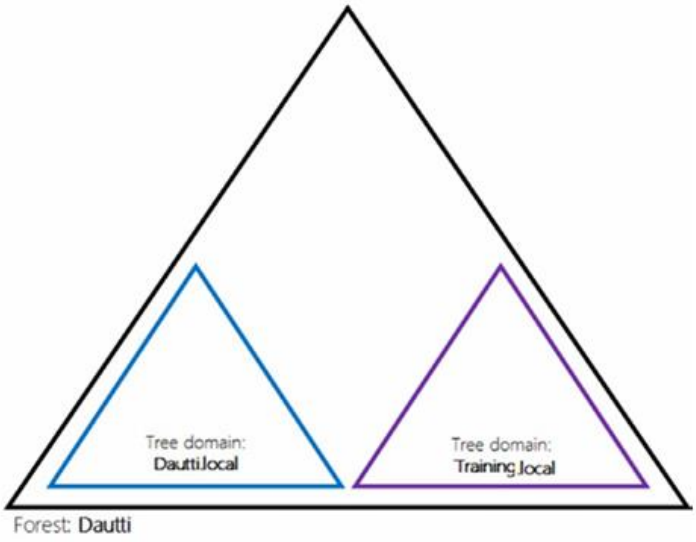

Рисунок 4.8 – Структура AD DS [3]

Ці п’ять ролей відомі як ролі FSMO (Flexible Single Master Operations). Термін «гнучкий» відображає можливість їх перенесення на інші DC, а «єдиний» вказує, що лише один DC може утримувати кожну роль у певний момент часу для запобігання конфліктам.

Для ефективного розрізнення домену та робочої групи (workgroup) важливо розуміти базові архітектури мережі: однорангову (P2P) та клієнт-серверну. У P2P-мережі, або робочій групі, кожен комп’ютер працює незалежно та керує власними ресурсами без централізованого контролю. Це підходить для малих мереж, але ускладнює управління зі зростанням кількості пристроїв. Натомість клієнт-серверна мережа, або домен, забезпечує структурований підхід, де центральний сервер (DC) контролює адміністративні завдання та забезпечує виконання політик безпеки. Централізоване управління є критичним для великих організацій, підтримуючи масштабованість та узгодженість політик.

Ключовою концепцією в AD є довірчі відносини, які відіграють важливу роль у взаємодії комп'ютерів, DC та доменів. Коли комп'ютер інтегрується в домен, він переходить від використання локального менеджера облікових записів безпеки (SAM) до системи автентифікації DC, зазвичай Kerberos. Це централізує автентифікацію та підвищує безпеку. Довірчі відносини поширюються і на рівень лісу, де кожен домен автоматично довіряє методам автентифікації інших доменів, створюючи єдину структуру безпеки (як проілюстровано на прикладі взаємодії доменів у лісі) [3].

Функціональні рівні в AD є критичними елементами, що визначають сумісність та поведінку середовища. Існує два основні рівні: функціональний рівень лісу (FFL) та функціональний рівень домену (DFL) (рис. 4.9).

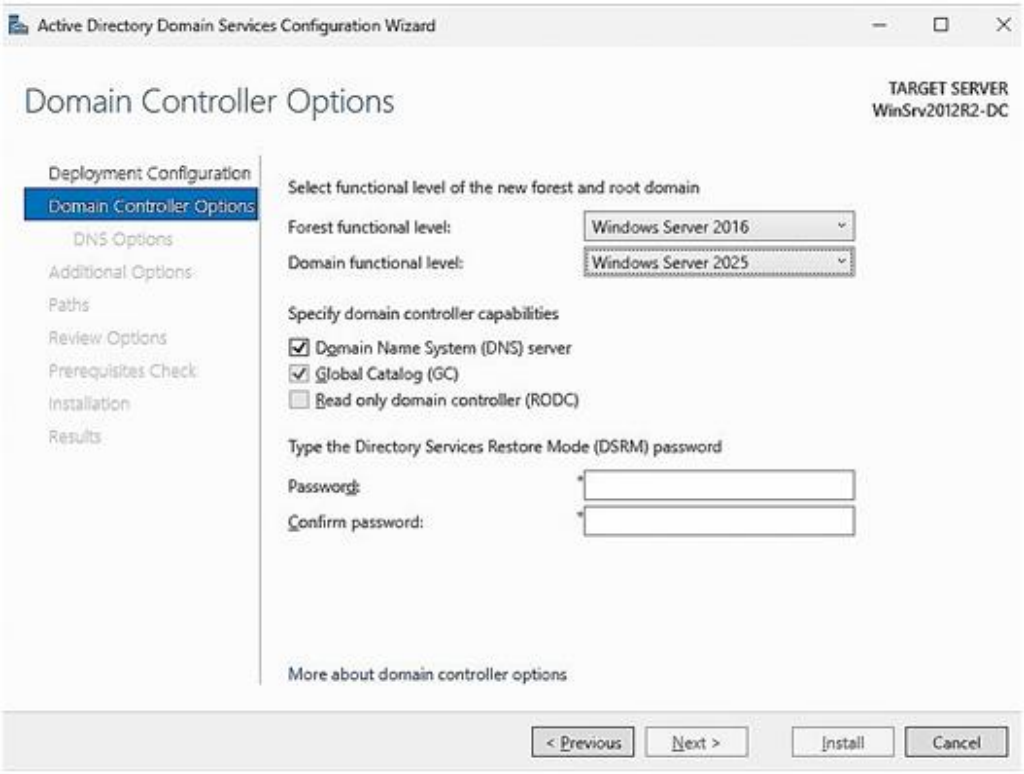

Рисунок 4.9 – FFL та DFL у Windows Server 2025 [3]

FFL визначає, які версії Windows Server можуть працювати на DC у всьому лісі, та розблоковує функції рівня лісу (наприклад, кошик AD). DFL застосовується до окремих доменів, визначаючи підтримувані версії серверів та функції рівня домену. У контексті Windows Server 2025 мінімальні рівні можуть бути встановлені на Windows Server 2016, що забезпечує сумісність. Підвищення рівнів до Windows Server 2025 активує найсучасніші функції. Важливо зазначити, що після підвищення функціонального рівня його не можна знизити. Для перевірки та управління рівнями використовується інструмент «Active Directory – домени і довіра» (Active Directory Domains and Trusts), де у властивостях кореневого домену відображаються поточні значення, як показано на рисунку 4.10.

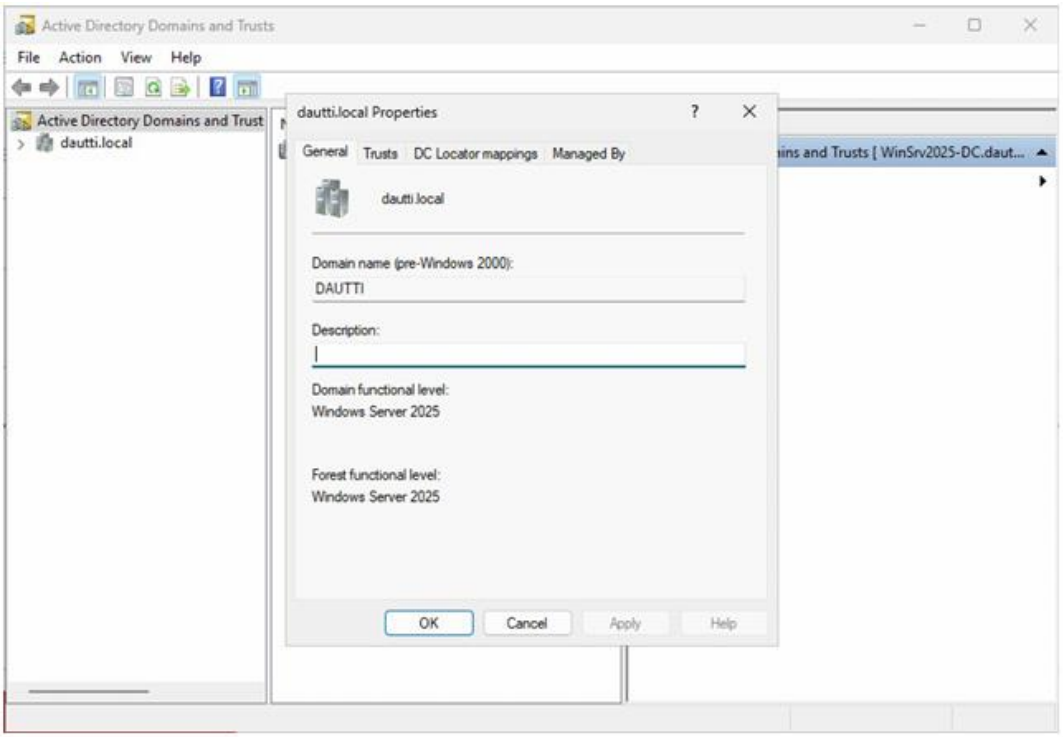

Рисунок 4.10 – Перевірка FFL та DFL [3]

В AD DS концепція простору імен є фундаментальною для організації доменів та лісів. Простір імен слугує логічним ідентифікатором, що унікально називає домен або ліс. Наприклад, як показано на рисунку 4.11, домен Dautti.local функціонує як кореневий домен та ліс, а ITTrainings.local та Administration.local є окремими деревами доменів.

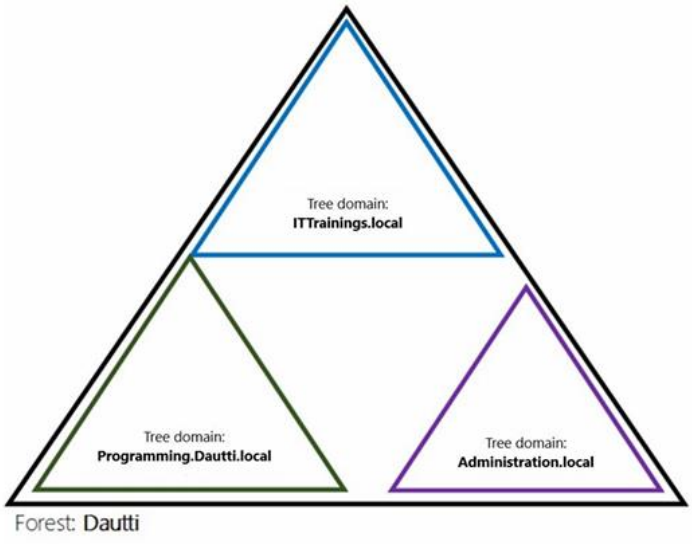

Рисунок 4.11 – Концепція простору імен у AD DS [3]

Спільний компонент Dautti.local вказує на безперервний простір імен, що означає зв’язок усіх доменів через спільну угоду про іменування. Це можна порівняти з системою URL в Інтернеті. Безперервний простір імен забезпечує логічний зв’язок доменів,

полегшуючи управління та навігацію [3].

Окрім логічної структури, AD включає фізичну структуру, відому як сайт. Сайт представляє конкретне фізичне розташування в мережевій інфраструктурі та може охоплювати один або кілька доменів, з'єднаних високошвидкісними каналами. Метою визначення сайтів є оптимізація мережевого трафіку, зокрема реплікації та автентифікації. Сайти зменшують непотрібний трафік через глобальні мережі (WAN), обмежуючи реплікацію швидкими локальними каналами. Також AD спрямовує запити автентифікації до DC у тому ж сайті, де знаходиться користувач, що пришвидшує процес входу.

Реплікація в AD є базовою функцією, що забезпечує узгодженість даних на всіх DC лісу. Процес реплікації безперервно поширює зміни (облікові записи, політики), запобігаючи конфліктам. Ефективність реплікації керується топологією, яку автоматично генерує та оптимізує перевірка узгодженості знань (Knowledge Consistency Checker – KCC). KCC створює маршрути реплікації, балансуючи навантаження. Розрізняють внутрішньосайтову (intra-site) реплікацію, що відбувається часто та швидко, та міжсайтову (inter-site) реплікацію, яка є менш частою та оптимізованою для збереження пропускної здатності WAN [3].

На завершення розгляду інфраструктури, схема в AD визначається як критичний компонент, що є проектом організації даних. Вона складається з трьох елементів: об'єктів (сутності, такі як користувачі), класів (категорії об'єктів, що визначають їх тип) та атрибутів (властивості об'єктів). Схема диктує, як дані зберігаються та організовуються, забезпечуючи стабільність інфраструктури AD.

Керування організаційними одиницями (OU) та типовими контейнерами

Розуміння ролей організаційних одиниць (Organizational Units – OU) та контейнерів визначається, як основа ефективного управління Active Directory. Ці елементи, доступні через консоль «Active Directory – користувачі й комп'ютери» (AD Users and Computers), є невід'ємною частиною організації та адміністрування об'єктів каталогу. OU забезпечують гнучку структуру, дозволяючи адміністраторам створювати ієрархічну організацію в середовищі AD, що полегшує застосування об'єктів групової політики (Group Policy Objects – GPOs) та управління дозволами в різних відділах або групах користувачів. На відміну від них, типові контейнери слугують попередньо визначеними місцями для певних типів об'єктів, таких як користувачі та комп'ютери. Однак їм бракує того ж рівня налаштування та контролю політик, який пропонують OU. У подальшому викладі ці концепції досліджуються глибше, розглядається, яким чином OU можуть бути використані для створення організованої та безпечної інфраструктури AD, а також аналізуються обмеження та використання типових контейнерів. Оволодіння цими компонентами дозволяє адміністраторам підвищити свою здатність ефективно керувати та захищати середовища AD, забезпечуючи добре

структурований та зручний для навігації каталог [3].

Організаційні одиниці є критично важливими компонентами в AD, що забезпечують структурований та ефективний підхід до управління користувачами, групами, комп'ютерами та іншими сутностями каталогу. Функціонуючи подібно до папок у файловій системі, OU дозволяють адміністраторам логічно групувати та керувати об'єктами AD на основі організаційних потреб. Це логічне групування є ключовим у спрощенні адміністративних завдань, таких як застосування GPOs та управління дозволами в різних відділах, командах або географічних локаціях організації. Зазвичай структури OU проектуються таким чином, щоб відображати внутрішню бізнес-ієрархію організації, що дозволяє застосовувати адаптований підхід до управління, який узгоджується з її операційною структурою. Кожен домен у лісі AD може встановлювати власну унікальну конфігурацію OU, створюючи гнучку та масштабовану систему, що адаптується до змінних потреб бізнесу. Ця гнучкість є особливо цінною у складних середовищах, де різні домени можуть вимагати відмінних політик та практик управління, як показано на рисунку 4.12.

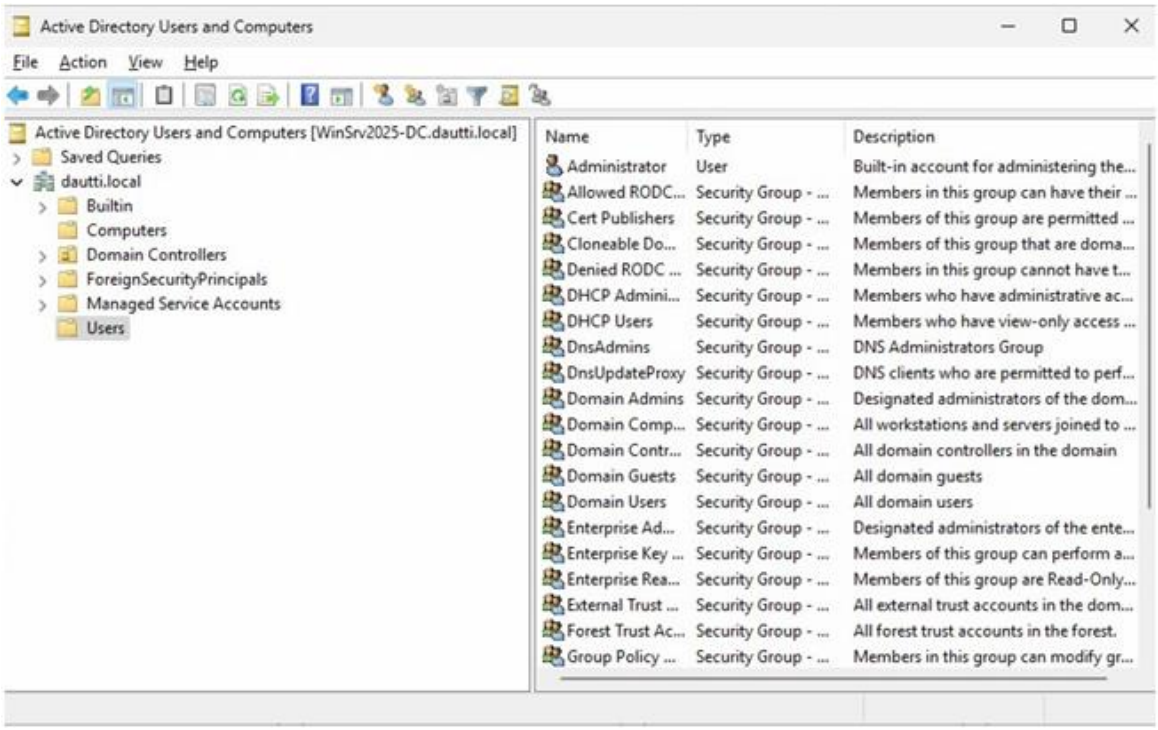

Рисунок 4.12 – Приклад ієрархії організаційних підрозділів у Windows Server 2025 [3]

Окрім OU, необхідно розуміти роль типових контейнерів в AD. Ці контейнери є попередньо визначеними місцями, куди автоматично поміщаються користувачі, комп'ютери та інші об'єкти під час їх створення. Глибоке розуміння попередньо визначених контейнерів є необхідним, коли сервер підвищується до контролера домену (DC). Це підвищення автоматично ініціює створення кількох типових контейнерів, які візуально представлені на рисунку 4.13.

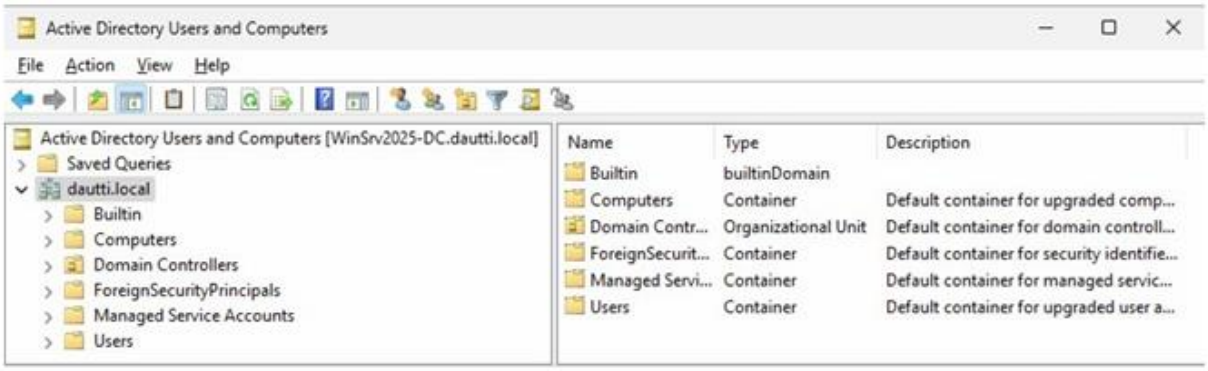

Рисунок 4.13 – Типові контейнери у Windows Server 2025 [3]

Ці контейнери відіграють критичну роль в AD і відрізняються своєю незмінною природою – їх не можна перейменувати, видалити або створити заново, і вони не підлягають зв'язуванню з жодним GPO. Ця незмінність, за задумом, гарантує, що фундаментальні елементи AD залишаються узгодженими та безпечними, тим самим зберігаючи структурну цілісність каталогу. Типові контейнери слугують специфічним цілям, таким як організація користувачів, комп'ютерів та інших об'єктів каталогу стандартизованим способом. Вони забезпечують стабільне середовище для основних операцій AD, гарантуючи, що певні критичні об'єкти завжди зберігаються в передбачуваному місці. Хоча вони не є такими гнучкими, як OU, які можуть бути налаштовані відповідно до потреб організації, типові контейнери залишаються життєво важливими для підтримки фундаментальної структури AD.

Розуміння концепції прихованих типових контейнерів є важливим для системних адміністраторів, навіть якщо ці контейнери не є безпосередньо актуальними для повсякденних завдань. Приховані контейнери виконують значну функцію у підтримці оптимізованого та організованого вигляду в консолі «Active Directory – користувачі й комп'ютери», запобігаючи непотрібному захаращенню, яке могло б ускладнити управління об'єктами AD. Залишаючи певні контейнери поза полем зору, AD забезпечує зручність та керованість інтерфейсу, особливо у великих та складних середовищах. Міркування безпеки також обумовлюють приховування цих контейнерів. Приховані контейнери захищають чутливі системні об'єкти, гарантуючи, що доступ до них мають лише користувачі з відповідними дозволами та знаннями. Цей рівень безпеки допомагає захистити цілісність каталогу та знижує ризик випадкових модифікацій або несанкціонованого доступу до критичних компонентів системи. Для відображення цих прихованих типових контейнерів адміністраторам потрібно увімкнути опцію «Розширені можливості» (Advanced Features) у меню «Вигляд» (View), як зображено на рисунку 4.14 [3].

Активація цієї функції відкриває приховані контейнери, дозволяючи отримати більш повний огляд та розширений контроль над ресурсами каталогу. Ця можливість є особливо цінною для виконання просунутих адміністративних завдань, таких як детальний аудит,

тонке налаштування параметрів безпеки або управління об’єктами, які зазвичай не відображаються у стандартному вигляді.

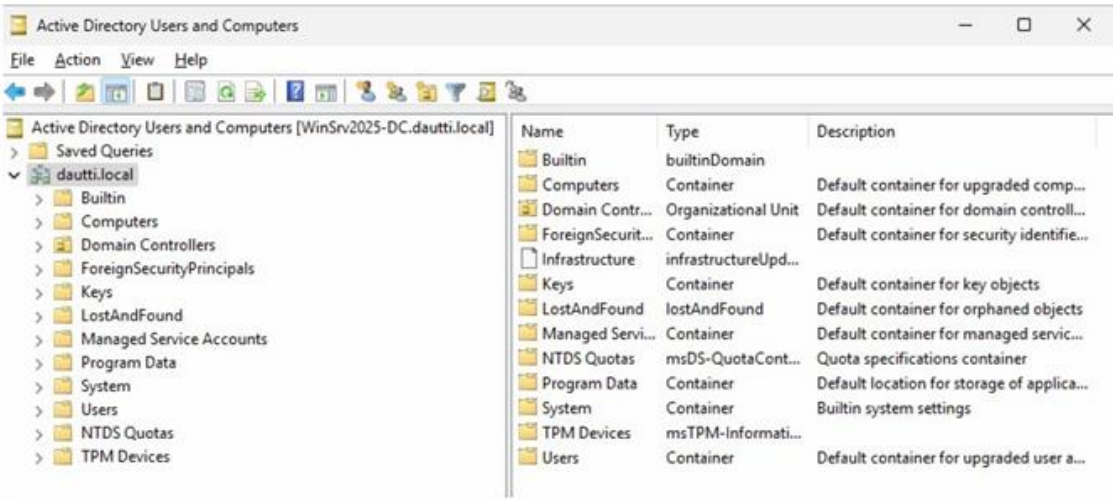

Рисунок 4.14 – Приховані типові контейнери у Windows Server 2025 [3]

Здобувши розуміння цих прихованих типових контейнерів, необхідно розглянути їх практичне застосування та ролі в середовищі AD. У цих контейнерах часто міститься важлива системна інформація, така як об’єкти інфраструктури, суб’єкти безпеки та дані реплікації, які є життєво важливими для безперебійної роботи AD. Розуміння того, як отримати доступ та керувати цими прихованими контейнерами, дозволяє адміністраторам бути повністю підготовленими до підтримки безпечної, ефективної та добре організованої інфраструктури каталогу.

Типові контейнери у Windows Server 2025 є невід’ємною частиною організації та управління об’єктами AD, кожен з яких слугує окремій меті. Контейнер Computers є типовим сховищем для новостворених облікових записів комп’ютерів, забезпечуючи централізоване місце для цих об’єктів. Контейнер Domain Controllers спеціально розроблений для розміщення всіх облікових записів DC, гарантуючи їх організованість та легкий доступ. Контейнер ForeignSecurityPrincipals зарезервований для ідентифікаторів безпеки (SIDs) із зовнішніх доменів, полегшуючи міждоменну безпеку та дозволи. Контейнер Keys зберігає об’єкти криптографічних ключів, які є важливими для безпечних комунікацій та шифрування в мережі. Контейнер LostAndFound відіграє критичну роль у підтримці цілісності каталогу, утримуючи осиротілі об’єкти, які від’єдналися від своїх оригінальних контейнерів, що запобігає потенційним проблемам з посиланнями на об’єкти. Контейнер Managed Service Accounts присвячений керованим обліковим записам служб, які використовуються для забезпечення підвищеної безпеки та управління службами, що працюють на серверах. Контейнер Users є типовим місцем для оновлених або новостворених облікових записів користувачів, що полегшує управління та доступ до об’єктів, пов’язаних з користувачами [4].

Після встановлення розуміння цих типових контейнерів, наступним кроком є розгляд концепції делегування контролю організаційній одиниці (OU). Делегування контролю передбачає призначення конкретних адміністративних дозволів користувачам або групам для певних OU, що дозволяє їм керувати об'єктами в межах цієї OU без надання повних адміністративних прав у всьому середовищі AD. Цей процес делегування є критично важливим для підтримки безпечного та організованого каталогу, оскільки він дозволяє адміністраторам призначати обов'язки користувачам без прав адміністратора, обмежуючи їхній доступ лише тими об'єктами та функціями, які необхідні для їхніх ролей. Такий підхід допомагає збалансувати адміністративний контроль із безпекою, гарантуючи, що користувачі мають належний рівень доступу для ефективного виконання своїх завдань без компрометації цілісності загальної інфраструктури AD.

Розуміння функції OU в AD є необхідним для ефективного управління каталогом. OU слугують засобом для систематичної організації та управління об'єктами AD. Для підвищення ефективності адміністрування контроль може бути делеговано конкретним користувачам або групам у межах OU. Цей процес дозволяє розподіляти адміністративні обов'язки без надання користувачам повних адміністративних прав у всьому середовищі AD. Для делегування контролю користувачі або групи спочатку повинні бути переміщені у визначену OU, як показано на рисунку 4.21.

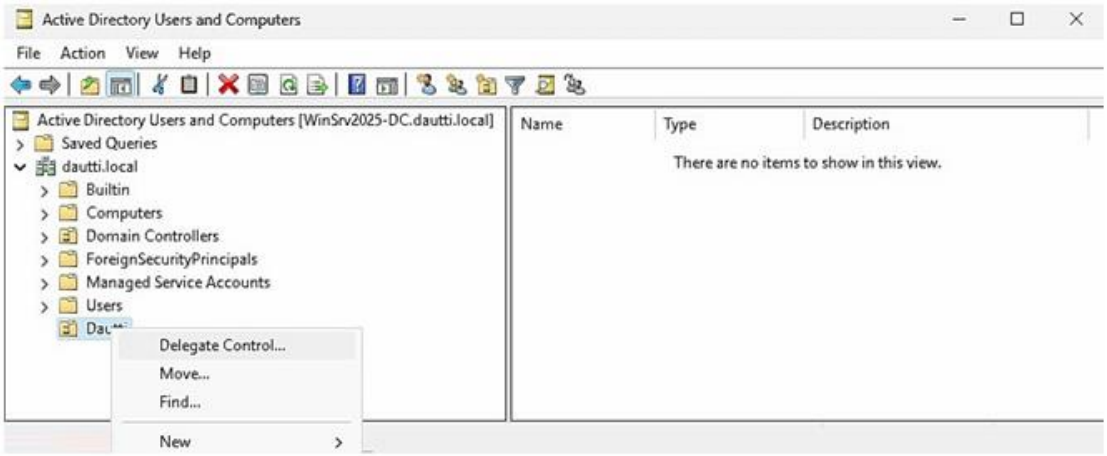

Рисунок 4.15 – Делегування керування організаційномій одиниці у Windows Server 2025 [3]

Делегування контролю включає призначення конкретних адміністративних дозволів, таких як управління обліковими записами користувачів, скидання паролів або зміна членства в групах у межах цієї OU. Це цілеспрямоване делегування допомагає забезпечити виконання адміністративних завдань відповідним персоналом, зберігаючи при цьому безпеку та організованість. Обмежуючи дозволи конкретними OU, адміністратори можуть ефективніше керувати ресурсами та знижувати ризик несанкціонованого доступу або ненавмисних змін. Делегування контролю також уможливлює впровадження адміністрування на основі ролей,

що може покращити операційну ефективність та підзвітність. Кожному делегованому адміністратору можуть бути призначені завдання, що відповідають його ролі, що полегшує відстеження змін та управління об'єктами каталогу відповідно до організаційних політик. У наступному розділі буде детальніше розглянуто управління обліковими записами користувачів, обліковими записами комп'ютерів та групами в AD, досліджено, як ці елементи взаємодіють з OU та сприяють створенню добре структурованого та безпечного середовища каталогу.

Перемещаємі профіля і домашні каталоги

Розуміння різних типів профілів користувачів у середовищах Windows Server визначається як фундаментальне для ефективного управління користувачами та налаштування системи. Профіль користувача являє собою сукупність налаштувань реєстру, файлової структури та даних, що визначають робоче середовище конкретного користувача. У наступному викладі надається пояснення трьох основних типів профілів користувачів в Active Directory: локальних профілів, які прив'язані до конкретної машини; переміщуваних профілів, які пропонують гнучкість при роботі на кількох пристроях; та обов'язкових профілів, які підтримують фіксовану конфігурацію без можливості модифікації користувачем.

Локальний профіль користувача створюється автоматично, коли користувач виконує вхід у комп'ютер вперше. Цей профіль зберігається на жорсткому диску конкретної машини (зазвичай у директорії C:\Users), як зображено на рисунку 4.16.

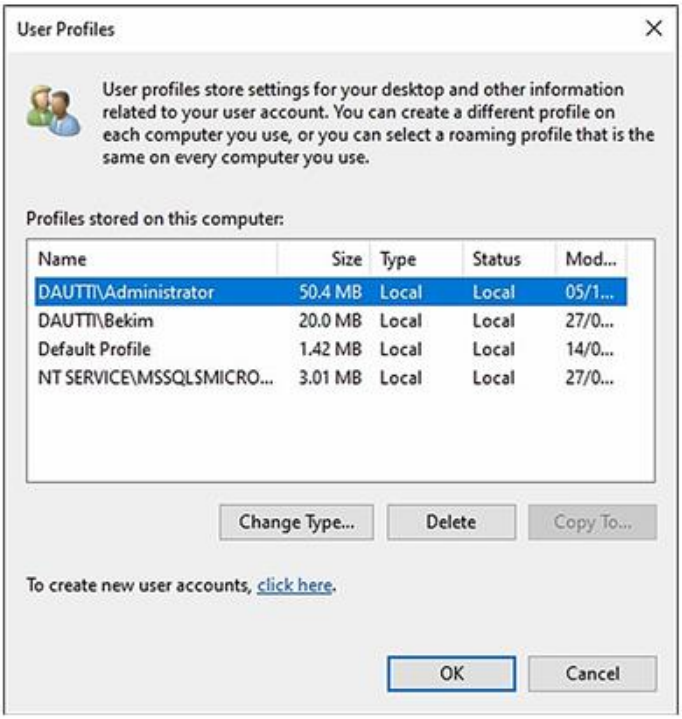

Рисунок 4.16 – Профілі користувачів у Windows Server 2025 [3]

Локальний профіль включає налаштування користувача (файл NTUSER.DAT), документи, а також дані програм, адаптовані до цього конкретного комп'ютера. Локальний профіль вважається ідеальним для індивідуального використання на одній машині, проте йому бракує гнучкості у випадках, коли користувачам необхідно отримувати доступ до свого робочого середовища з декількох пристроїв, оскільки налаштування не синхронізуються між різними робочими станціями [3].

Переміщуваний профіль користувача (Roaming User Profile) розширює гнучкість робочого середовища, дозволяючи користувачам отримувати доступ до своїх персоналізованих налаштувань та файлів з будь-якого комп'ютера в межах мережі. Цей профіль, по суті, є копією локального профілю, що зберігається на централізованому мережевому ресурсі (файловому сервері). Процес функціонування переміщуваного профілю реалізується наступним чином: під час входу користувача система завантажує профіль з сервера на локальний клієнтський комп'ютер; під час сеансу зміни вносяться локально; при виході з системи всі зміни синхронізуються назад на сервер. Це забезпечує послідовний досвід роботи на різних машинах. Такий тип профілю є особливо корисним у середовищах, де користувачі часто змінюють робочі місця, наприклад, у офісах з незакріпленими робочими місцями (hot-desking) [3].

Обов'язковий профіль користувача (Mandatory User Profile) забезпечує дотримання фіксованої конфігурації профілю. Ці профілі, які також зберігаються на мережевому ресурсі, базуються на попередньо налаштованому шаблоні. Ключова технічна відмінність полягає у зміні розширення файлу куща реєстру з .DAT на .MAN. Будь-які зміни, внесені користувачем під час сеансу (наприклад, зміна фонового малюнка або налаштувань робочого столу), не зберігаються після виходу з системи. Це гарантує, що кожного разу, коли користувач виконує вхід, він починає роботу з тією ж базовою конфігурацією. Такий підхід є корисним у середовищах, де вимагається уніфікованість і небажані налаштування користувача, наприклад, у навчальних класах, інтернет-кіосках або на публічних терміналах [3].

Підсумовуючи, локальні профілі прив'язані до окремих комп'ютерів, переміщувані профілі забезпечують мобільність завдяки доступності з будь-якої мережевої машини, а обов'язкові профілі підтримують узгодженість шляхом скасування змін користувача та використання фіксованого шаблону. Кожен тип профілю слугує окремим цілям, допомагаючи адміністраторам ефективно керувати середовищами користувачів відповідно до організаційних потреб.

Окремою, але тісно пов'язаною з профілями концепцією, є використання домашніх каталогів (Home Directories). У той час як переміщуваний профіль призначений для зберігання налаштувань середовища (App Data, налаштування робочого столу), домашній каталог використовується як централізоване місце для зберігання особистих файлів та

документів користувача. Налаштування домашнього каталогу виконується через властивості облікового запису користувача в Active Directory. При вході в систему домашній каталог автоматично підключається як мережевий диск (наприклад, диск H:) у сеансі користувача. Використання домашніх каталогів дозволяє відокремити дані користувача від його профілю, що пришвидшує процес входу в систему (оскільки не потрібно завантажувати великі обсяги документів разом із профілем) і спрощує централізоване резервне копіювання критично важливих даних на сервері. Це також забезпечує доступ до документів з будь-якого комп'ютера в мережі, навіть якщо переміщувані профілі не використовуються [4].

Поєднання переміщуваних профілів для налаштувань та домашніх каталогів для даних вважається найкращою практикою для забезпечення повноцінної мобільності користувачів у корпоративній мережі.

Безпека файлової системи і принципи побудови безпеки (користувачі, групи, права)

Безпека, побудована навколо Active Directory, була спроектована для захисту цінних мережевих активів. На розвиток безпеки Windows Server, починаючи з версії 2012, вплинула ініціатива Trustworthy Computing («Надійні обчислення») від Microsoft, яка змінила основний фокус продуктів компанії на безпеку. По суті, увага до безпеки продуктів є вищою, ніж будь-коли раніше, і всі нові функції повинні пройти так званий «лакмусовий тест» на безпеку перед випуском. Ця ініціатива вплинула на розробку серверних операційних систем і чітко простежується у функціях безпеки.

Важливим елементом системи безпеки є протокол автентифікації Kerberos. Спочатку він був розроблений у MIT як безпечний метод автентифікації користувачів без фактичного відправлення пароля користувача через мережу, незалежно від того, зашифрований він чи ні. Можливість передачі даних автентифікації таким чином значно знижує загрозу крадіжки пароля, оскільки зловмисники більше не можуть перехопити копію пароля під час його проходження через мережу та застосувати атаки грубої сили (brute-force) для його розшифровки. Фактична функціональність Kerberos є складною, але, по суті, відбувається наступне: комп'ютер надсилає клієнту інформаційний пакет, який вимагає автентифікації. Цей пакет містить свого роду «загадку», відповідь на яку може бути надана лише за допомогою правильних облікових даних користувача. Користувач застосовує «відповідь» до загадки та надсилає її назад на сервер. Якщо до відповіді було застосовано правильний пароль, користувач проходить автентифікацію. Хоча ця форма автентифікації використовується в Windows Server, вона не є власністю Microsoft і доступна як інтернет-стандарт.

Реалізації AD DS, по суті, є настільки безпечними, наскільки безпечним є середовище

Windows Server, у якому вони працюють. Безпека структури AD DS може бути підвищена за допомогою додаткових запобіжних заходів, таких як захищений зв'язок між серверами з використанням IPsec або використання смарт-карт та інших методів шифрування. Крім того, середовище користувача може бути захищене за допомогою групових політик, які дозволяють встановлювати зміни параметрів, такі як обмеження паролів користувачів, безпека домену та привілеї доступу при вході в систему.

У Windows Server 2025 представлено комплексний набір покращень безпеки для AD DS, розроблений для посилення протоколів автентифікації та захисту критичної інфраструктури від кіберзагроз, що стають дедалі складнішими. В основі цих покращень лежить вдосконалення автентифікації Kerberos, яка протягом багатьох років була наріжним каменем AD DS. У цьому випуску Kerberos отримує переваги від більш надійних алгоритмів шифрування, що посилює захист від поширених вразливостей, таких як атаки Pass-the-Ticket та Golden Ticket. Ці вразливості часто використовуються для атак з бічним переміщенням всередині мережі. Завдяки цим оновленням Windows Server 2025 забезпечує дотримання вищих криптографічних стандартів, знижуючи ймовірність крадіжки облікових даних та несанкціонованого доступу [3].

Ще одним ключовим досягненням визначається покращена інтеграція можливостей багатофакторної автентифікації (MFA), які стали необхідними для пом'якшення сучасних ризиків кібербезпеки. Windows Server 2025 забезпечує більш плавну та гнучку інтеграцію MFA з політиками умовного доступу, що дозволяє організаціям динамічно застосовувати MFA на основі різних факторів, таких як чутливість ресурсів, до яких здійснюється доступ, роль користувача або навіть місцезнаходження доступу. Такий контекстний підхід до безпеки гарантує, що привілейовані ресурси отримують найвищий рівень захисту, мінімізуючи при цьому незручності для звичайних користувачів, які виконують рутинні завдання. Включення біометрії та MFA на основі токенів додатково покращує структуру безпеки, узгоджуючись із моделями безпеки Zero Trust («Нульова довіра»), які надають пріоритет безперервній перевірці [3].

Управління груповою політикою також зазнало значних покращень у Windows Server 2025. Адміністратори тепер можуть впроваджувати та забезпечувати дотримання політик безпеки з підвищеною точністю, отримуючи вигоду від ширшого діапазону попередньо визначених шаблонів безпеки, адаптованих для різних організаційних потреб. Ці шаблони, приклад яких (файли ADMX) наведено на рисунку 4.17, допомагають спростити розгортання конфігурацій безпеки в середовищах AD DS.

У поєднанні з можливостями моніторингу в реальному часі та оповіщення, ці покращення дозволяють швидше виявляти та усувати потенційні загрози безпеці. Організації можуть точно налаштовувати параметри контролю доступу та відстежувати активність

користувачів, тим самим мінімізуючи вектори атак у мережі.

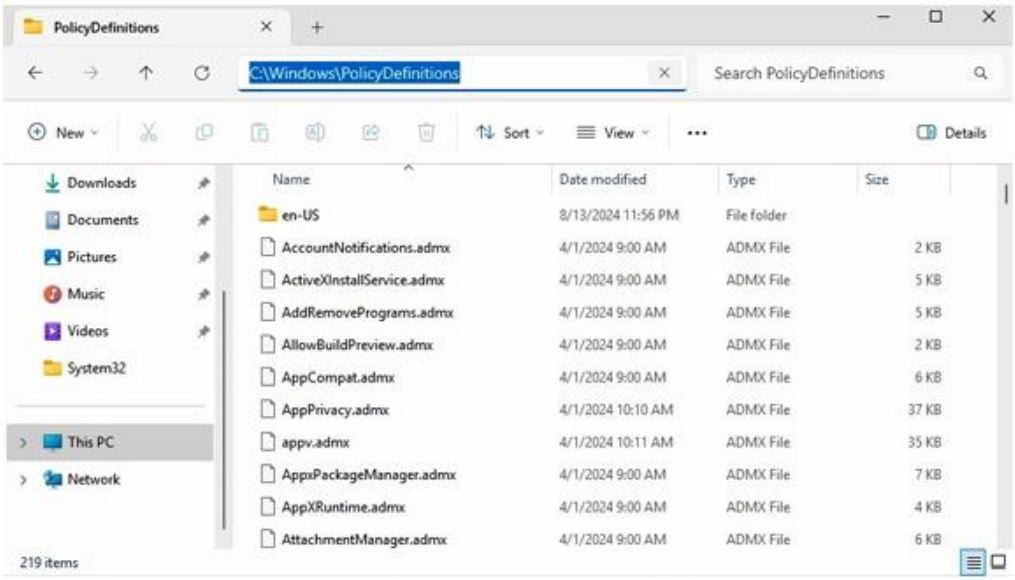

Рисунок 4.17 – Файли ADMX у Windows Server 2025 [3]

На додаток до цих функцій, Windows Server 2025 покращує механізми аудиту та логування в межах AD DS. Впровадження більш гранулярних можливостей аудиту дозволяє командам безпеки отримувати глибше розуміння патернів автентифікації та швидше виявляти аномалії. Завдяки покращеному логуванню подій організації можуть краще відстежувати спроби входу, патерни доступу та потенційні порушення, що є критично важливим для криміналістичних розслідувань та дотримання правил безпеки. Це гарантує, що команди безпеки обладнані для швидкого реагування на спроби несанкціонованого доступу та підтримки постійної пильності щодо мережі.

Окремо слід зазначити наявність великої кількості безкоштовних сценаріїв PowerShell у центрі скриптів Microsoft та галереї PowerShell. Ці платформи слугують відомими репозиторіями, де IT-фахівці можуть знайти та поділитися сценаріями для різних адміністративних завдань. Обидва ресурси містять великі колекції скриптів, що стосуються саме AD та DNS, що робить їх безцінними для автоматизації та спрощення складних заходів з управління мережею.

У сукупності ці досягнення в галузі безпеки позиціонують AD DS як життєво важливий інструмент для захисту сучасних IT-середовищ, особливо в організаціях із гібридними хмарними архітектурами. Зміцнюючи фундаментальні протоколи автентифікації, покращуючи інтеграцію MFA, вдосконалюючи управління політиками та забезпечуючи глибшу видимість подій безпеки, Windows Server 2025 пропонує комплексний захист від ландшафту загроз, що постійно розвивається. Ці покращення дозволяють організаціям прийняти проактивну позицію щодо безпеки, гарантуючи, що їхня IT-інфраструктура

залишається стійкою до нових викликів кібербезпеки. Маючи чітке розуміння впроваджених розширених функцій безпеки та механізмів автентифікації, важливо розглянути, як ці покращення інтегруються з ширшими IT-інфраструктурами.

Керування користувачами та групами в межах AD

Розуміння облікових записів користувачів і комп'ютерів, разом із групами, є фундаментальним для керування доступом до мережі в середовищі домену на базі Windows. Ці облікові записи є критично важливими елементами AD, що забезпечують автентифікацію як користувачів, так і пристроїв у всій мережі. У цій централізованій системі групи мають особливе значення, оскільки вони спрощують процес призначення та керування правами й дозволами. Групи агрегують численні облікові записи, дозволяючи адміністраторам застосовувати політики та дозволи колективно, а не індивідуально. Такий оптимізований підхід підвищує як безпеку, так і ефективність.

Розуміння облікових записів домену є необхідним для ефективного керування доступом до мережі в середовищі AD. Облікові записи домену проходять автентифікацію через AD, що дозволяє користувачам отримувати доступ як до локальних, так і до мережевих ресурсів відповідно до дозволів, призначених самому обліковому запису або успадкованих від членства в групах. Ця централізована структура автентифікації забезпечує оптимізований і безпечний підхід до керування доступом до різних служб і програм у мережі.

Для створення облікового запису домену у Windows Server 2025 виконується наступна послідовність дій: спочатку відкривається консоль «Active Directory – користувачі й комп'ютери» (Active Directory Users and Computers) шляхом переходу до інструментів Windows (Windows Tools). Далі виконується натискання правою кнопкою миші на контейнері Users, обирається пункт New, а потім – user. Після цього вводиться необхідна інформація про користувача, як показано на рисунку 4.18**,** і натискається кнопка Next [3].

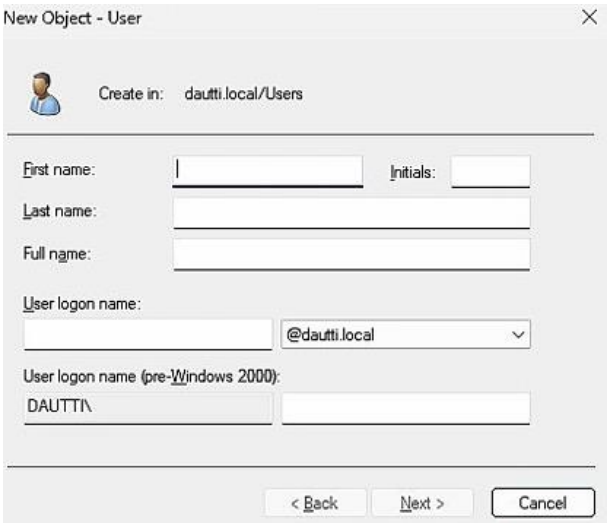

Рисунок 4.18 – Створення облікового запису домену в Windows Server 2025 [3]

На наступному етапі встановлюється тимчасовий пароль, підтверджується, і процес продовжується натисканням кнопки Next. Завершується створення облікового запису домену натисканням кнопки Finish. Цей процес встановлює обліковий запис домену та інтегрує його в структуру AD, надаючи користувачам доступ до мережевих ресурсів на основі призначених дозволів. У наступному підрозділі досліджується створення та керування локальними обліковими записами, які також є критичними для керування доступом користувачів та безпекою на окремих машинах і в межах специфічних локальних середовищ.

Розуміння локальних облікових записів є критично важливим для ефективного керування доступом на окремих комп'ютерах. На відміну від облікових записів домену, які проходять автентифікацію через AD і надають доступ у межах усієї мережі, локальні облікові записи є специфічними для комп'ютера, на якому вони створені, і керуються диспетчером безпеки облікових записів Windows (Security Accounts Manager – SAM). Ці облікові записи надають доступ до ресурсів на локальній машині та можуть взаємодіяти зі спільними ресурсами в одноранговій (P2P) мережі без необхідності отримання додаткових дозволів рівня домену. Локальні облікові записи є особливо корисними в сценаріях, коли комп'ютер працює незалежно від домену або коли підключення до домену недоступне. Вони створюються та керуються локально, що дозволяє здійснювати гранулярний контроль над дозволами та доступом користувачів на основі кожної окремої машини. Це може бути вигідним для керування невеликими робочими групами або автономними комп'ютерами, де централізоване керування доменом є недоцільним [4].

Для створення локального облікового запису у Windows Server 2025 виконуються наступні кроки: здійснюється доступ до консолі «Керування комп'ютером» (Computer Management) через інструменти Windows (Windows Tools). Ця консоль надає централізований інтерфейс для керування різними компонентами системи, включаючи облікові записи користувачів. Потім необхідно перейти до System Tools, розгорнути розділ Local Users and Groups, натиснути правою кнопкою миші на контейнері Users і вибрати New, а потім – user. Далі вводяться необхідні дані користувача, такі як ім'я користувача та пароль, як зображено на рисунку 4.19. Процес завершується натисканням кнопки Create [3].

Важливим зауваженням при створенні локального облікового запису у Windows Server 2025 є те, що сервер не повинен функціонувати як контролер домену (DC). Якщо сервер призначено контролером домену, він оброблятиме функції, пов'язані з доменом, і керуватиме AD DS, що ускладнює керування локальними обліковими записами. Забезпечуючи, що сервер не є DC, можна уникнути складнощів керування доменом, що дозволяє просте налаштування та керування локальними обліковими записами без додаткового навантаження служб домену. Локальні облікові записи зберігаються та автентифікуються SAM на локальній машині, що гарантує дотримання контролю доступу та дозволів незалежно від домену

мережі. Ці облікові записи ідеально підходять для сценаріїв, де потрібне локальне адміністрування та контроль доступу.

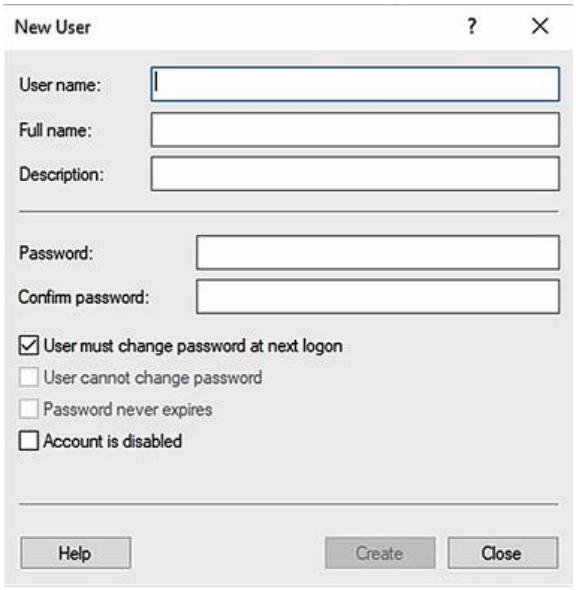

Рисунок 4.19 – Створення локального облікового запису в Windows Server 2025 [3]

У середовищі AD облікові записи комп'ютерів є критичними для ідентифікації та керування комп'ютерами в домені. Перед приєднанням до домену кожен комп'ютер повинен мати унікальне ім'я хоста для запобігання конфліктам. Цей унікальний ідентифікатор гарантує, що комп'ютер може бути точно відстежений і керований у мережі. Після успішного додавання комп'ютера до домену він зберігає своє ім'я хоста для постійної взаємодії з іншими ресурсами домену, включаючи файли, програми та служби. Це налаштування дозволяє безперебійну комунікацію та інтеграцію з доменом. Консоль «Active Directory – користувачі й комп'ютери» ефективно обробляє адміністрування облікових записів комп'ютерів, як показано на рисунку 4.20.

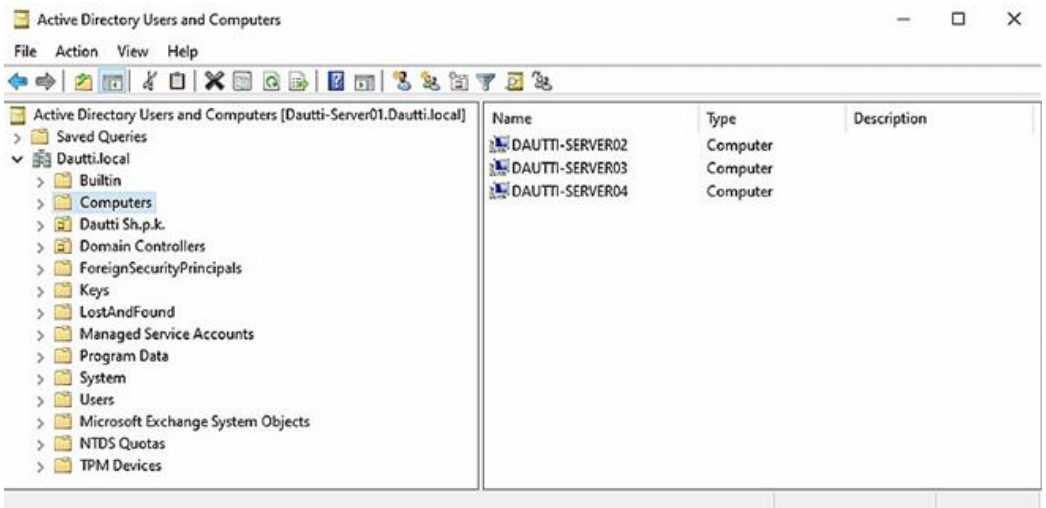

Рисунок 4.20 – Облікові записи комп'ютерів у Windows Server 2025 [3]

Ця консоль дозволяє адміністраторам переглядати та керувати обліковими записами комп’ютерів, налаштовувати властивості та застосовувати політики. Тут виконуються такі завдання, як скидання паролів, увімкнення або вимкнення облікових записів та зміна налаштувань облікового запису.

Розуміння облікових записів комп’ютерів є необхідним для підтримання цілісності мережі та забезпечення належного доступу до ресурсів. Ці облікові записи відіграють життєво важливу роль в автентифікації та авторизації комп’ютерів у домені, підтримуючи таким чином ефективне керування мережею та безпеку. Далі увага зміщується на групи в межах структури AD. Групи є невід’ємною частиною керування дозволами та правами доступу, спрощуючи призначення ролей і привілеїв та оптимізуючи адміністративні завдання. Вони допомагають організовувати користувачів і комп’ютери, застосовувати послідовні політики та підвищувати загальну безпеку мережі.

Розуміння типів груп в AD є фундаментальним для оптимізації керування мережею та забезпечення безпеки. Групи AD спрощують адміністрування дозволів і прав, дозволяючи адміністраторам керувати декількома об’єктами AD колективно, а не налаштовувати кожен об'єкт індивідуально. Такий підхід не тільки підвищує ефективність, але й допомагає підтримувати послідовні політики безпеки в мережі. Групи самі по собі також є об’єктами AD і можуть бути переміщені або реорганізовані в межах різних OU для узгодження з організаційними змінами або адміністративними потребами. Як представлено на рисунку 4.21, групи адмініструються за допомогою консолі «Active Directory – користувачі й комп’ютери». В AD групи класифікуються на дві основні категорії [3].

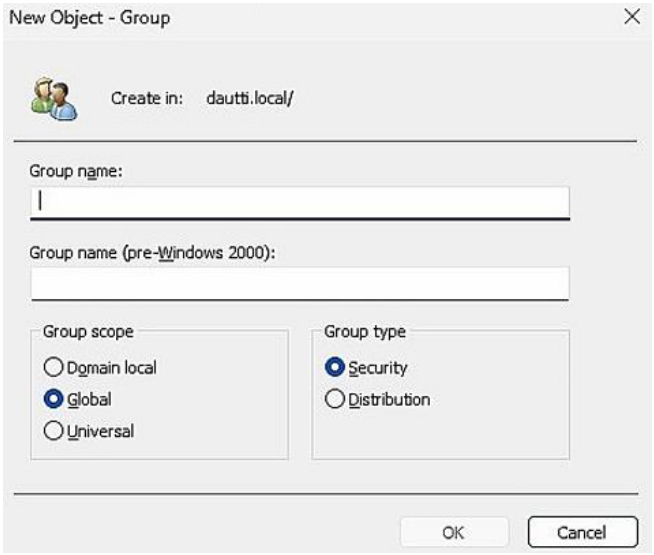

Рисунок 4.21 – Типи груп у Windows Server 2025 [3]

Групи безпеки (Security groups) – це групи, які є важливими для керування доступом до спільних мережевих ресурсів, таких як файли, папки та принтери. Вони застосовують

дозволи та забезпечують дотримання політик безпеки в мережі. Групи безпеки можуть бути вкладені в інші групи безпеки для створення ієрархічної структури дозволів, що дозволяє здійснювати більш гранулярний контроль над доступом до ресурсів [3].

Групи розповсюдження (Distribution groups) – це групи, що спроектовані для полегшення розсилки електронних повідомлень в організації. Вони спрощують процес надсилання повідомлень великим групам користувачів, діючи як списки розсилки. Хоча групам розповсюдження не призначаються дозволи і вони не можуть використовуватися для контролю доступу до ресурсів, вони відіграють вирішальну роль у спрощенні внутрішньої комунікації [3].

Розуміння цих типів груп та їхніх функцій дозволяє адміністраторам ефективно керувати мережевими ресурсами та комунікацією. У наступних розділах будуть розглянуті типові групи – попередньо визначені групи, що постачаються з AD, – та процес створення нових груп. Це знання є необхідним для організації ролей користувачів, керування доступом до ресурсів та ефективного делегування адміністративних завдань у середовищі AD.

Розуміння типових груп (default groups) в AD є фундаментальним для ефективного адміністрування мережі. Коли сервер підвищується до ролі контролера домену (DC), він автоматично генерує різноманітні типові групи, як показано на рисунку 4.22, який ілюструє типові групи у Windows Server 2025. Ці типові групи спроектовані для спрощення адміністративних завдань шляхом групування пов’язаних об’єктів AD, тим самим полегшуючи процес призначення дозволів та прав доступу.

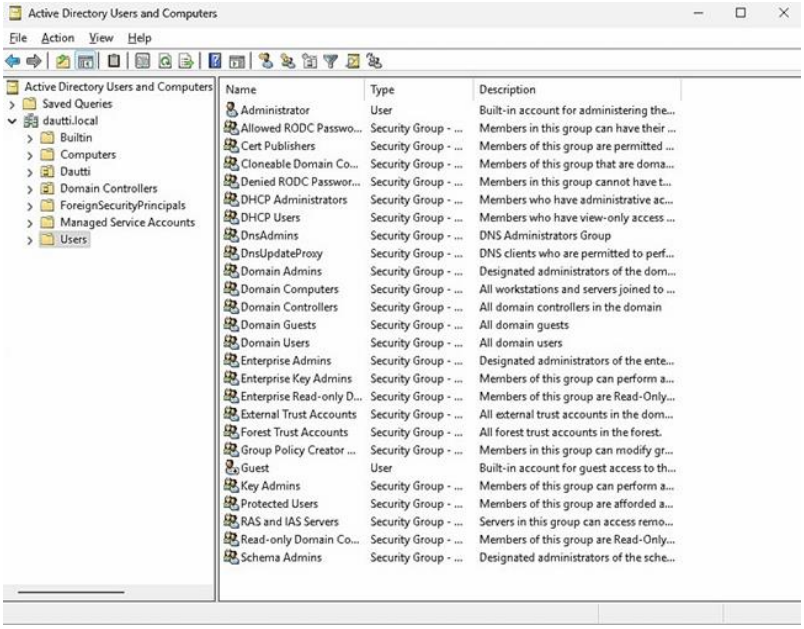

Рисунок 4.22 – Групи за замовчуванням у Windows Server 2025 [3]

Типові групи попередньо налаштовані зі специфічними ролями та дозволами, що може значно оптимізувати керування мережею. Наприклад, такі типові групи, як Domain

Admins, Enterprise Admins та Schema Admins, мають попередньо визначені рівні адміністративних привілеїв, які є критичними для керування різними аспектами середовища AD. Використовуючи ці групи, адміністратори можуть ефективно керувати доступом користувачів та забезпечувати дотримання політик безпеки без необхідності налаштовувати дозволи для кожного користувача або об'єкта вручну. Крім того, типові групи допомагають забезпечити послідовне застосування політик і дозволів у мережі, що підвищує як безпеку, так і операційну ефективність. Вони також полегшують делегування адміністративних завдань, надаючи попередньо визначені ролі, які можуть бути призначені користувачам залежно від їхніх обов'язків.

Розуміння областей дії груп є основоположним аспектом ефективного керування середовищами AD, оскільки вони безпосередньо впливають на те, як дозволи та політики застосовуються в мережі організації. Області дії груп визначають охоплення та застосовність членства в групах у структурі AD, що є критичним для підтримки безпеки та ефективності керування ресурсами. В AD існує три основні області дії груп, кожна з яких слугує відмінним цілям та контекстам, як показано на рисунку 4.23.

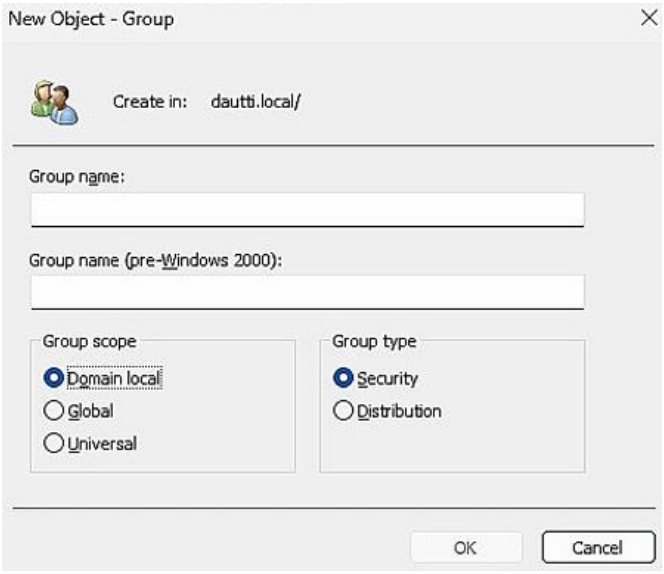

Рисунок 4.23 – Області дії груп у Windows Server 2025 [3]

Локальна група домену (Domain local group scope) – це область дії, яка спроектована для керування доступом до ресурсів у межах локального домену. Вона дозволяє включати облікові записи, локальні групи домену, глобальні групи та універсальні групи, що дозволяє адміністраторам ефективно призначати дозволи для локальних ресурсів. Локальні групи домену є особливо корисними при керуванні доступом до ресурсів, таких як файлові ресурси, принтери та інші специфічні для домену ресурси, де потрібно обмежити доступ користувачам і групам у межах цього домену [3].

Глобальна група (Global group scope) – це область дії, яка використовується для

організації користувачів і груп у межах одного домену, які мають спільні вимоги до доступу. Ця область дії включає облікові записи та глобальні групи, специфічні для глобальної групи батьківського домену. Глобальні групи зазвичай використовуються для призначення дозволів на ресурси в різних доменах у межах одного лісу, що робить їх ідеальними для сценаріїв, де користувачі з кількох доменів потребують доступу до спільних ресурсів [3].

Універсальна область дії групи (Universal group scope) є найбільш широкою, дозволяючи включення облікових записів, глобальних груп та універсальних груп з будь-якого домену в лісі. Ця область дії є необхідною для керування дозволами в декількох доменах, що робить її високоефективною у великих багатодоменних середовищах. Універсальні групи є особливо корисними, коли потрібно призначити дозволи послідовно по всьому лісу, гарантуючи, що користувачі в різних доменах мають належний доступ до ресурсів незалежно від їхнього членства в домені.

Кожна з цих областей дії груп відіграє критичну роль у забезпеченні належного та послідовного застосування дозволів і політик у середовищі AD. Розуміючи та правильно використовуючи ці області дії, адміністратори можуть підвищити як ефективність, так і безпеку своїх практик керування мережею. Крім того, належне використання областей дії груп може запобігти поширеним проблемам, таким як надмірні дозволи, коли користувачі мають більше доступу, ніж необхідно, або недостатні дозволи, коли законний доступ заборонено. Цей баланс є критичним для підтримки безпечного та добре функціонуючого середовища AD.

Концепція вкладеності груп базується на принципах областей дії груп, дозволяючи адміністраторам створювати більш складні та гнучкі структури груп. Вкладеність груп додатково вдосконалює здатність керувати дозволами та правами доступу, пропонуючи потужний інструмент для масштабних середовищ AD. Розуміння вкладеності груп в AD є фундаментальним аспектом ефективного та безпечного керування дозволами в складних IT-середовищах. Вкладеність груп дозволяє ієрархічно організовувати групи, що дає змогу адміністраторам ефективніше призначати дозволи, використовуючи структурований, багаторівневий підхід. Цей метод не тільки спрощує адміністрування контролю доступу, але й зменшує надлишковість та потенційні помилки, які можуть виникнути при індивідуальному призначенні дозволів численним обліковим записам користувачів.

На практиці вкладеність груп керується найкращими практиками, такими як методології Microsoft AGDLP (Accounts, Global, Domain Local, Permissions) та AGUDLP (Accounts, Global, Universal, Domain Local, Permissions). Ці моделі пропонують систематичний підхід до керування членством у групах та дозволами в мережі [3].

У моделі AGDLP облікові записи користувачів спочатку призначаються глобальній групі, яка зазвичай представляє певну роль або відділ в організації. Ця глобальна група потім

вкладається в локальну групу домену, яка відповідає за керування доступом до конкретних ресурсів у межах локального домену. Дозволи призначаються локальній групі домену, тим самим надаючи доступ усім членам глобальної групи за один крок. Цей метод є особливо ефективним у середовищах, де користувачі потребують послідовного доступу до ресурсів у межах одного домену [3].

Методологія AGUDLP розширює модель AGDLP, включаючи універсальну групу в структуру вкладеності. Тут глобальна група спочатку додається до універсальної групи, яка може охоплювати кілька доменів у межах лісу. Потім універсальна група включається в локальну групу домену, яка контролює доступ до ресурсів. Цей підхід ідеально підходить для великих багатодоменних середовищ, де користувачі потребують доступу до ресурсів у різних доменах. Використовуючи універсальні групи, адміністратори можуть підтримувати послідовну структуру дозволів по всьому лісу, гарантуючи, що користувачі мають необхідний доступ незалежно від домену, в якому вони працюють [3].

Ці структуровані методології не лише оптимізують керування дозволами, але й підвищують безпеку та масштабованість середовища AD. Зменшуючи кількість індивідуальних призначень дозволів і централізуючи контроль у чітко визначених структурах груп, адміністратори можуть легше забезпечувати дотримання політик безпеки, проводити аудит контролю доступу та реагувати на організаційні зміни. Після отримання ґрунтовного розуміння фундаментальних елементів AD, таких як DNS, OU та контейнери, а також класифікації облікових записів комп’ютерів і груп, наступним кроком є перехід до встановлення ролей AD DS і DNS. Цей етап є критичним, оскільки він закладає основу для налаштування та керування середовищем AD, гарантуючи, що воно відповідає потребам організації щодо безпеки, масштабованості та адміністрування.

Створення доменів і лісів

Процес розгортання інфраструктури Active Directory Domain Services (AD DS) розпочинається зі створення логічної основи, ключовими елементами якої виступають домени та ліси. Створення нового лісу визначається як фундаментальний етап проектування мережевого середовища, оскільки саме ліс встановлює межі безпеки, реплікації та адміністрування для всіх об’єктів директорії.

Практична реалізація розгортання інфраструктури розпочинається з підготовки віртуалізованого середовища. Перед початком виконання завдань ініціюється запуск віртуальної машини під керуванням операційної системи Windows Server 2025, що функціонує в середовищі гіпервізора Hyper-V. Дана віртуальна машина має бути попередньо налаштована в межах підготовчих етапів розгортання лабораторного стенду.

Після успішного завантаження операційної системи процес конфігурації виконується

через централізовану консоль керування «Диспетчер серверів» (Server Manager). Для створення та налаштування домену першочерговим завданням є інсталяція відповідної ролі сервера. У меню «Управління» (Manage) обирається пункт «Додати ролі та компоненти» (Add Roles and Features), що ініціює запуск майстра встановлення. Серед переліку доступних ролей обирається пункт «Доменні служби Active Directory» (Active Directory Domain Services). Цей алгоритм є стандартизованим для серверних операційних систем сімейства Windows [4].

Після вибору необхідної ролі здійснюється перехід до наступних етапів майстра, що завершується вікном підтвердження налаштувань. На цьому етапі підтверджується інсталяція обраних компонентів, після чого розпочинається процес копіювання бінарних файлів та налаштування залежностей.

Завершення процесу встановлення ролі не означає автоматичного створення домену. Сервер потребує процедури підвищення статусу (promotion). Після закінчення інсталяції в області сповіщень «Диспетчера серверів» з'являється інтерактивне повідомлення «Підвищити роль цього сервера до рівня контролера домена» (Promote this server to a domain controller). Активація цього посилання ініціює запуск спеціалізованого інструменту конфігурації.

Після натиснення відкривається «Майстер налаштування доменних служб Active Directory» (Active Directory Domain Services Configuration Wizard). Цей етап є критичним, оскільки саме тут визначається топологія майбутньої мережі.

У вікні вибору операції розгортання адміністратору пропонується обрати один із трьох сценаріїв, кожен з яких відповідає певним архітектурним потребам.

«Додати контролер домена в існуючий домен» (Add a domain controller to an existing domain) – ця опція використовується для масштабування інфраструктури, коли домен вже функціонує, і виникає потреба у додатковому контролері для розподілу навантаження або забезпечення відмовостійкості.

«Додати новий домен в існуючий ліс» (Add a new domain to an existing forest) – обирається у випадку, коли організація вже має розгорнутий ліс і потребує створення дочірнього домену або нового дерева доменів у межах спільної інфраструктури.

«Додати новий ліс» (Add a new forest) – використовується при первинному розгортанні, коли створюється абсолютно нова інфраструктура, де відсутні як ліс, так і домени.

Оскільки в межах даного завдання створення домену виконується вперше, обирається опція «Додати новий ліс». У відповідному полі вводиться повне доменне ім'я (FQDN) кореневого домену, після чого здійснюється перехід до наступного етапу натисканням кнопки «Далі».

На етапі налаштування параметрів контролера домену визначаються функціональні рівні лісу та домену. Зазвичай ці параметри залишаються без змін, що відповідають версії поточної операційної системи. Критично важливим кроком є встановлення складного пароля для режиму відновлення служб каталогів (Directory Services Restore Mode – DSRM). Цей пароль використовується для аварійного відновлення бази даних Active Directory у випадку серйозних збоїв.

Подальші кроки налаштування, такі як «Параметри DNS» (DNS Options) та «Додаткові параметри» (Additional Options), у базовому сценарії розгортання не потребують модифікації, тому підтверджуються натисканням кнопки «Далі». Аналогічний підхід застосовується на вкладці «Шляхи» (Paths), де визначаються місця розташування бази даних NTDS, файлів журналів та папки SYSVOL. Рекомендується залишити значення шляхів за замовчуванням [4].

На етапі «Переглянути параметри» (Review Options) здійснюється фінальна верифікація введених даних. Після перевірки система автоматично проводить аналіз відповідності сервера попереднім вимогам. У разі успішного проходження перевірки ініціюється процес інсталяції. Завершення процедури просування сервера до ролі контролера домену супроводжується автоматичним перезавантаженням операційної системи.

Після перезавантаження сервера верифікація успішності розгортання виконується через «Диспетчер серверів». У меню «Інструменти» (Tools) обирається консоль «Користувачі і комп'ютери Active Directory» (Active Directory Users and Computers). Відкриття вікна консолі та наявність у ньому створеного домену (наприклад, server.lab) з відповідною ієрархією контейнерів свідчить про те, що домен успішно створено, а сервер набув статусу контролера домену. На цьому етап створення та базового налаштування домену вважається завершеним [3].

Структура об'єктів

Логічна структура доменних служб Active Directory (AD DS) спроектована таким чином, щоб забезпечити масштабування від невеликих офісів до великих транснаціональних організацій. У систему вбудовано адміністративну гранулярність, що дозволяє делегувати контроль групам або окремим користувачам, завдяки чому призначення адміністративних прав більше не розглядається як бінарний сценарій «все або нічого». AD DS вільно наслідує модель каталогу X.500, але набуває низки власних характеристик. Багато фахівців вже адаптувалися до понять лісів та дерев в AD DS, а деякі обмеження, що існували в попередніх версіях служби каталогів, було знято. Для глибокого розуміння AD DS необхідно детально розглянути її основні структурні компоненти.

Домен AD DS, який традиційно зображується у вигляді трикутника, як показано на

рисунку 4.24, визначається як початкова логічна межа служби каталогів. В автономному розумінні домен AD DS діє подібно до застарілої структури домену Windows NT 4.0, яку він замінив. Усі користувачі та комп'ютери зберігаються та керуються в межах домену. Проте було внесено кілька значних змін у структуру домену та його взаємодію з іншими доменами в межах структури AD DS. Домени слугують адміністративними межами безпеки для об'єктів і містять власні політики безпеки. Важливо пам'ятати, що домени є логічною організацією об'єктів і можуть охоплювати кілька фізичних розташувань. Отже, налаштування кількох доменів для різних віддалених офісів або сайтів більше не є необхідним, оскільки питання реплікації та безпеки більш належним чином вирішуються за допомогою сайтів AD DS або контролерів домену лише для читання (RODC) [4].

Рисунок 4.24 – Розгляд зразка домену в AD DS [4]

Дерево AD DS складається з кількох доменів, з'єднаних двосторонніми транзитивними довірчими відносинами. Кожен домен у дереві AD DS спільно використовує загальну схему та глобальний каталог. На рисунку 4.25 зображено структуру, де кореневим доменом дерева AD DS є companyabc.com, а піддоменами виступають asia.companyabc.com та europe.companyabc.com. Транзитивні довірчі відносини встановлюються автоматично. Це означає, що оскільки домен Asia довіряє кореневому домену companyabc, а домен Europe також довіряє домену companyabc, то домен Asia автоматично довіряє і домену Europe. Довіра поширюється наскрізь через структуру доменів.

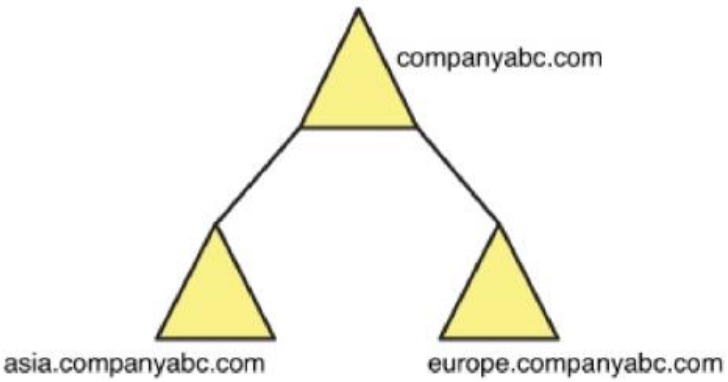

Рисунок 4.25 – Дерево AD DS Windows Server 2012 з піддоменами [4]

Слід зазначити, що хоча довірчі відносини в середовищі AD DS є транзитивними, це

не означає, що дозволи є повністю доступними для всіх користувачів або навіть адміністраторів між доменами. Довіра забезпечує лише шлях маршрутизації від одного домену до іншого. За замовчуванням права доступу не надаються від одного транзитивного домену до іншого. Адміністратор домену повинен явно надати права користувачам або адміністраторам іншого домену для доступу до ресурсів у своєму домені. Усі домени в межах дерева використовують спільний простір імен (у цьому прикладі – companyabc.com), але мають діючі механізми безпеки для відокремлення доступу від інших доменів. Наприклад, адміністратор у домені Europe може мати відносний контроль над усім своїм доменом без надання привілеїв до ресурсів користувачам із доменів Asia або companyabc. І навпаки, адміністратори в Europe можуть дозволити групам користувачів з інших доменів доступ за потреби, що робить адміністрування гранулярним та налаштовуваним [4].

Також варто враховувати, що технічна можливість створення піддоменів у лісі, таких як показані на рисунку 4.25, не завжди означає доцільність такого рішення. Для багатьох середовищ оптимальним є єдиний домен для всіх світових ресурсів, оскільки після прийняття рішення про створення піддоменів змінити його та перемістити ресурси пізніше буде складно.

Ліси визначаються як група взаємопов’язаних дерев доменів, де корені кожного дерева з’єднані неявними довірчими відносинами в спільний ліс. Основними характеристиками, що об’єднують усі домени та дерева доменів у спільний ліс, є наявність спільної схеми та спільного глобального каталогу. Однак домени та дерева доменів у лісі не зобов’язані використовувати спільний простір імен. Наприклад, домени microsoft.internal та technet.internal теоретично можуть бути частиною одного лісу, але підтримувати власні окремі простори імен. Ліси є головною організаційною межею безпеки для AD DS, і передбачається, що всім адміністраторам доменів у межах лісу довіряють певною мірою. Якщо довіра до адміністратора домену відсутня, такий домен слід розмістити в окремому лісі.

Операційна система Windows NT 4.0 використовувала систему автентифікації, відому як NT LAN Manager (NTLM). Ця форма автентифікації передавала зашифрований пароль через мережу у вигляді хешу. Проблема цього методу полягала в тому, що будь-хто міг моніторити мережу для перехоплення хешів, збирати їх, а потім використовувати сторонні інструменти дешифрування, які ефективно розшифровували пароль за допомогою словникових методів та методів повного перебору. Усі версії Windows Server після Windows 2000 використовують форму автентифікації, відому як Kerberos. По суті, Kerberos не передає інформацію про пароль через мережу і за своєю природою є більш безпечним, ніж NTLM [4].

Аналогічно до того, як Windows 2000 та Windows 2003 мали власні функціональні рівні для забезпечення сумісності із застарілими версіями доменів, Windows Server 2025

використовує власні функціональні рівні для підтримки сумісності. За замовчуванням нова інсталяція Active Directory на контролерах домену Windows Server 2025 автоматично встановлює функціональні рівні домену та лісу Windows Server 2025. Однак, якщо контролери домену Windows Server 2025 встановлюються в існуючий застарілий домен, дозволяється обрати, з якого функціонального рівня розпочати роботу лісу.

Процедура підвищення функціонального рівня існуючого лісу до рівня Windows Server 2025 виконується послідовно. Насамперед забезпечується, щоб усі контролери домену в лісі були оновлені до Windows Server 2025 або замінені на нові. Далі на контролері домену відкривається консоль «Домени і довіра Active Directory» (Active Directory Domains and Trusts) через меню інструментів у диспетчері серверів. У лівій області перегляду необхідно натиснути правою кнопкою миші на імені домену та обрати опцію «Підвищити функціональний рівень домену» (Raise Domain Functional Level). У діалоговому вікні обирається рівень Windows Server 2025, після чого дія підтверджується натисканням кнопки «Підвищити» та фінальним підтвердженням. Описана послідовність дій повторюється для всіх доменів у лісі [3].

Заключним етапом є виконання аналогічних дій для кореня лісу, за винятком того, що в контекстному меню обирається пункт «Підвищити функціональний рівень лісу» (Raise Forest Functional Level) і виконуються відповідні вказівки майстра. Коли рівень усіх доменів та лісу підвищено до функціональності Windows Server 2025, ліс отримує можливість використовувати новітні функціональні можливості AD DS. Виконуючи це, важливо пам’ятати, що до моменту виконання цього завдання в середовищі змішаного режиму Windows Server 2025 по суті працює в режимі зниженої сумісності.

Тема 5
Групові політики

Розуміння основ групових політик (GP) у Windows Server

У практиці системного адміністрування часто виникає необхідність примусового застосування специфічних конфігурацій у мережі організації з метою забезпечення узгодженості та безпеки. До таких завдань, наприклад, належать встановлення веб-сайту компанії як домашньої сторінки за замовчуванням у всіх браузерах на комп'ютерах організації, а також обмеження доступу до знімних носіїв інформації. Додатково може виникнути потреба у відключенні використання облікових записів Microsoft у системах Windows 10 та 11. Ці всі завдання ефективно вирішуються за допомогою групових політик (GP) у середовищі Windows Server, що забезпечує централізований спосіб застосування та примусового виконання політик без необхідності покладатися на інструменти або утиліти сторонніх розробників.

Групова політика – це критично важлива функція Windows Server, що дозволяє адміністраторам примусово застосовувати політики як на рівні користувача, так і на рівні комп'ютера [3].

За допомогою об'єктів групової політики (GPO) адміністратори мають можливість визначати та впроваджувати налаштування, що контролюють поведінку користувачів та комп'ютерів у мережі. GPO надають адміністративні шаблони, які специфікують дозволені дії та конфігурації для користувачів і пристроїв, гарантуючи уніфіковане застосування організаційних стандартів та заходів безпеки. Окрім того, GPO можуть використовуватися як механізм безпеки для застосування критично важливих налаштувань захисту до користувачів та комп'ютерів у мережі під керуванням домену, що підвищує загальний рівень захищеності організації [24].

Важливо провести розмежування між перевагами групової політики (Group Policy Preferences, GPP) та налаштуваннями групової політики (Group Policy Settings, GPS). У той час як GPS примусово задають специфічні конфігурації та параметри для користувачів і комп'ютерів, GPP забезпечують більшу гнучкість, дозволяючи користувачам модифікувати свої налаштування без адміністративного втручання. Розуміння цієї відмінності сприяє ефективному використанню обох інструментів для керування середовищем.

За замовчуванням об'єкти групової політики зберігаються в директорії C:\Windows\SYSVOL\sysvol\<domain name>\Policies на контролері домену, як це продемонстровано на рисунку 5.1. Таке розташування за замовчуванням гарантує систематичне керування всіма налаштованими політиками та їх реплікацію між контролерами домену [3].

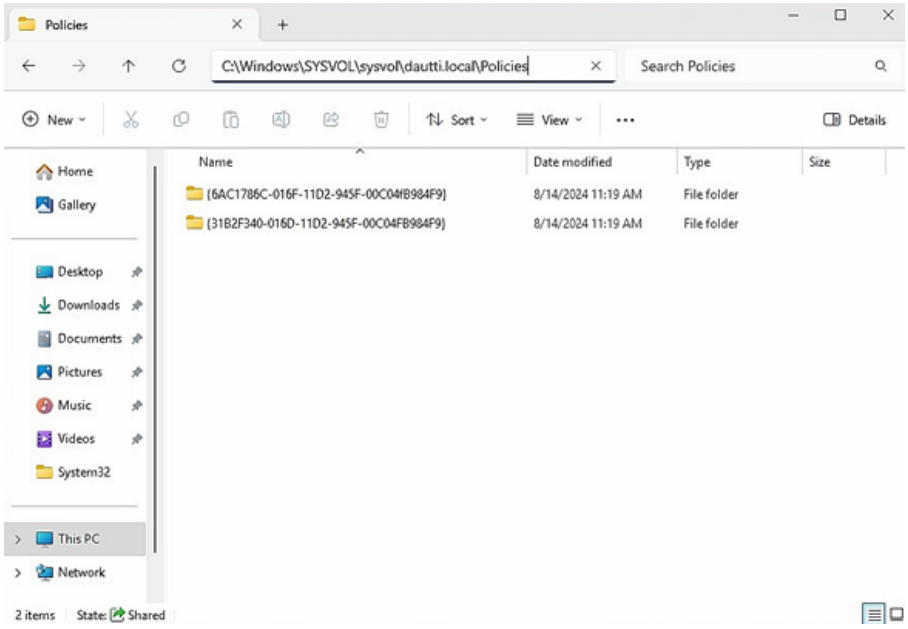

Рисунок 5.1 – Розташування GPO за замовчуванням у Windows Server 2025 [3]

Після формування ґрунтовного розуміння групових політик (GP) та об’єктів групових політик (GPO), важливо вивчити методи ефективного керування та конфігурації цих політик для узгодження з організаційними потребами та вимогами безпеки.

Варто зазначити, що ефективне усунення несправностей групових політик є критичним для підтримання належного функціонування середовища Windows Server. Використання таких інструментів, як «Результуюча політика» (Resultant Set of Policy, RSoP), gpresult та засіб перегляду журналів групової політики (Group Policy Log Viewer), здатне суттєво покращити можливості діагностики та вирішення проблем. Ці інструменти надають цінну інформацію про застосування політик, дозволяючи адміністраторам ідентифікувати конфлікти, оцінювати пріоритетність політик та гарантувати, що конфігурації застосовуються належним чином. У наступних розділах ці інструменти будуть детально розглянуті, що забезпечить оволодіння практичними стратегіями ефективного усунення несправностей в організації [23].

Групові політики та керування політиками Windows Server

Ефективне керування об’єктами групової політики (GPO) є критично важливим для системних адміністраторів з метою забезпечення примусового виконання та стандартизації конфігурацій у мережі. Основним інструментом для реалізації цього завдання виступає Консоль керування груповою політикою (Group Policy Management Console, GPMC), що пропонує централізований інтерфейс для створення, налаштування та застосування GPO у мережі на базі домену.

Інтерфейс GPMC розділено на дві основні панелі: панель лісу (Forest pane) та панель об’єктів GPO (GPOs pane). Панель лісу відображає ієрархічну структуру домену, надаючи

адміністраторам можливість ефективної навігації між доменами та організаційними одиницями (OU). Панель GPO містить детальні вкладки, зокрема «Статус» (Status), «Пов'язані об'єкти групової політики» (Linked Group Policy Objects), «Спадкування групової політики» (Group Policy Inheritance) та «Делегування» (Delegation). Ці вкладки дозволяють переглядати поточний стан GPO, розуміти механізми застосування та спадкування політик, а також керувати налаштуваннями делегування для контролю повноважень щодо модифікації політик. На рисунку 5.2 продемонстровано інтерфейс GPMC на контролері домену з виділенням ключових компонентів та макета [3].

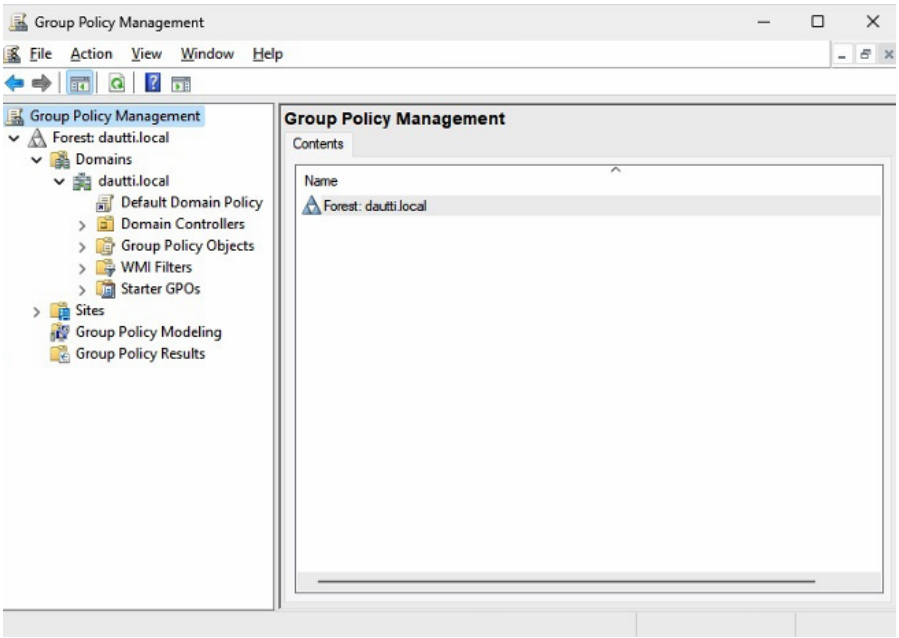

Рисунок 5.2 – Консоль GPM на контролері домену [3]

Доступ до консолі GPM у Windows Server 2025 може бути реалізований кількома методами, кожен з яких пропонує різні шляхи запуску інструменту залежно від адміністративних потреб. Ці методи, які забезпечують всебічне розуміння ефективного використання GPMC для керування налаштуваннями GP та гарантування послідовного застосування політик у мережі, будуть розглянуті нижче. Важливо також зазначити необхідність надання чітких інструкцій щодо виключення або фільтрації конкретних користувачів та пристроїв із процесу застосування GP, оскільки багато середовищ вимагають адаптованих конфігурацій. Розуміння нюансів обробки GP, включаючи налаштування фільтрації та безпеки, дозволяє адміністраторам впевнено орієнтуватися у складних середовищах [4].

Адміністративні шаблони є критичним компонентом керування GP у Windows Server 2025, забезпечуючи структурований спосіб конфігурації та примусового застосування політик у середовищі. Шаблони для Windows Server постачаються у вигляді файлів формату .ADMX і зазвичай входять до складу інсталяції Windows Server. Однак для доступу до

найновіших налаштувань, особливо для нових функцій, адміністраторам рекомендується періодично завантажувати актуальні версії з Центру завантажень Microsoft. Отримані файли .ADMX розміщуються у Центральному сховищі для GP у папці SYSVOL контролера домену, що гарантує можливість посилання всіх GPO на найновіші налаштування адміністративних шаблонів [3].

Процедура оновлення адміністративних шаблонів є важливою, оскільки Microsoft випускає нові шаблони з оновленнями та пакетами оновлень. Для оновлення виконуються наступні кроки: завантаження останніх версій з веб-сайту Microsoft, заміна існуючих файлів .ADMX у Центральному сховищі новими версіями, оновлення пов’язаних мовних файлів .ADML (які також зберігаються в Центральному сховищі) для відображення нових або змінених налаштувань, та оновлення всіх екземплярів GPMC для розпізнавання змін. Ефективне керування шаблонами вимагає дотримання найкращих практик, таких як регулярна перевірка оновлень (особливо після значних оновлень Windows), тестування нових шаблонів у невиробничому середовищі перед широким розгортанням для оцінки їх впливу, а також ведення документації щодо внесених змін, включаючи обґрунтування та дату оновлень, для сприяння майбутнім аудитам та усуненню несправностей. Впровадження цих практик дозволяє використовувати повний функціонал GP та мінімізувати ризики помилок конфігурації [26].

Для відкриття консолі GPM можна скористатися опцією «Засоби адміністрування» (Administrative Tools) у меню «Пуск», яка надає доступ до різноманітних інструментів керування. Процес розпочинається натисканням кнопки «Пуск» та переходом до розділу «Засоби Windows» (Windows Tools), де у списку наявних інструментів обирається «Керування груповою політикою» (Group Policy Management), як це проілюстровано на рисунку 5.3.

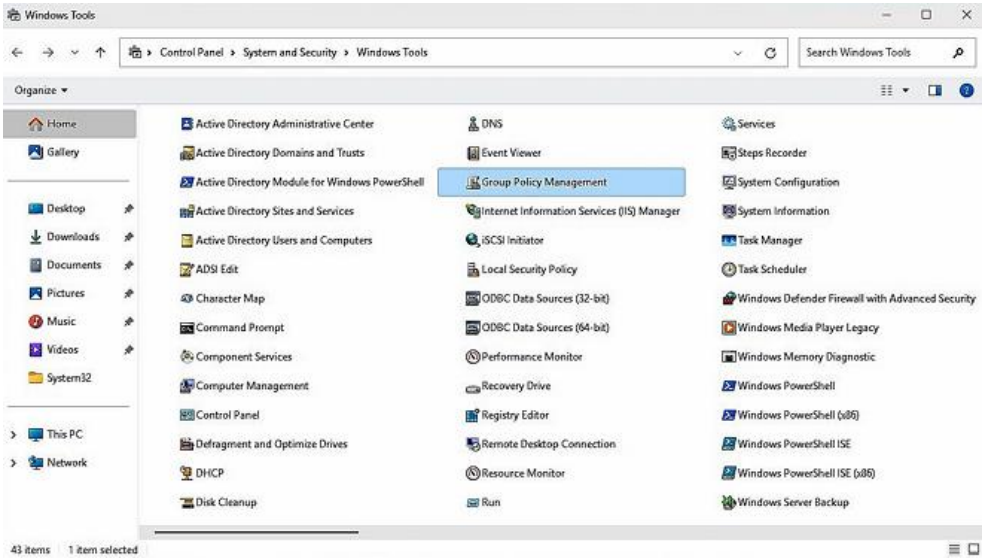

Рисунок 5.3 – Доступ до консолі GPM із засобів Windows [3]

Альтернативним та ефективним методом є використання діалогового вікна «Виконати», що дозволяє швидко отримати доступ до консолі за допомогою простої команди. Для цього необхідно одночасно натиснути клавіші Windows + R, у текстовому полі ввести команду gpmc.msc та натиснути OK, як показано на рисунку 5.4. Ця команда забезпечує миттєвий запуск GPMC, надаючи централізований інтерфейс для керування налаштуваннями групових політик.

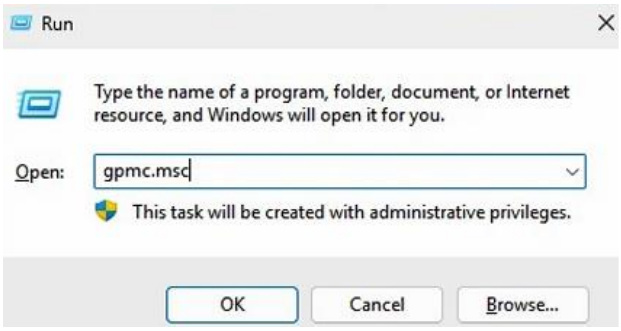

Рисунок 5.4 – Доступ до консолі GPM з діалогового вікна «Виконати» [3]

Також консоль GPM можна запустити через «Диспетчер серверів» (Server Manager) у меню «Пуск». Після відкриття вікна диспетчера серверів слід перейти до меню «Засоби» (Tools) та обрати «Керування груповою політикою», як зображено на рисунку 5.5. Ця дія відкриває GPMC, дозволяючи ефективно керувати налаштуваннями групових політик.

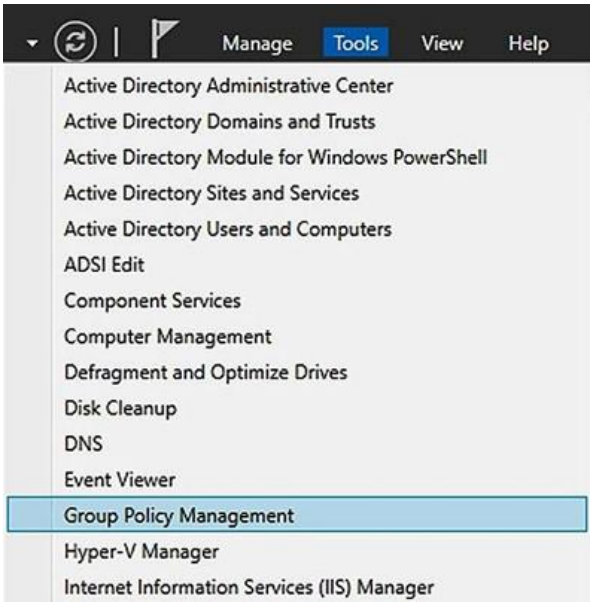

Рисунок 5.5 – Доступ до консолі GPM з диспетчера серверів [3]

Ефективне керування групровими політиками є необхідною умовою підтримання безпечного та ефективного середовища Windows Server. Дотримання найкращих практик дозволяє оптимізувати впровадження GP, забезпечити відповідність вимогам та мінімізувати

потенційні проблеми. Рекомендується обмежувати використання стандартних політик (Default GPs), оскільки вони можуть бути надто складними. Натомість доцільно створювати спеціальні GPO, адаптовані до конкретних потреб організації, що зменшує ризик ненавмисних наслідків. Необхідно впровадити чітку конвенцію найменування GPO, що відображає їх призначення та сферу дії (наприклад, із префіксом відділу), що спрощує ідентифікацію та аудит. Важливим є регулярний перегляд та очищення застарілих або надлишкових GPO для підтримки керованості ландшафту політик та покращення продуктивності системи. Перед розгортанням у виробничих системах нові або модифіковані GPO завжди повинні проходити тестування у контрольованому середовищі для виявлення конфліктів. Адміністратори зобов'язані вести ретельну документацію налаштувань, призначень та змін GPO. Крім того, слід використовувати фільтрацію безпеки та фільтрацію інструментарію керування Windows (WMI Filtering) для цільового застосування GPO до конкретних користувачів або груп, а також використовувати функцію моделювання GP (GP Modeling) для прогнозування впливу політик перед їх впровадженням [26].

Групова політика відіграє ключову роль у підвищенні організаційної ефективності та безпеки, узгоджуючи IT-практики з бізнес-цілями. Розглянемо реальні сценарії застосування. У фінансовій установі середнього розміру для зниження ризиків було впроваджено GPO для примусового виконання суворих політик паролів (зміна кожні 90 днів) та відключення локальних адміністративних прав на робочих станціях, що призвело до зниження кількості інцидентів безпеки на 40% протягом першого року. В університетському середовищі використання GP дозволило стандартизувати налаштування робочих столів, конфігурації принтерів та доступу до мережевих дисків, що зменшило кількість звернень до служби підтримки щодо проблем конфігурації на 30% та покращило робочий процес викладачів і студентів. У медичній організації IT-команда використала GP для налаштування служб оновлення Windows Server (WSUS), забезпечуючи автоматичне отримання пристроями останніх оновлень та патчів безпеки. Цей проактивний підхід мінімізував час простою через вразливості програмного забезпечення та дозволив досягти високого рівня відповідності стандартам охорони здоров'я. Ці приклади підкреслюють можливості GP щодо посилення безпеки та покращення взаємодії з користувачем у різних контекстах. У наступному розділі будуть детально розглянуті різноманітні налаштування конфігурації GPO [3].

Обробка групових політик, безпека і примінення по групах: як це працює?

Першочерговим аспектом, який необхідно усвідомити адміністратору стосовно групових політик, є той факт, що політики обробляються та застосовуються комп'ютерами та користувачами. Обробка виконується у чітко визначені моменти: під час запуску комп'ютера, при вході користувача, а також через фіксовані періоди часу. У процесі цієї обробки для

визначення доцільності застосування політики враховується множина факторів. Одним із таких важливих факторів є те, чи застосовувалася політика раніше, і якщо так, то чи зазнала вона змін з моменту останнього застосування. Цей та багато інших факторів використовуються для перевірки кожної політики перед її безпосереднім застосуванням до комп'ютера або користувача.

Комп'ютер здійснює обробку політик під час процедур запуску та зупинки, а також у ході періодичних фонових оновлень. За замовчуванням на рядових серверах та робочих станціях інтервал оновлень встановлено на рівні 90 хвилин із часовим зсувом від 0 до 30 хвилин. На контролерах доменів групові політики оновлюються кожні 5 хвилин. Впровадження зсуву є необхідним заходом для уникнення одночасної обробки або оновлення групових політик усіма комп'ютерами домену, що могло б призвести до зниження продуктивності контролерів доменів та рядових комп'ютерів. Якщо під час запуску комп'ютер здатен успішно виявити контролер домену з можливістю автентифікації та встановити з ним зв'язок, виконується обробка GPO. У ході цього процесу система перевіряє для кожного пов'язаного або успадкованого GPO, чи не змінилася політика з часу останнього циклу обробки, та чи виникає необхідність виконання стартових сценаріїв і перевірки інших вимог для повторного застосування політики. Під час зупинки системи та періодичних оновлень об'єкти групових політик знову підлягають перевірці на наявність оновлень або змін з моменту останнього застосування. Обробка GPO комп'ютера детермінується зв'язками GPO, фільтрами доступу та фільтрами інструментальних засобів керування Windows (Windows Management Instrumentation – WMI) [3].

Процес обробки GPO користувачів є значною мірою подібним до обробки GPO комп'ютерів. Ключова відмінність полягає в тому, що обробка GPO користувачів ініціюється при вході та виході користувача із системи, а також здійснюється періодично. Інтервал оновлення за замовчуванням для обробки GPO користувачів також дорівнює 90 хвилинам із додаванням зсуву від 0 до 30 хвилин. Обробка GPO користувачів визначається наявними зв'язками GPO та налаштованими фільтрами доступу.

Служба визначення розташування в мережі (Network Location Awareness – NLA) являє собою вбудовану у Windows службу, яка спроектована для визначення статусу підключення комп'ютера до інфраструктури Active Directory. Інфраструктура групових політик використовує NLA для прийняття рішення щодо необхідності завантаження та застосування об'єктів групових політик. Ця функція групових політик використовується також при перевірці зв'язності мережі – так званому визначенні повільних каналів зв'язку.

У попередніх версіях операційних систем при обробці групових політик для визначення надійності мережі застосовувалося повільне виявлення зв'язків. Цей механізм використовував для перевірки зв'язності протокол ICMP (Internet Control Message Protocol)

або пінгування, що характеризувалося недостатньою надійністю. Внаслідок цього обробка групових політик на мобільних та віддалених клієнтських робочих станціях була вкрай нестабільною. Коли робоча станція мобільного клієнта підключалася до корпоративної мережі через VPN-з'єднання або після виходу з режиму очікування чи сну, зміна у мережевій зв'язності зазвичай залишалася непоміченою системою, і об'єкти GPO не застосовувалися та/або не оновлювалися. У таких випадках єдиним способом застосування GPO до цих клієнтів було ручне примусове оновлення групових політик з командного рядка або перезавантаження комп'ютерів при підключенні до корпоративної мережі через провідні з'єднання Ethernet [4].

Починаючи з Windows Vista та у більш пізніх версіях, включаючи Windows Server 2012, 2016, 2022 та 2025, обробка групових політик використовує для виявлення змін у мережі перероблену службу NLA. Оновлена служба NLA значно ефективніше розпізнає зміни у мережевих підключеннях, і при встановленні з'єднання NLA перевіряє доступність контролера домену. За наявності зв'язку з контролером домену служба NLA повідомляє службу групових політик на комп'ютері, яка, у свою чергу, ініціює обробку параметрів групових політик як для комп'ютера, так і для користувача. Служба NLA функціонує незалежно від ICMP або ping, що саме по собі робить її більш надійною. Служба NLA повинна коректно виконуватися у більшості мереж без необхідності спеціальних налаштувань на мережевих пристроях або брандмауерах, навіть якщо протокол ICMP відключено або заблоковано.

Групові політики класифікуються на політики та переваги, а в їх структурі наявні різні частини, розділи та визначення, що регламентують порядок, час та умови обробки цих розділів. Обробка групових політик на стороні клієнта керується розширеннями групових політик на стороні клієнта (Client-Side Extension – CSE). Ці розширення представляють собою файли бібліотек DLL, які встановлюються в операційній системі сервера або локальної робочої станції. При обробці групових політик застосування налаштувань до клієнта відбувається саме за допомогою CSE. У клієнтських системах можуть існувати CSE як для політик, так і для переваг, і кожне розширення CSE має власну поведінку обробки [28].

Локальні групові політики (комп'ютер і користувач)

До Windows-систем та облікових записів користувачів Windows-систем можуть застосовуватися два різних типи політик: локальні групові політики та групові політики доменів Active Directory. Слід зазначити, що локальні групові політики існують у всіх Windows-системах, тоді як доменні групові політики доступні виключно в лісі Active Directory.

До випуску операційних систем Windows Vista та Windows Server 2008 сервери та

робочі станції мали можливість містити та застосовувати лише одну політику локального комп'ютера та користувача. Ця політика містила параметри, які можна було застосувати до локального комп'ютера та об'єктів користувачів з метою управління безпекою та конфігураційними налаштуваннями [4].

У багатьох середовищах, зазвичай через наявність вимог застарілих або виробничих систем, кінцевим користувачам часто призначалося членство в групі локальних адміністраторів для робочих станцій. Це виключало застосування багатьох параметрів безпеки, які повинні були поширюватися як на локальні, так і на групові політики. Кінцеві користувачі, які входять до групи локальних адміністраторів, могли перекривати параметри та змінювати налаштування, що створювало загрозу компрометації безпеки або, як це траплялося частіше, призводило до зниження надійності системи (рис. 5.6).

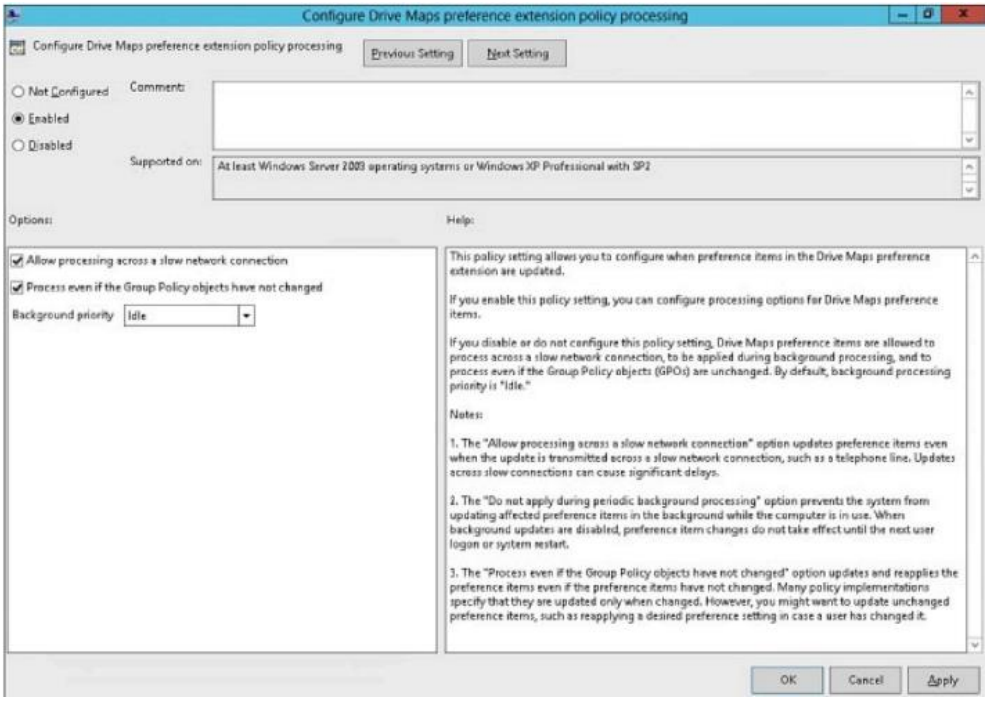

Рисунок 5.6 – Параметри обробки відображення дисків [4]

Крім того, політики можуть застосовуватися як до адміністраторів, так і до не адміністраторів локальних комп'ютерів. Це дозволяє адміністратору робочої станції нічого не вказувати в розділі користувача стандартної політики локального комп'ютера, натомість створюючи більш жорсткі політики для локальних користувачів і менш жорсткі – для членів групи адміністраторів на локальній робочій станції. Локальні групові політики користувачів можуть бути створені для конкретних користувачів, для всіх користувачів, які не є адміністраторами, а також для адміністраторів. Такий підхід дозволяє створювати різні конфігурації користувачів на основі облікових даних цих користувачів, зазначених під час входу в систему (рис. 5.7).

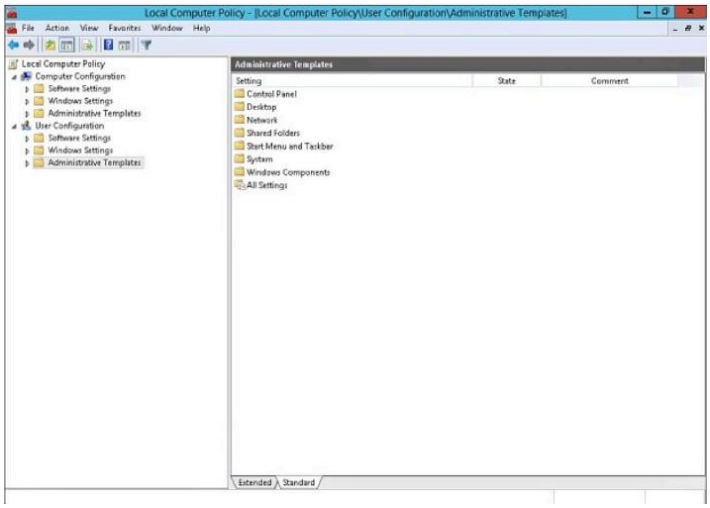

Рис. 5.7 – Перегляд параметрів локальної політики комп'ютера [4]

Групові політики на основі домену

Доменні групові політики мають суттєві відмінності від локальних групових політик, що зумовлено необхідністю наявності середовища Active Directory для їх створення та подальшого застосування. Ще однією значною відмінністю є те, що налаштування у групових політиках містять вузли як політик, так і вподобань, тоді як локальні групові політики позбавлені параметрів вподобань. Незважаючи на зазначені відмінності, більшість налаштувань залишаються ідентичними [4].

Слід зазначити, що доменні групові політики є більш зручними при визначенні критеріїв, які використовуються для застосування політики. Передбачено можливість фільтрації доменних політик для їх застосування до конкретних членів груп безпеки Active Directory, комп'ютерів або об'єктів, розташованих у конкретній підмережі чи організаційній одиниці (OU). Також існує можливість застосування політик до комп'ютерів, що функціонують під управлінням конкретної версії операційної системи. Крім того, при визначенні вподобань у доменній груповій політиці можна вказувати застосовність параметрів на рівні окремих елементів, базуючись на різних критеріях (рис. 5.8).

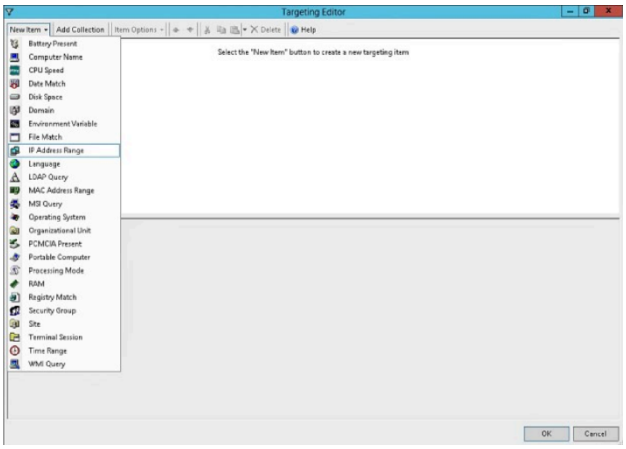

Рисунок 5.8 – Вказівка на рівні елементів для доменних GPP [4]

У структурі кожної політики локального комп'ютера та у вузлі конфігурації комп'ютера об'єкта групової політики (GPO) наявний розділ «Security Settings» (Параметри безпеки). Цей розділ включає параметри для політик аудиту комп'ютера, параметри управління обліковими записами, а також права, призначені користувачам. Унікальність цього розділу політики полягає в тому, що його можна імпортувати та експортувати окремо.

У попередніх версіях операційної системи Windows шаблони безпеки були сформовані заздалегідь, що надавало адміністраторам можливість швидкого завантаження набору рекомендованих параметрів конфігурації доступу. До переліку таких шаблонів належали базові шаблони робочої станції та сервера, а також шаблони високої безпеки, сумісної безпеки та безпеки контролера домену [4].

Для забезпечення управління стандартним набором налаштувань безпеки та його застосування до робочих груп і відокремлених систем адміністратори мають можливість скористатися функціями управління шаблонами безпеки. Використовуючи редактор об'єктів групових політик, редактор локальних політик безпеки або консоль налаштування та аналізу безпеки, можна імпортувати певний базовий шаблон, налаштувати або скоригувати параметри відповідно до наявних вимог, після чого експортувати чи зберегти ці параметри у спеціалізованому файлі шаблону. Надалі цей спеціалізований файл шаблону може бути імпортований або застосований до всіх необхідних систем за допомогою вищезгаданих інструментів.

Варто зауважити, що шаблони безпеки існують у Windows Vista, Windows Server 2008 та новіших версіях Windows. Ці базові шаблони безпеки розміщуються в каталозі %systemroot%\inf або c:\windows\inf. Номенклатура імен усіх стандартних шаблонів безпеки передбачає початок з deflt та розширення .inf. Наприклад, у Windows Server 2012 наявні шаблони з іменами defltbase.inf, defltsv.inf та defltdc.inf, за допомогою яких можна виконати стандартну конфігурацію параметрів безпеки системи [4].

Окрему увагу слід приділити ризикам, пов'язаним із застосуванням шаблонів. Імпорт шаблонів безпеки на вже розгорнуті сервери, робочі станції та контролери доменів може призвести до виникнення проблем із безпекою, таких як неможливість входу в комп'ютер або втрата доступу до системи з мережі. У зв'язку з цим, обов'язковою вимогою є проведення тестування всіх змін параметрів безпеки у випадку виконання імпорту та застосування шаблонів безпеки.

Розуміння групової політики

Об'єкти групових політик (GPO) зберігаються одночасно у файловій системі та в базі даних Active Directory. Кожен домен у лісі Active Directory містить повну копію всіх GPO цього домена. Усередині Active Directory зв'язки та відомості про версії GPO зберігаються в

розділі бази даних, що містить контекст іменування доменів. Оскільки цей розділ реплікується лише в межах одного домену, завантаження та обробка GPO, що мають зв'язки з іншими доменами (за допомогою сайтів або просто міждоменних зв'язків GPO), може зайняти більше часу [25].

Параметри GPO зберігаються у файловій системі всіх контролерів домену, в папці SYSVOL. Ця папка спільно використовується всіма контролерами домену. У кожного GPO домену є відповідна йому папка, яка знаходиться в підпапці sysvol\companyabc.com\Policies (рис. 5.9).

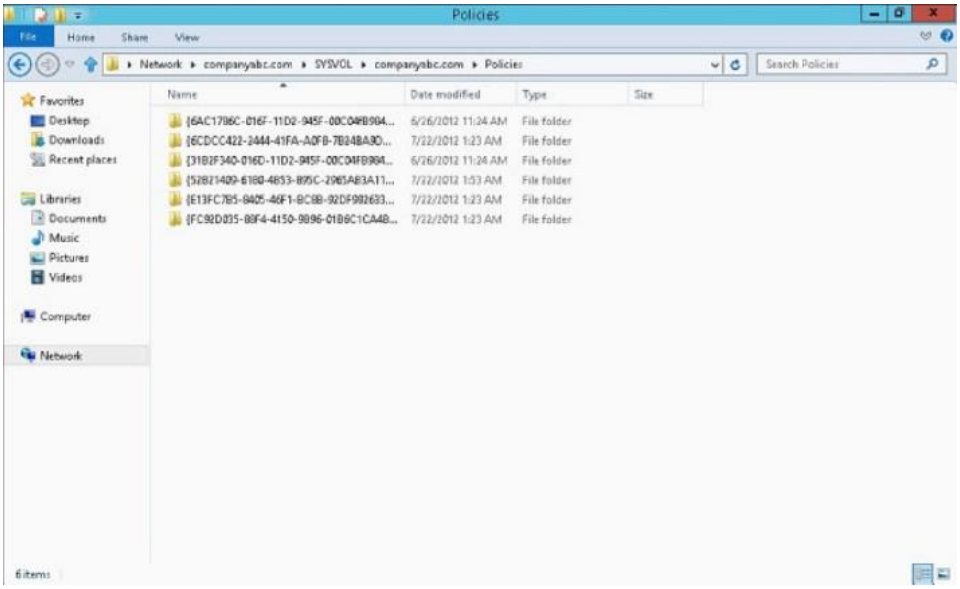

Рисунок 5.9 – Вміст підпапки Policies папки SYSVOL [4]

В якості імені папки GPO використовується глобально унікальний ідентифікатор (Globally Unique Identifier – GUID), привласнений цьому GPO під час його створення. Цей GUID відображається при перегляді властивостей GPO домену в консолі управління груповими політиками [4].

У папці GPO знаходиться звичайний набір підпапок і файлів: папка User, папка Machine (іноді папки ADM, Preferences, Scripts тощо) і файл gpt.ini. Кожна підпапка в ієрархії папок GPO містить файли та папки, пов'язані з конкретним розділом політики або вподобання.

Оскільки об'єкти GPO зберігаються в базі даних Active Directory та у файловій системі контролера домену, вся інформація GPO реплікується контролерами домену. Частина об'єктів GPO домену, що зберігається у файловій системі, реплікується в групі Domain System Volume Distributed File System Replication за допомогою служби реплікації розподіленої файлової системи (Distributed File System Replication – DFSR) [4].

Графік реплікації SYSVOL управляється графіком DFSR, який за замовчуванням

збігається з циклом реплікації бази даних Active Directory. Реплікація виконується кожні 5 хвилин або негайно між контролерами домену одного сайту Active Directory та за графіком реплікації зв'язків сайтів між контролерами домену для різних сайтів. Для застарілих доменів замість DFSR використовується служба реплікації файлів (FRS) [4].

Підпапка User (Користувач) містить файли та папки, що використовуються для зберігання параметрів, програм, сценаріїв та інших налаштувань для політик користувача та об'єкта користувача, сконфігурованих у даному GPO.

Підпапка Machine (Комп'ютер) містить файли та папки, що використовуються для зберігання параметрів, програм, сценаріїв та інших налаштувань для політик комп'ютера або об'єкта комп'ютера, сконфігурованих у даному GPO.

Підпапка Preference (Вподобання) містить файли та папки, що використовуються для зберігання параметрів, завдань і будь-яких інших налаштувань політик для конкретного комп'ютера або об'єкта комп'ютера, сконфігурованих у даному GPO.

Підпапка ADM створюється для нових GPO, якщо в них імпортуються файли адміністративних шаблонів старого формату. Усі GPO, створені за допомогою клієнтських програм Windows 2012 Server і Windows XP або Windows 2022 Server і Windows Server 2025, містять підпапку ADM, де зберігаються всі файли адміністративних шаблонів, які імпортовані в цей GPO і на які є посилання в цьому GPO. Нові об'єкти GPO, створені в Windows Server 2012, за замовчуванням не містять цю підпапку.

У кожній груповій політиці параметри розбиті на кілька розділів. Багато параметрів GPO визначають ключі та значення системного реєстру. Стан і значення таких ключів зберігаються у файлах registry.pol в одній із папок User або Machine. Для оптимізації роботи файл registry.pol містить лише параметри, налаштовані в GPO.

При створенні об'єкта GPO для нього створюється папка в папці SYSVOL пов'язаного з ним контролера домену. У корені цієї папки GPO є файл з іменем gpt.ini, який містить номер ревізії GPO. Цей номер використовується при обробці GPO об'єктом комп'ютера або користувача. Під час першої обробки GPO номер ревізії зберігається в системі, а при наступних обробках номер із файлу gpt.ini порівнюється зі значенням, що зберігається в кеш-пам'яті локальної системи. Якщо цей номер не змінився, деякі частини GPO не обробляються. Однак існують і такі частини GPO, які обробляються завжди – наприклад, сценарії [4].

При кожній зміні GPO номер посилання або ревізії збільшується, і хоча файл gpt.ini містить одне число, воно насправді представляє собою окремий номер ревізії для розділу комп'ютера і користувача даного GPO.

Стандартне налаштування на відсутність обробки деяких розділів GPO при незмінному номері ревізії можна скасувати. У деяких випадках, навіть якщо GPO не

змінився, користувач або програма можуть змінити важливі параметри, а іноді просто потрібна примусова обробка всього GPO.

У більшості випадків адміністративні шаблони GPO являють собою набір текстових або XML-файлів, що містять чітко визначені параметри, яким можна присвоїти ряд різних значень. Адміністративні шаблони надають адміністраторам легкий доступ до багатьох конфігураційних параметрів, що зазвичай використовуються для управління комп'ютерами серверів і робочих станцій, а також кінцевими користувачами [4].

При створенні нового GPO в цю політику імпортується базовий набір адміністративних шаблонів або посилання на них. Можна імпортувати й додаткові адміністративні шаблони, щоб додати в будь-яку політику потрібні функції. Коли в існуючій мережі встановлюються нові операційні системи, адміністратори групових політик побачать інші значення в редакторах групових політик при редагуванні політики в новішій ОС. Це може призвести до плутанини та проблем, тому всім адміністраторам слід застосовувати нові адміністративні шаблони. Швидкий спосіб для ефективного використання таких шаблонів в організації – задіяння центрального сховища групових політик і оновлення адміністративних шаблонів у цьому сховищі при появі кожної нової операційної системи.

Як було зазначено раніше, кожен GPO в лісі Active Directory повинен був мати відповідну папку в папці SYSVOL кожного контролера того домену, в якому створювався цей GPO. Якщо контролери конкретного домену працюють під управлінням Windows Server, то кожна з таких папок GPO повинна була містити (в папці ADM) копії всіх адміністративних шаблонів, завантажених у даний GPO. Це призводило до великого обсягу дублювання файлів адміністративних шаблонів, вимагало додаткового місця та збільшувало обсяг реплікації між контролерами доменів.

У новій інфраструктурі групових політик, яка з'явилася в Windows Vista та Windows Server 2008 і присутня в Windows Server 2025, створені GPO зберігають лише файли та папки, потрібні для зберігання встановлених параметрів, сценаріїв, registry.pol та інших файлів, що мають відношення до GPO. При відкритті GPO для редагування або обробки на комп'ютері Windows Vista, Windows Server 2008 або новішої версії використовується посилання на локальну копію адміністративних шаблонів, але вони не копіюються в папку нового GPO в папці SYSVOL. Натомість у файлах, які зберігаються на локальних робочих станціях або в центральному сховищі домену, є посилання на адміністративні шаблони [3].

Центральне сховище GPO – це файлове сховище, в якому зберігаються всі адміністративні шаблони наступного покоління. Це центральне сховище призначене для зберігання всіх нових адміністративних шаблонів ADMX і ADML, і в кожній робочій станції зберігаються посилання на файли в контролері домену, який застосовується для обробки її групових політик. Тепер при відкритті або обробці GPO система спочатку перевіряє

наявність центрального сховища, а потім використовує шаблони, що зберігаються тільки в цьому сховищі. Центральне сховище GPO можна створювати в інфраструктурах Active Directory, де працюють контролери доменів Windows Server 2003 або новішої версії [4].

Консолі управління груповими політиками в Windows Server надають інструмент управління GPO під назвою «стартові об'єкти GPO». Стартові GPO схожі на звичайні GPO, але містять лише параметри, доступні з адміністративних шаблонів. Як і шаблони безпеки, які можна використовувати для імпорту та експорту сконфігурованих параметрів у розділі безпеки політики, стартові GPO можна застосовувати для первинного заповнення розділів Administrative Templates (Адміністративні шаблони) вузлів GPO під назвами Computer Configuration (Конфігурація комп'ютера) і User Configuration (Конфігурація користувача) [4].

Після появи Windows Server 2008 компанія Microsoft випустила набір визначених стартових GPO, які зараз входять до складу Windows Server 2025 і які можна отримати на основі інформації з керівництва Microsoft з безпеки клієнтів у Windows XP та Windows. Ці стартові GPO є політиками лише для читання, але адміністратори мають можливість створювати власні стартові GPO, необхідні в організації. Активація функціональності стартових GPO, створення та управління ними описані в розділі «Створення та застосування стартових об'єктів GPO» далі.

Параметри політики – це параметри, доступні для налаштування в конкретному об'єкті GPO. Ці параметри беруться з базових адміністративних шаблонів, налаштувань безпеки, сценаріїв, якості обслуговування (QoS), заснованого на політиці, і, в деяких випадках, з пакетів розгортання ПЗ. Багато параметрів політик відповідають «один до одного» деяким ключам і значенням системного реєстру. Для різних параметрів існують різні допустимі значення, у тому числі й довільний текст.

Параметри політик GPO зазвичай мають одне з трьох значень: не вказано, увімкнено або вимкнено. Адміністраторам дуже важливо не тільки усвідомити різницю між цими трьома значеннями, а й знати, чим керує кожен параметр політики. Наприклад, параметр політики, що забороняє доступ до панелі управління, блокує доступ, коли він увімкнений, і дозволяє доступ, якщо він вимкнений.

Параметри політик GPO застосовуються до об'єктів комп'ютерів або користувачів. Адміністратор може виявити в одному й тому ж GPO певний параметр політики і у вузлі конфігурації комп'ютера, і у вузлі конфігурації користувача. У таких випадках, тобто коли параметр політики заданий для обох об'єктів, і політика пов'язана з об'єктом користувача та робочої станції, в яку входить користувач, налаштування комп'ютера перекриває налаштування користувача.

У групових політик є два основних вузли налаштувань – Computer Configuration (Конфігурація комп'ютера) та User Configuration (Конфігурація користувача). Кожен із них

містить два інші вузли – Policies (Політики) та Preferences (Вподобання/Рекомендовані).

Вузол Policies (Політики), який знаходиться в конфігурації групових політик як для комп'ютерів, так і для користувачів, містить параметри, які здебільшого застосовуються примусово і не можуть переналаштовуватися клієнтами. Якщо параметри можуть мати кілька значень, то параметри з вузлом Policies обов'язково застосовуються до клієнта, але адміністратори можуть додати або змінити і свою частину налаштувань. Наприклад, якщо присвоєння прав користувачеві виконано за допомогою доменної політики, адміністратор не зможе видалити елементи цих прав, призначені з політики, але він зможе додавати та змінювати інші елементи. Вузол Policies містить налаштування безпеки (брандмауера та мережі), але основний обсяг налаштувань міститься в розділі Administrative Templates (Адміністративні шаблони) [4].

Вузол Preferences (Вподобання), який знаходиться в конфігурації групових політик як для комп'ютерів, так і для користувачів, містить параметри, які здебільшого раніше не були присутні в групових політиках і управляються спеціальними сценаріями та адміністративними шаблонами. Параметри вподобань задаються початково, але зазвичай кінцевий користувач може змінити їх після обробки групових політик [4].

Інструменти керування політиками

Корпорацією Microsoft було розроблено кілька різних засобів, за допомогою яких адміністратори мають можливість створювати локальні та групові політики й керувати ними. Функціональні можливості цих засобів варіюються залежно від версії операційної системи, що використовується для адміністрування. Наприклад, при створенні групових політик за допомогою консолі управління груповими політиками у Windows Server 2025 у папках GPO застосовуються нові шаблони ADMX/ADML, тоді як засоби Windows XP та Windows Server 2003 заносять у ці папки файли шаблонів у первинному форматі ADM.

Найбільш функціональним і корисним засобом, призначеним для створення та управління груповими політиками Active Directory, є консоль управління груповими політиками (Group Policy Management Console – GPMC). Ця консоль була впроваджена після випуску Windows Server 2003, причому параметри та дії для створення й управління груповими політиками Active Directory, що надаються нею, різняться залежно від версії операційної системи. Вона виступає основним інструментом керування інфраструктурою групових політик. GPMC являє собою оснастку консолі управління Microsoft (Microsoft Management Console – MMC), яку можна інтегрувати у спеціалізовану консоль. Вона пропонує адміністраторам більшу частину функцій, необхідних для управління політиками [27].

Консоль GPMC, що постачається з Windows Server 2025, дозволяє виконувати

широкий спектр функцій адміністрування. Зокрема, здійснюється активізація можливостей стартових GPO, створення нових стартових GPO, створення нових групових політик домену, а також створення нових групових політик із використанням стартових об'єктів GPO як шаблонів. Окрім того, забезпечується створення та налаштування зв'язків GPO із сайтами, доменами та організаційними одиницями, перегляд та управління GPO у доменах у локальних і довірених лісах Active Directory. Важливою функцією є резервне копіювання та відновлення одного GPO або всіх GPO у домені, а також стартових GPO. Також підтримується імпорт групових політик із зовнішніх доменів та перенесення параметрів безпеки за допомогою таблиць перенесення для забезпечення коректного виконання імпорту.

Функціонал консолі також охоплює управління зв'язками GPO, включно з примусовим застосуванням, увімкненням та вимкненням, блокування успадкування параметрів для сайтів, доменів та організаційних одиниць, а також управління статусом GPO для вказівки того, які вузли в GPO мають бути увімкнені або вимкнені. Передбачено створення та прив'язку фільтрів WMI для GPO, управління фільтрами доступу GPO, управління делегуванням GPO та адміністративною безпекою, а також управління порядком обробки GPO у контейнерах із кількома прив'язаними GPO. Адміністратор має змогу переглядати всі встановлені у наявних групових політиках параметри та іншу додаткову інформацію, таку як номер ревізії, фільтри, делегування, та створювати експортовані звіти про конфігурацію. Також доступна перевірка стану реплікації інфраструктури GPO, генерація HTML-звітів зі зведенням налаштувань і параметрів групових політик. Додатково можна запустити майстер моделювання групових політик (Group Policy Modeling Wizard) для визначення того, як будуть застосовуватися групові політики до користувачів або комп'ютерів у конкретних контейнерах, або майстер результатів групових політик (Group Policy Results Wizard) для аналізу застосування політик до конкретних об'єктів. Багато з перерахованих функцій адміністрування GPMC будуть детально описані далі в цьому розділі [25].

Редактор об'єктів групової політики (Group Policy Object Editor – GPOE) визначається як засіб, призначений для редагування локальних групових політик для комп'ютерів і користувачів. У кожного комп'ютера-сервера або робочої станції наявна стандартна локальна політика безпеки. Доступ до цієї політики здійснюється за допомогою ярлика спеціальної оснастки MMC під назвою «Local Security Policy» (Локальна політика безпеки), який розміщено в папці «Administrative Tools» (Адміністрування). Оскільки у Windows Server 2008 і пізніших версіях підтримуються кілька локальних групових політик, редактор GPOE слід використовувати для управління або створення всіх локальних групових політик, відмінних від стандартної. Редактор GPOE дозволяє правити всі конфігураційні параметри політики: задавати параметри безпеки, встановлювати програмні пакети, створювати обмежуючі політики, визначати сценарії, що використовуються комп'ютерами та користувачами, та

виконувати багато інших функцій [3].

Для управління груповими політиками доменів належить застосовувати редактор управління груповими політиками (Group Policy Management Editor – GPME), який виконує ті ж функції, що і GPOE, плюс додаткові, доступні тільки в цьому редакторі. Однією з істотних відмінностей є те, що в GPME наявний не тільки вузол Policy Settings (Параметри політики), а й вузол Preferences Settings (Рекомендовані параметри), який доступний тільки в доменах. Для встановлення GPME у Windows Vista і пізніших версіях потрібно завантажити та встановити засіб RSAT для конкретної операційної системи та пакету виправлень. В операційних системах Windows Server 2012, Windows Server 2022 та Windows Server 2025 засоби роботи з груповими політиками можна встановити з аплету Add Features (Додавання компонентів), який наявний у диспетчері серверів.

Редактор стартових об’єктів GPO для групових політик (Group Policy Starter GPO Editor) призначений для редагування стартових GPO, створених адміністраторами групових політик. Ця консоль відображає тільки вузли Administrative Templates (Адміністративні шаблони) у розділах Computer Configuration (Конфігурація комп’ютера) та User Configuration (Конфігурація користувача) для стартового об’єкта GPO. За замовчуванням у стартових GPO можна встановлювати лише параметри, доступні в розділах адміністративних шаблонів. Проте Microsoft надає стартові GPO, доступні тільки для читання. Редактор стартових об’єктів GPO входить до складу засобу адміністрування віддаленого сервера (Remote Server Administration Tools) для Windows Server 2025 [4].

Консоль управління друком (Print Management Console) вперше з’явилася в редакції Windows Server 2003 R2. Вона використовується для управління принтерами Active Directory та принтерами локальних серверів і робочих станцій (рис. 5.10).

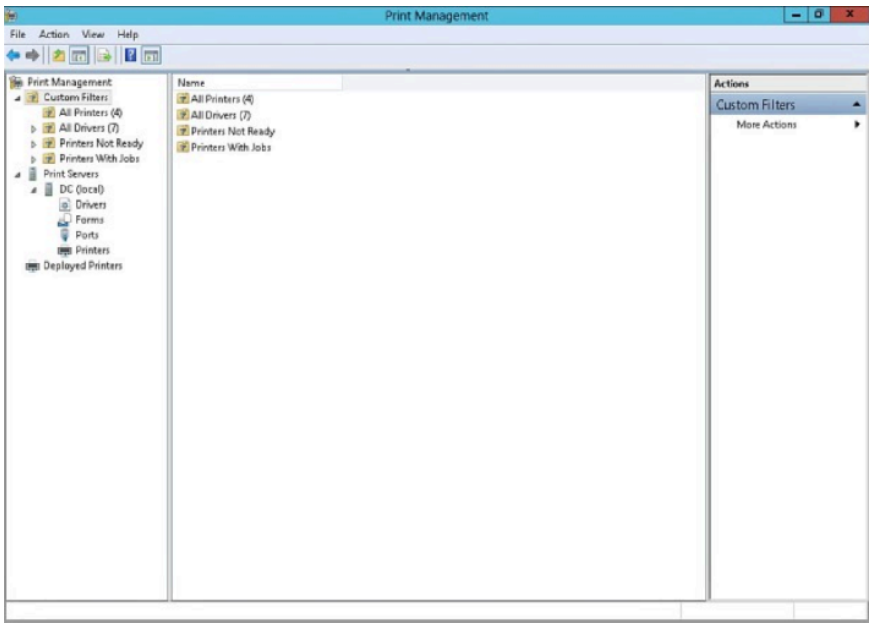

Рисунок 5.10 – Консоль управління друком [4]

За допомогою консолі управління друком, показаної на рисунку 5.10, можна переглядати налаштування, конфігурувати драйвери та параметри, а також керувати принтерами та завданнями друку в окремих системах або у всій Active Directory. Крім того, за її допомогою можна розгортати принтери для комп'ютерів або користувачів – використовуючи вузол Deployed Printers (Розгорнуті принтери). Функція розгортання принтерів розширює можливості групових політик щодо розгортання принтерів у визначеній множині об'єктів користувачів або комп'ютерів, до яких прив'язаний GPO.

Засоби GPOE та GPME, містять вузол Deployed Printers (Розгорнуті принтери) під вузлом Windows Settings (Параметри Windows) у розділах параметрів Computer Configuration та User Configuration. У Windows Server 2008 і пізніших версіях консоль управління друком необхідно встановити за допомогою посилання Server Manager Features – Add Features (Компоненти диспетчера серверів – Додавання компонентів), і тоді вузол Deployed Printers стане доступним у консолях редактора групових політик. Якщо певна політика містить принтери, визначені у вузлах Deployed Printers, і ця політика переглядається за допомогою GPMC або GPME з Windows XP, то розгорнуті принтери не будуть відображатися. Вони також не будуть видимі у випадку, якщо політика відкрита на сервері Windows Server 2003 R2, а консоль управління принтерами не встановлена з компонентів Windows. У системах Windows Vista, Windows Server 2008 і пізніших версіях рекомендовано створювати GPO для розгортання принтерів виключно за допомогою GPMC та GPME. Щоб встановити консоль управління друком у Windows Server 2025, необхідно запустити в диспетчері серверів аплет Add Features і вибрати в підменю Remote Administration Tools (Засіб віддаленого адміністрування) пункт Print and Document Services Tools (Засіб обслуговування друку та документів).

Утиліта командного рядка gpupdate.exe призначена для допомоги адміністраторам у налагодженні обробки GPO та запуску обробки GPO за вимогою. Деякі розділи групових політик застосовуються тільки під час запуску комп'ютера та входу користувача, а інші – у ці моменти, а також при періодичних оновленнях. Якщо в такі моменти мережевий зв'язок із контролерами домену відсутній, параметри, що застосовуються під час запуску комп'ютера та входу користувача, можуть ніколи не бути застосовані. Крім того, ці політики зазвичай не застосовуються до віддалених або мобільних робочих станцій, систем у сплячому режимі або режимі очікування, та до користувачів, які входять у систему за допомогою кешованих повноважень. У цьому контексті важливу роль відіграє служба мережевого розташування (Network Location Awareness) з Windows Vista, Windows Server 2008 і пізніших версій, оскільки вона сповіщає систему про доступність контролера домену та ініціює цикл оновлення групових політик. Засіб gpupdate.exe дозволяє застосовувати політики користувача та комп'ютера негайно. Поширеним застосуванням є додавання виклику gpupdate.exe у

сценарій, що виконується у VPN після встановлення з'єднання, для застосування налаштувань до віддалених робочих станцій в інфраструктурі Active Directory [4].

У даної утиліти наявний ряд опцій. Параметр gpupdate.exe /Target: {Computer | User} дозволяє обробити тільки вказаний вузол групової політики. Опція gpupdate.exe /Force повторно застосовує всі параметри політики, при цьому не виконується автоматичне перезавантаження комп'ютера або вихід усіх користувачів. Параметр gpupdate.exe /Wait визначає час очікування (у секундах) завершення обробки GPO (значення за замовчуванням дорівнює 600 секунд, тобто 10 хвилин). Опція gpupdate.exe /Logoff виводить із системи обліковий запис користувача після завершення обробки GPO. Параметр gpupdate.exe /Boot виконує перезавантаження комп'ютера після завершення обробки групових політик, що необхідно для застосування параметрів GPO, які діють тільки під час запуску комп'ютера. Нарешті, опція gpupdate.exe /Sync обробляє параметри GPO, які застосовуються тільки під час запуску комп'ютера та входу користувача. Дана опція вимагає вказівки адміністратора щодо можливості перезапуску комп'ютера або виходу користувача із системи.

У Windows Server, починаючи з версії 2012 було впроваджено нову можливість. Адміністратори можуть примусово виконати оновлення групових політик на всіх системах заданої організаційної одиниці (OU) безпосередньо з GPMC. Ця функція була необхідна адміністраторам для максимально швидкого створення та застосування політик. Слід зазначити, що вона застосовна тільки до комп'ютерів, але не до користувачів. Для виконання цього завдання необхідно клацнути правою кнопкою миші на потрібній OU та вибрати в контекстному меню пункт Group Policy Update (Оновлення групової політики), як показано на рисунку 5.11.

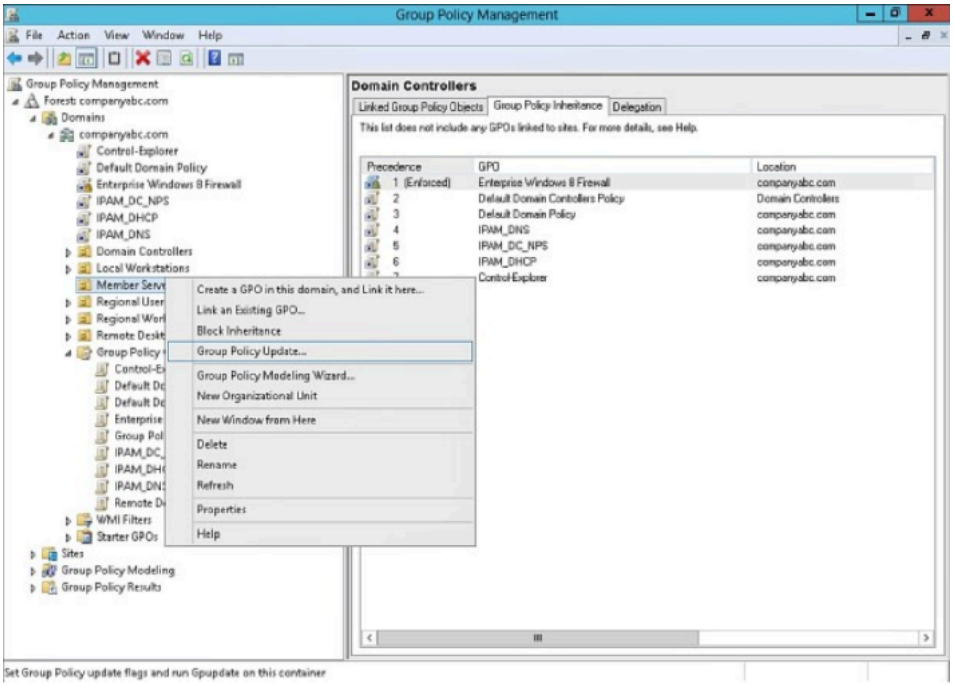

Рисунок 5.11 – Дистанційне оновлення групових політик із консолі GPMC [4]

Після вибору даного пункту буде запитано підтвердження, після чого у вікні Remote Group Policy Update Results (Результати дистанційного оновлення групової політики) можна буде переглянути результати.

Ще одним доповненням у консолі управління груповими політиками є відображення стану інфраструктури групових політик. Тепер із вікна GPMC адміністратори можуть переглянути стан реплікації GPO по всіх контролерах домену.

У версіях Windows Server 2012, 2016, 2022, 2025 додано можливість управління груповими політиками за допомогою PowerShell. Ця можливість автоматично активується при встановленні оснастки Group Policy Management. Корпорація Microsoft включила 28 готових командлетів PowerShell для роботи з груповими політиками. Ці командлети дозволяють адміністратору виконувати ряд різних дій, зокрема створення нових GPO та нових стартових GPO, створення нових зв'язків GPO, відновлення або імпорт GPO. Також підтримується видалення GPO та зв'язків GPO, читання та/або встановлення властивостей OU, успадкування зв'язків батьківського GPO або блокування успадкування, перейменування GPO. Засоби PowerShell дозволяють генерувати звіти по параметрах і конфігураціях GPO, звіти утиліти Resultant Set of Policies (Результуючий набір політик) та звіти по успадкуванню групових політик. Крім того, можливе встановлення та делегування адміністративних повноважень GPO, а також завдання політики GPO та рекомендованих параметрів, що зберігаються в системному реєстрі.

Для отримання списку командлетів для роботи з груповими політиками необхідно виконати певний алгоритм дій. Спершу потрібно увійти в систему зі встановленим засобом управління груповими політиками (Group Policy Management Tools), який можна встановити за допомогою засобу дистанційного адміністрування серверів. Потім слід помістити курсор миші в правий нижній кут робочого столу для появи панелі Charm і натиснути значок лупи для відкриття меню пошуку.

У меню Search (Пошук) знайти розділ Apps (Додатки), ввести слово «Windows» та вибрати елемент Windows PowerShell ISE. Коли вікно розкриється, необхідно у меню View (Перегляд) пересвідчитися, що відмічено прапорець Show Command Add-on (Показувати модуль команд). У правій частині вікна консолі, на панелі команд, розгорнути список Modules (Модулі) і вибрати пункт GroupPolicy, після чого з'явиться список відповідних командлетів (рис. 5.12). Для завершення роботи слід вибрати потрібні командлети та натиснути кнопку Show Details (Показати інформацію) для перегляду параметрів або значок із знаком питання для перегляду підказки, а потім закрити вікно консолі. Інтегроване середовище сценаріїв (Integrated Scripting Environment – ISE) Windows PowerShell є потужним засобом, що дозволяє опанувати використання PowerShell новими способами [4].

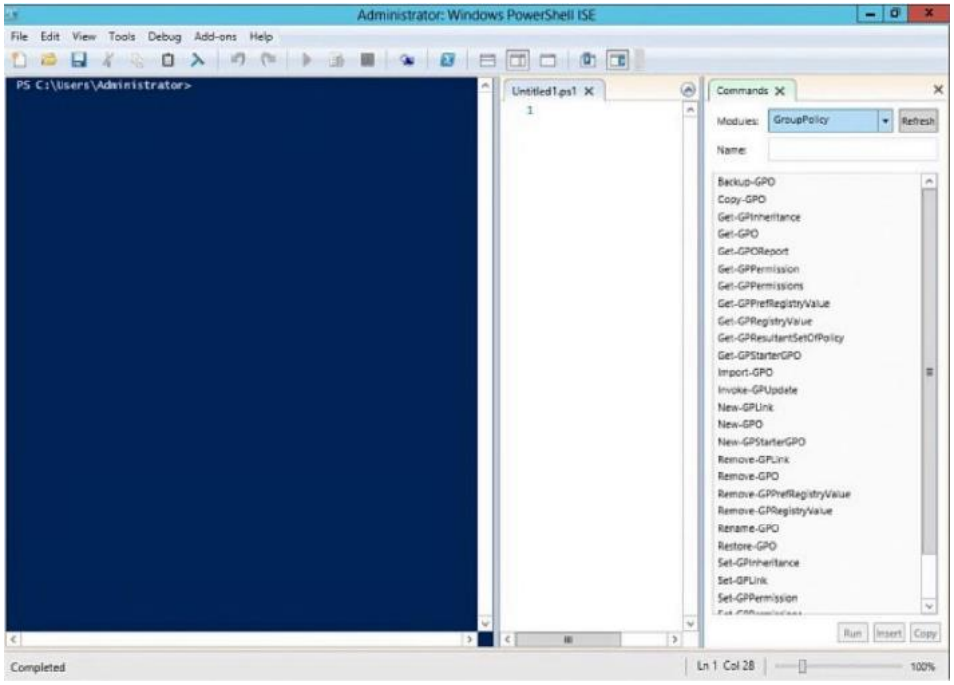

Рисунок 5.12 – Командлети PowerShell для роботи з груповими політиками [4]

Засіб Event Viewer (Перегляд подій) для Windows Server 2025 містить кілька нових журналів подій, до яких заносяться події обробки GPO (рис. 5.13). У журналах обробки GPO тепер фіксуються адміністративні події GPO, які зберігаються в системному журналі в категорії Group Policy зі шляхом Microsoft\Windows\GroupPolicy, та в журналі операційних подій GPO в категорії Applications and Services Logs (Журнали програм та служб) зі шляхом доступу Microsoft\Windows\GroupPolicy\Operational. За замовчуванням при обробці групових політик виконується мінімальна фіксація в журналі, але при необхідності обсяг інформації можна збільшити.

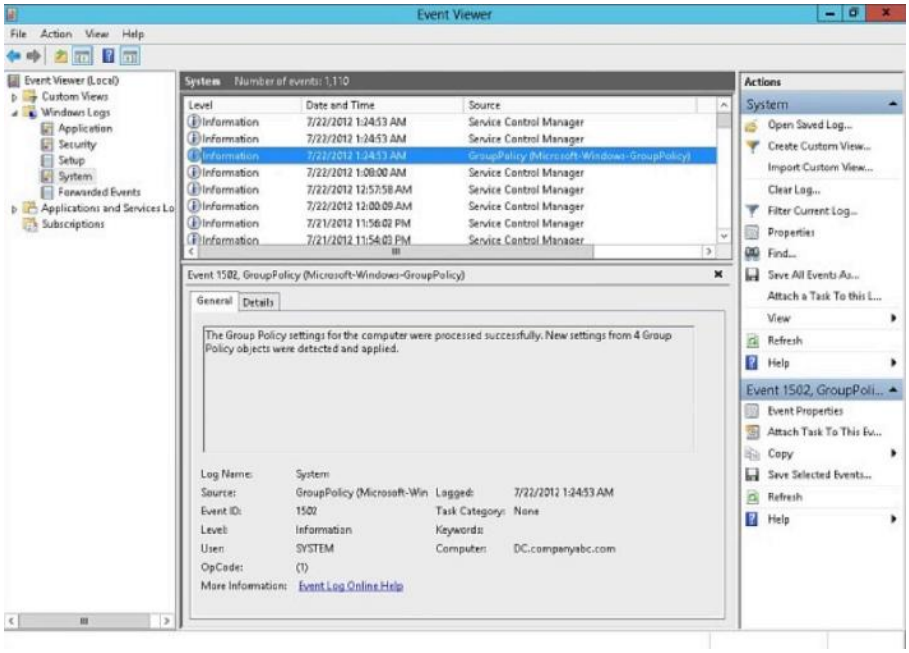

Рисунок 5.13 – Події групових політик [4]

Для перегляду адміністративних подій групових політик слід увійти в потрібний адміністративний сервер під управлінням Windows Server 2025 та відкрити засіб Event Viewer через меню Search – Apps. У вікні Event Viewer необхідно розкрити вузол Windows Logs (Журнали Windows), клацнути правою кнопкою миші на журналі System (Система) і вибрати пункт Filter Current Log (Фільтрувати даний журнал). У середині вікна фільтра слід розкрити список Event Sources (Джерела подій), знайти пункт Group Policy, відмітити його і знову клацнути у вікні фільтра для закриття списку. Після натискання кнопки ОК фільтр буде застосовано, і можна буде переглянути події. Якщо задачу завершено, фільтр можна очистити через контекстне меню пунктом Clear Filter [3].

До операційних подій відноситься дуже детальна інформація про обробку GPO. Під час обробки GPO операційні події з'являються майже для кожної задачі, що виконується, що суттєво полегшує налагодження. Для перегляду цих подій необхідно увійти на сервер, відкрити Event Viewer через All Programs – Administrative Tools, розкрити вузол Applications and Services Logs, далі вузол Microsoft, потім Windows і нарешті Group Policy. У контейнері Group Policy слід вибрати журнал Operational, де в правій панелі відобразяться події. Для отримання детальної інформації про конкретну подію достатньо натиснути на неї.

Файли GPO зберігаються в папці SYSVOL домену Active Directory та реплікуються службою реплікації розподіленої файлової системи (Distributed File System Replication – DFSR). Консоль DFS Management (Управління DFS) дозволяє адміністраторам налаштовувати параметри реплікації, зокрема графік реплікації та інші задачі управління DFS. Спільний ресурс SYSVOL називається томом доменної системи, і реплікація цього тому виконується за графіком реплікації зв'язків сайтів. Зміна або управління графіком реплікації системного тому домену між контролерами домену в одному й тому ж сайті Active Directory не підтримується. Натомість у GPMC Windows Server 2025 з'явилася можливість переглядати стан інфраструктури групових політик, тобто стан реплікації файлів GPO, що зберігаються на сервері в папці SYSVOL.

Проєктування інфраструктури групових політик

Для успішного проєктування інфраструктури групових політик необхідне глибоке розуміння конфігурацій та параметрів, доступних в об'єктах групових політик (GPO). У спеціалізованій літературі та відповідних розділах курсу описуються доступні параметри, які адміністратори можуть задавати за допомогою групових політик, а також деякі рекомендовані конфігурації. У даному розділі будуть описані високорівневі кроки, необхідні для успішного планування та розгортання надійної інфраструктури групових політик.

Щоб зрозуміти, як найкраще спланувати інфраструктуру групових політик, спочатку необхідно з'ясувати, яким чином сконфігурована інфраструктура Active Directory.

Інфраструктура Active Directory у сайті, домені та організаційній одиниці (OU) зазвичай ґрунтується на кількох ключових елементах: фізичному розташуванні офісів, мережевому зв’язку та делегуванні адміністрування. До останнього елемента входять управління філіями, розподіл завдань управління Active Directory, адміністрування робочих комп'ютерів і серверів та, безумовно, безпека й надійність.

Групові політики можна прив’язувати до об’єктів сайтів Active Directory. Не існує стандартної політики сайтів, що створюється під час первинного розгортання Active Directory. У групових політиках, прив’язаних до сайтів, часто застосовуються параметри, що стосуються мережі – профілі бездротових мереж, налаштування безпеки та, можливо, розгортання принтерів на сайті [27].

При вирішенні питання про доцільність прив’язки GPO до сайту слід враховувати низку факторів. Необхідно визначити, чи буде обробляти політику кожен об’єкт сайту, визначений пов’язаною з цим сайтом підмережею, незалежно від домену, в якому знаходиться обліковий запис користувача або комп’ютера, та чи є бажаною така конфігурація. Також важливо з’ясувати, чи містить сайт контролер домену в тому домені, в якому створена групова політика. Слід проаналізувати, чи містять пов’язані із сайтом підмережі ділянки з повільними зв’язками або віртуальні приватні мережі, оскільки в такому випадку для правильної обробки може знадобитися зміна стандартних значень або відключення визначення повільних зв’язків у політиці сайту. Крім того, варто звернути увагу на наявність спеціальних вимог до безпеки сайту, для яких потрібен вищий рівень безпеки або спеціальне налаштування програм.

Перш ніж виконати прив’язку GPO до сайту, цей сайт необхідно додати в консоль управління груповими політиками (GPMC). Процедура додавання сайту та створення зв’язку GPO передбачає виконання певної послідовності дій. Спершу здійснюється вхід на потрібний адміністративний сервер під управлінням Windows Server 2025 та відкривається консоль управління груповими політиками. Далі необхідно клацнути правою кнопкою миші на контейнері Sites (Сайти) і вибрати в контекстному меню пункт Show Sites (Показати сайти). У вікні Show Sites слід натиснути кнопку Select All (Вибрати все) або відзначити прапорець біля сайту, який потрібно додати в GPMC, та натиснути кнопку ОК. Після цього в панелі з деревоподібним поданням розкривається контейнер Sites, виконується клік правою кнопкою миші на потрібному сайті та обирається варіант Link an Existing GPO (Зв’язати з наявним GPO). У вікні Select GPO обирається вихідний домен, з якого потрібно виконати прив’язку, вказується необхідний об’єкт GPO в розділі Group Policy Objects і натискається кнопка ОК. Завершальним етапом є налаштування параметрів для кожного нового зв’язку за необхідності [3].

Під час розгортання Active Directory створюються дві заздалегідь налаштовані

стандартні групові політики. Одна з них прив’язана до домену і називається Default Domain Policy (Стандартна політика домену), а інша прив’язана до OU контролерів домену і має назву Default Domain Controllers Policy (Стандартна політика контролера домену). Стандартна політика домену містить стандартні параметри безпеки для всього домену, зокрема й політики облікових записів і паролів. Рекомендується застосовувати цю політику тільки для управління стандартними політиками облікових записів для всього домену.

Усі додаткові параметри GPO, які потрібно застосовувати до всіх користувачів та/або комп’ютерів (контролерів доменів, серверів-членів та клієнтських робочих станцій), слід додавати в нові об’єкти групових політик і прив’язувати їх на рівні домену. Необхідно, щоб кількість політик, прив’язаних до доменного рівня, була мінімальною – інакше обробка групових політик в організації може сповільнитися. Зміни в стандартній політиці контролера домену будуть застосовані до всіх контролерів домену, тому до них треба ставитися з обережністю або реалізувати різні GPO, прив’язані до організаційної одиниці контролера домену.

Прив’язки GPO до організаційних одиниць є найбільш поширеним застосуванням зв’язків GPO. Вони забезпечують точне налаштування програм і детальний адміністративний контроль завдань, що відносяться до GPO організаційних одиниць, а також до налаштування та управління об’єктами, що містяться в OU. Єдиний спосіб більш точно вказати прив’язку до GPO організаційної одиниці – застосувати фільтр доступу або фільтр WMI до цього об’єкта GPO, але це вплине на всі прив’язки GPO, що відносяться до даної політики. Нова можливість у GPMC дозволяє адміністраторам примусово оновити комп’ютери в OU, і, хоча це не обов’язково змінить прив’язку або розміщення GPO, все ж вона може вплинути на проєктування OU [3].

Крім визначення того, які можливості та налаштування GPO будуть використані, необхідно також вирішити, як розгортати ці налаштування. При управлінні GPO необхідно відповісти на одне важливе питання: чи потрібно створити один GPO, що містить усі необхідні налаштування, або кілька окремих GPO для окремих наборів можливостей чи функцій? Взагалі, розподіл функцій між кількома GPO збільшує гнучкість, хоча й збільшує обсяг необхідного для них адміністрування. Крім того, при цьому з’являються додаткові можливості для налагодження, а також прив’язки GPO та їх фільтрації.

Як приклад розподілу функцій GPO можна розглянути структуру, що застосовується до OU філії організації. Об’єкт GPO служби технічної підтримки філії містить налаштування, що полегшують адміністраторам служби підтримки ручне виконання оновлень Windows, доступ до всіх засобів панелі керування та запуск всіх програм з необмеженим доступом. Цей GPO повинен застосовуватися останнім і перевизначати всі конфліктні параметри. Його статус слід встановити в Computer Configuration Settings Disabled, а фільтр доступу повинен

бути налаштований на використання групи доступу Branch Office Help Desk. Об’єкт GPO серверів філії може містити стандартні налаштування безпеки та програмні пакети, характерні для серверів даної філії, а також задавати спеціальні політики аудиту та налаштування управління обліковими записами. Значення статусу GPO можна встановити рівним User Configuration Settings Disabled із прив’язкою фільтру WMI для серверних ОС. Об’єкт GPO користувачів філії містить налаштування для конфігурування середовища кінцевих робочих комп’ютерів (Internet Explorer, перенаправлення папок, мережеві принтери тощо), а його статус встановлюється в Computer Configuration Settings Disabled. Нарешті, Об’єкт GPO робочих станцій філії містить налаштування безпеки, встановлення корпоративних програм і клієнтів VPN. Для нього застосовується фільтр WMI для клієнтських ОС (XP, Vista, 10, 11), а статус встановлюється в User Configuration Settings Disabled [4].

З кожним випуском клієнтської або серверної операційної системи Microsoft пропонує нові параметри та можливості групових політик. Випуски Windows 10, 11 та Windows Server 2022, 2025 не є виключенням. Лише кілька нових параметрів групових політик не застосовні до інших операційних систем, а більшість сумісні з Windows 7. Це параметри політик і рекомендовані параметри. До рекомендованих параметрів відносяться параметри управління живленням у Windows Vista та новіших операційних системах. Крім того, додано заплановані завдання та завдання, що виконуються негайно, які запускаються під час найближчого циклу оновлення групових політик.

При застосуванні параметрів групових політик, які характерні для конкретної операційної системи, рекомендується відфільтрувати всі інші операційні системи, до яких застосовується GPO. Це найкраще зробити за допомогою фільтрів WMI для комп’ютерів. Можна використовувати й фільтри доступу, але якщо застосовуються групи доступу, комп’ютер помітить під час запуску тільки групові зміни, тому застосування нової політики буде не таким успішним. Фільтр WMI обробляється всіма системами: Windows 10 та Windows Server 2012, 2016, 2022 та пізнішими версіями.

Адміністративні завдання групової політики

Після концептуального проєктування інфраструктури настає етап безпосередньої реалізації та технічного супроводу, який вимагає від адміністратора чіткого розуміння інструментарію та послідовності дій.

Для того щоб керувати груповими політиками, необхідно забезпечити наявність встановленого засобу управління груповими політиками (Group Policy Management Tools). Цей засіб встановлюється за замовчуванням на контролери доменів Windows Server 2025, однак в інших системах їх потрібно встановлювати вручну.

Для управління груповими політиками із системи Windows Server 2025 необхідно встановити компонент Group Policy Management. Процедура починається із входу в потрібну адміністративну систему, що працює під управлінням Windows Server, та відкриття через панель завдань Windows PowerShell. Далі вводиться команда Import-Module ServerManager і натискається клавіша Enter. Після цього слід ввести Add-WindowsFeature GPMC і також натиснути Enter. Завершується процес переглядом стану встановлення у вікні Windows PowerShell та закриттям вікна у разі успішного виконання операції.

У системі Windows Server 2025 зі встановленим засобом Group Policy Management Tools з'являється кілька нових командлетів PowerShell, призначених для управління груповими політиками. Для доступу до них необхідно увійти в потрібну адміністративну систему під управлінням Windows Server та відкрити з панелі завдань Windows PowerShell. У вікні PowerShell вводиться команда Import-module grouppolicy та натискається клавіша Enter для увімкнення управління груповими політиками. Після цього введення команди Get-command -module grouppolicy дозволяє отримати список із 28 доступних командлетів для роботи з груповими політиками. Для отримання довідкової інформації щодо конкретного командлета групових політик, наприклад get-gporeport, слід ввести команду Get-help get-gporeport і натиснути клавішу Enter. Щоб вивести синтаксис конкретного командлета, наприклад того ж get-gporeport, вводиться команда Get-help get-gporeport -example і натискається клавіша Enter, після чого буде виведено кілька різних прикладів [3].

Починаючи з версій Windows Server 2008 та 2012, адміністратори отримали можливість вручну створювати на контролері домену Active Directory папку, в якій містяться всі необхідні файли ADMX та ADML. Ця папка називається центральним сховищем об'єктів GPO (Central GPO Store) і допускає тільки ручне створення та управління. Її можна створити в домені, що містить контролери доменів Windows Server 2003 або новішої версії. При створенні або відкритті для редагування GPO система за замовчуванням спочатку перевіряє контролер домену на наявність центрального сховища GPO. Якщо воно існує, GPO завантажує шаблони, що зберігаються в ньому. Якщо ж воно не існує, для перегляду GPO завантажуються локальні копії файлів ADMX та ADML. Важливо зауважити, що для коректної роботи централізованого сховища необхідно модернізувати схему лісу та домену Active Directory хоча б до схеми Windows Server 2012, навіть якщо контролер домену вимагає лише Windows Server 2003 з останнім пакетом оновлень [4].

Створення центрального сховища об'єктів GPO надає адміністраторам простий, але ефективний спосіб управління адміністративними шаблонами із сервера. Для створення центрального сховища GPO необхідно увійти в потрібну адміністративну систему під Windows 8 або Windows Server 2012, відкрити папку C:\Windows\ і скопіювати в буфер обміну папку PolicyDefinitions. Далі в домені

https://www.google.com/url?sa=E&source=gmail&q=companyabc.com слід відкрити папку \\companyabc.com\sysvol\companyabc.com\policies та вставити з буфера обміну папку PolicyDefinitions у папку, зазначену в попередньому кроці. Після цього закриваються всі відкриті у вікнах папки. Описані кроки створюють центральне сховище та заповнюють його шаблонними файлами ADMX і мовними файлами ADML з адміністративної робочої станції або сервера. Якщо потрібні додаткові мовні файли, то можна скопіювати мовну підпапку з папки PolicyDefinitions адміністративної системи в центральне сховище домену, яке знаходиться тепер за адресою \\companyabc.com\sysvol\companyabc.com\policies\PolicyDefinitions.

Щоб перевірити, чи дійсно використовується центральне сховище, необхідно увійти в потрібну адміністративну систему та відкрити консоль управління груповими політиками. Далі слід розкрити домен, щоб став видимим контейнер Group Policy Objects (Об'єкти групових політик), і розкрити його. Потрібно вибрати всі наявні GPO, які містять принаймні один встановлений параметр у розділі Administrative Templates (Адміністративні шаблони) вузла Computer Configuration (Конфігурація комп'ютера) або User Configuration (Конфігурація користувача). У правій панелі здійснюється перехід на вкладку Settings (Параметри) для перегляду параметрів GPO, як показано на рисунку 5.14.

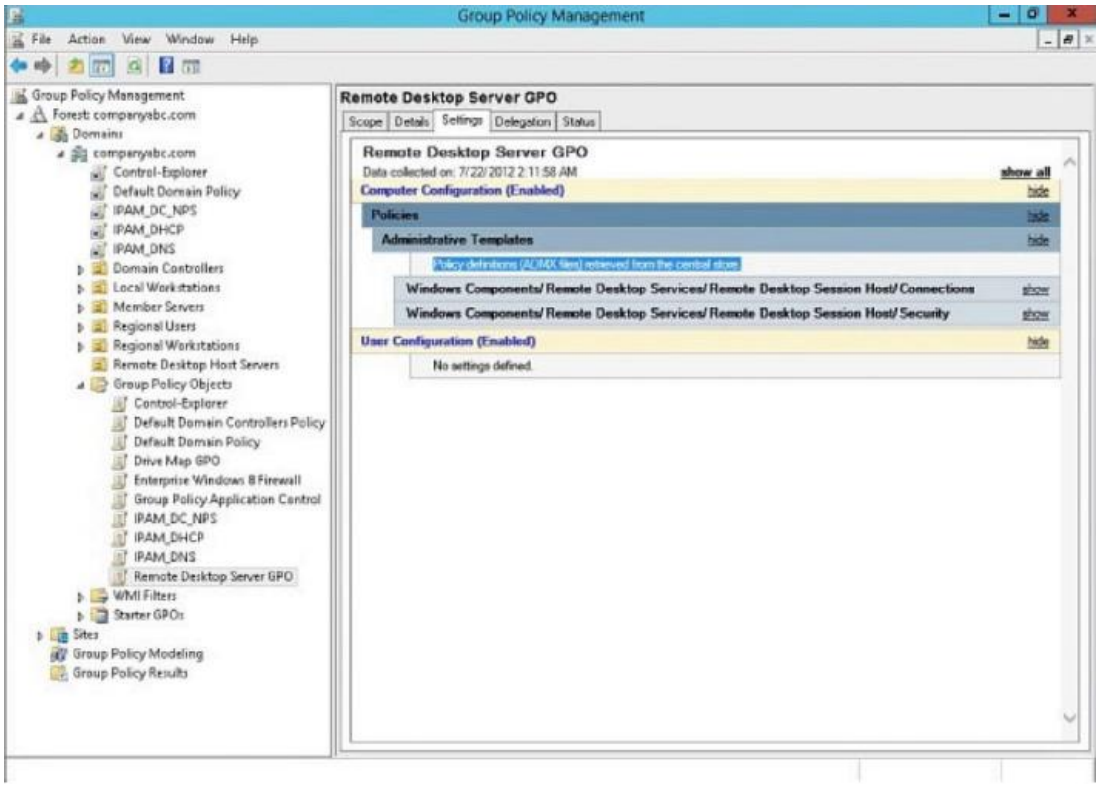

Рисунок 5.14 – Вкладка Settings для перегляду параметрів GPO [4]

Для створення нового стартового GPO за допомогою PowerShell вводиться команда New-GPStarterGPO -Name «MyStarterGPO» і натискається клавіша Enter. У вікні Windows

PowerShell з’являться результати створення нового стартового GPO. Для перевірки статусу GPO виконується команда Get-GPStarterGPO -Name MyStarterGPO, після чого вікно Windows PowerShell закривається.

Резервне копіювання та відновлення стартових об’єктів GPO є простими діями, які можна виконати за допомогою консолі GPMC з Windows Server 2025. Виконати копіювання GPO можна або окремо, або разом для всіх стартових об’єктів GPO. Починаючи з Windows Server 2008, функція резервного копіювання в GPMC дозволяє копіювати кілька версій одного і того ж GPO. У попередніх версіях, якщо потрібно було відновлювати більш ранні копії (ревізії) GPO, їх потрібно було копіювати в роздільні папки. Тепер усі резервні копії можна зберігати в одній папці.

Існує багато командлетів, що стосуються групових політик, але для роботи зі стартовими об’єктами GPO призначені лише New-GPStarterGPO та Get-GPStarterGPO, і для виконання будь-якого з них необхідно використовувати консоль GPMC. Щоб створити резервну копію всіх стартових GPO домену, необхідно увійти в потрібну адміністративну систему під управлінням Windows Server, відкрити консоль управління груповими політиками, розкрити домен і вибрати контейнер Starter GPOs (Стартові GPO). Далі слід клацнути правою кнопкою миші на стартовому GPO і вибрати в контекстному меню пункт Back Up All (Копіювати все). Потім вказується папка для зберігання резервної копії, вводиться опис цієї копії та натискається кнопка Back Up (Копіювати) для створення резервної копії стартових об’єктів GPO. Рекомендується використовувати спеціальну папку та опис резервної копії, або іншим чином розрізняти резервні копії стартових GPO та резервні копії GPO домену, хоча їх можна зберігати в тій самій папці. У вікні Backup (Копіювання) переглядається стан копіювання, а потім натискається кнопка ОК [4].

Усі стартові об’єкти GPO можна копіювати за допомогою методу, описаного в попередньому розділі – з веденням хронології версій або ревізій – а крім того, можна зберегти окремий стартовий GPO у вигляді копії або cab-файлу. Для виконання резервного копіювання одного стартового GPO слід увійти в потрібну адміністративну систему, відкрити консоль GPMC, розкрити контейнер Starter GPOs та вибрати потрібний стартовий GPO. Після клацання на ньому правою кнопкою миші в контекстному меню обирається пункт Back Up (Копіювати). Далі вказується папка для зберігання, вводиться опис та натискається кнопка Back Up. У вікні Backup переглядається стан копіювання, після чого натискається кнопка ОК.

Стартові об’єкти GPO можна експортувати або зберігати у вигляді окремих cab-файлів. Такі файли можна потім використовувати для створення нових стартових GPO або для переміщення стартових GPO з ізольованого тестового середовища Active Directory у виробниче середовище або навпаки. Щоб зберегти окремий стартовий об’єкт GPO у вигляді cab-файлу, необхідно увійти в систему, відкрити консоль GPMC, розкрити контейнер Starter

GPOs та вибрати його. У правій панелі обирається потрібний стартовий GPO і натискається кнопка Save as Cabinet (Зберегти у вигляді cab-файлу). За допомогою огляду або введення вказується місце розташування, де необхідно зберегти cab-файл, вводиться його ім'я та натискається кнопка Save (Зберегти) [4].

Відновлення стартового об'єкта GPO виконується для повернення GPO в раніше скопійований стан, переміщення GPO з одного домену або лісу в інший або для відновлення після видалення. Щоб відновити видалений стартовий GPO, слід увійти в систему, відкрити консоль GPMC, розкрити домен і вибрати контейнер Starter GPOs. Далі виконується клацання правою кнопкою миші на контейнері Starter GPO і вибирається пункт Manage Backups (Управління резервними копіями). За допомогою огляду або введення знаходиться місце розташування резервної копії GPO для завантаження набору копій. У вікні, що відкрилося, вибирається потрібний GPO. Можна відфільтрувати подання, відзначивши прапорець Show Only the Latest Version of Each Starter GPO (Показати тільки останню версію кожного стартового GPO). Щоб переглянути параметри конкретного скопійованого GPO, вибирається цей GPO і натискається кнопка View Settings (Перегляд параметрів). Після того як необхідний стартовий GPO буде знайдено, він вибирається і натискається кнопка Restore (Відновити). У діалоговому вікні Restore Confirmation (Підтвердіть відновлення) слід клацнути кнопку ОК, переглянути статус відновлення GPO, натиснути ОК і закрити вікно Manage Backups.

Якщо необхідно видалити з домену функції стартового GPO, виконується наступна процедура. Після входу в систему та відкриття GPMC перевіряється в правій панелі контейнера Starter GPOs, що функціональність стартових GPO включена. Якщо вона включена, консоль закривається. Натискається кнопка Start, у полі пошуку вводиться \\companyabc.com\sysvol\companyabc.com\ і натискається Enter (де https://www.google.com/url?sa=E&source=gmail&q=companyabc.com замінюється на реальне доменне ім'я). У вікні провідника одна з папок називається StarterGPOs. На ній слід клацнути правою кнопкою миші та видалити всю папку. Після закриття провідника та повторного відкриття GPMC, при виборі контейнера Starter GPO у правій панелі повинна відображатися кнопка Create Starter GPO Folder (Створити папку Starter GPO), що свідчить про відключення функціональності. Видалення функціональності стартових об'єктів GPO не впливає на жодні групові політики домену, які були створені раніше за допомогою будь-яких стартових об'єктів GPO [4].

Щоб створити нові групові політики домену, необхідно увійти у відповідну систему та відкрити Windows PowerShell. У вікні PowerShell вводиться команда import-module GroupPolicy та натискається клавіша Enter. Далі вводиться команда New-GPO -Name MyNewGPO і натискається клавіша Enter.

Наступним кроком після створення та налаштування об'єктів GPO повинна бути їх

прив’язка до необхідних контейнерів Active Directory. Для прив’язки наявного об’єкта GPO до контейнера Active Directory потрібно увійти в систему, відкрити Windows PowerShell і ввести команду import-module GroupPolicy. У даному прикладі виконується прив’язка об’єкта GPO з іменем MyNewGPO до організаційної одиниці Local Workstations, яка знаходиться в корені домену https://www.google.com/url?sa=E&source=gmail&q=companyabc.com. Для цього вводиться команда New-GPLink -Name «MyNewGPO» -Target «OU=Local Workstations, DC=companyabc, DC=Com» і натискається Enter. При успішному виконанні команди у вікні PowerShell з’явиться результат, після чого вікно можна закрити.

За замовчуванням зв’язок GPO після створення активний. У кожного зв’язку є свої параметри налаштування: примусове застосування та можливість включення і відключення зв’язку. Щоб змінити стандартні налаштування зв’язку GPO, слід відкрити консоль GPMC, розкрити вузол Domains or Sites (Домени або сайти), щоб став видимим контейнер, до якого прив’язаний GPO. Якщо потрібно виконати примусове застосування GPO, необхідно клацнути правою кнопкою миші на потрібному зв’язку GPO і вибрати в контекстному меню пункт Enforced (Застосовувати). Якщо стан зв’язку GPO потрібно змінити з «включено» на «виключено», клацається правою кнопкою миші на потрібному зв’язку GPO і обирається пункт Link Enabled (Зв’язок активний), щоб включити (Enabled) або виключити (Disabled) даний зв’язок.

Статус GPO визначає, включений або відключений весь об’єкт GPO або один з його вузлів. Статус GPO – це характеристика самого об’єкта GPO, тому будь-які його зміни впливають на всі зв’язки. Щоб переглянути або змінити статус GPO, необхідно відкрити GPMC, розкрити контейнер Group Policy Objects, вибрати потрібний GPO і перейти на вкладку Details (Інформація) у правій панелі. У списку GPO Status (Статус GPO) на вкладці Details можна переглянути поточний статус. Якщо цей статус потрібно змінити, у списку обирається один із варіантів: Enabled (Включений), User Configuration Settings Disabled (Параметри конфігурації користувача відключені), Computer Configuration Settings Disabled (Параметри конфігурації комп’ютера відключені) або All Settings Disabled (Всі параметри відключені). Після вибору потрібного статусу відкриється вікно з вимогою підтвердження, де слід натиснути ОК [4].

Управління фільтрами доступу є одним із найкращих способів вказати конкретну групу користувачів і комп’ютерів для застосування об’єкта GPO. Фільтри доступу можна задати для конкретного користувача, комп’ютера, об’кта групи доступу або комбінації всіх цих трьох типів. Щоб змінити фільтр доступу GPO зі стандартного значення Authenticated Users (Аутентифіковані користувачі), слід відкрити GPMC, вибрати потрібний GPO і перейти на вкладку Scope (Область). У розділі Security Filtering (Фільтр доступу) вибирається група Authenticated Users і натискається кнопка Remove (Видалити), після чого дія підтверджується

натисканням ОК. У тому ж розділі Security Filtering натискається кнопка Add (Додати), вводиться ім'я користувача або групи доступу та натискається ОК. Якщо необхідно додати конкретний об'єкт комп'ютера, натискається кнопка Object Types (Типи об'єктів), відзначається об'єкт Computers (Комп'ютери), натискається ОК, вводиться ім'я об'єкта комп'ютера та знову натискається ОК.

Якщо застосування до об'єкта GPO фільтра доступу не дає необхідної деталізації для вказівки потрібного набору комп'ютерів, до цього GPO можна прив'язати фільтр WMI. У даному прикладі створюється фільтр WMI для виділення комп'ютерів. Для цього слід відкрити GPMC, розкрити домен і вибрати контейнер WMI Filters (Фільтри WMI). Після клацання правою кнопкою миші на цьому контейнері вибирається пункт New (Створити). У полі Name (Ім'я) вводиться «Windows 8 WMI Filter», а в полі Description (Опис) – «WMI filter to include only Windows workstations». Далі натискається кнопка Add (Додати) для створення запиту фільтра WMI. У полі Query (Запит) вводиться Select * from Win32_OperatingSystem where (Name LIKE «%Windows 8%»). Отримана інформація повинна бути схожа на наведену на рисунку 5.15.

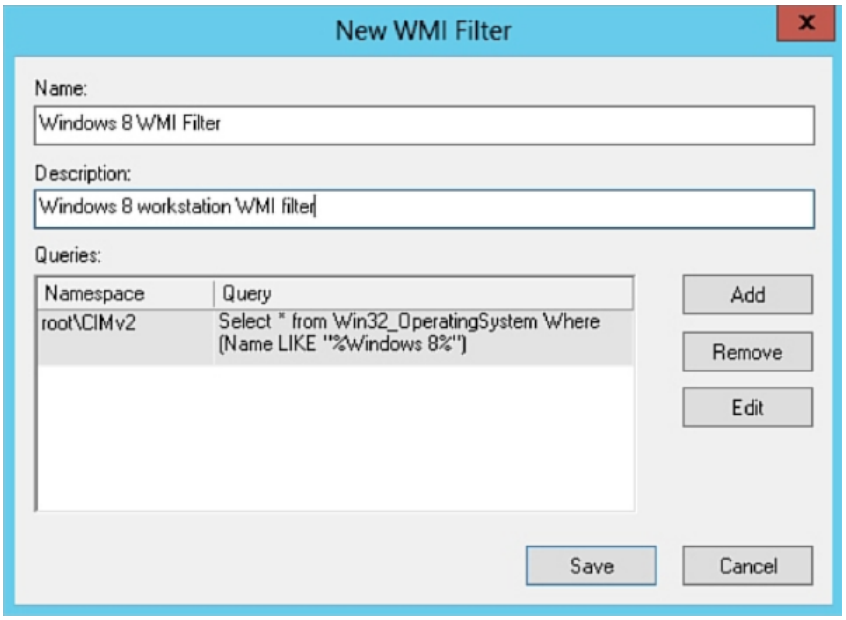

Рисунок 5.15 – Створення фільтра групової політики WMI у Windows [4]

Після введення запиту натискається кнопка ОК, щоб зберегти запит і повернутися у вікно WMI Filters, а потім натискається кнопка Save (Зберегти) для створення фільтра WMI в домені.

Якщо до контейнера Active Directory прив'язано кілька об'єктів GPO, то вони повинні оброблятися в певному порядку. У багатьох випадках набір прив'язаних GPO містить параметри, що конфліктують один з одним, і для отримання потрібного результату потрібно змінити порядок обробки GPO. При перегляді списку зв'язків об'єктів групових політик

групові політики застосовуються у зворотному порядку, тобто останньою застосовується політика з номером 1. Порядок прив'язки групових політик успадковується від будь-яких батьків або контейнерів домену, і його можна змінити лише в тому домені або контейнері, з яким пов'язаний GPO.

Щоб змінити порядок обробки зв'язків GPO, необхідно відкрити GPMC, розкрити вузол Domains (Домени) або Sites (Сайти) та вибрати необхідний контейнер з кількома прив'язаними GPO. У правій панелі здійснюється перехід на вкладку Linked Group Policy Objects (Прив'язані об'єкти групових політик).

Варто зауважити, що якщо вказано порядок обробки, то спочатку застосовується політика з найбільшим номером, а потім інші політики в порядку спадання їх номерів. Об'єкт GPO з номером 1 у списку обробляється останнім. Якщо розміщення або порядок будь-якого GPO потрібно змінити, вибирається цей GPO і натискається одна з розташованих зліва кнопок: Move Link to Top (Перемістити зв'язок наверх – подвійна стрілка вгору), Move Link Up (Перемістити зв'язок вище – одиночна стрілка вгору), Move Link Down (Перемістити зв'язок нижче – одиночна стрілка вниз) або Move Link to Bottom (Перемістити зв'язок вниз – подвійна стрілка вниз). Коли зв'язки GPO опиняться в необхідному порядку, завдання вважається завершеним.

Однією з важливих функцій консолі управління груповими політиками (GPMC) є можливість перегляду параметрів об'єктів групової політики (GPO) та їх збереження у вигляді HTML-файлів для подальшого спільного використання. Для перегляду параметрів певного GPO адміністратору необхідно увійти в систему під управлінням Windows Server, відкрити консоль GPMC та розкрити ліс або домен до рівня контейнера Group Policy Objects. Після вибору необхідного GPO у правій панелі здійснюється перехід на вкладку Settings (Параметри). Перегляд параметрів відбувається шляхом розкриття розділів за допомогою гіперпосилань Hide (Приховати) та Show (Показати). Для експорту параметрів у файл формату XML або HTML необхідно клацнути правою кнопкою миші на обраному GPO у лівій панелі та вибрати пункт Save Report (Зберегти звіт). У діалоговому вікні вказується місце збереження звіту та формат файлу, після чого натискається кнопка Save (Зберегти) [4].

Резервне копіювання об'єктів групової політики є критично важливим завданням, яке повинно виконуватися на регулярній основі. Для створення резервної копії всіх GPO домену використовується засіб Windows PowerShell в адміністративній системі зі встановленим інструментарієм Group Policy Management Tools. Процес починається з введення команди Import-Module GroupPolicy. Після цього виконується команда Backup-GPO -Path C:\GPOBackup -All, яка ініціює копіювання всіх об'єктів у папку C:\GPOBackup локальної системи. Важливою умовою є попереднє існування вказаного шляху до папки, інакше виконання завдання завершиться помилкою. У випадку, коли необхідно скопіювати лише

один конкретний GPO, після імпорту модуля вводиться команда Backup-GPO -Path C:\GPOBackup -Name MyNewGPO, де MyNewGPO – ім’я цільового об’єкта [4].

Відновлення GPO домену здійснюється для повернення об’єкта до стану, зафіксованого перед копіюванням, або для відновлення після видалення. Процедура відновлення видалених GPO починається з входу в адміністративну систему та відкриття GPMC. У консолі необхідно розкрити ліс і домен, знайти контейнер Group Policy Objects, клацнути на ньому правою кнопкою миші та обрати пункт Manage Backups (Управління копіями). Далі вказується розташування резервних копій, обирається потрібний об’єкт GPO (можливе використання фільтра Show Only the Latest Version of Each Starter GPO для відображення лише останніх версій). Перед відновленням можна переглянути параметри, натиснувши кнопку View Settings. Після вибору необхідного об’єкта натискається кнопка Restore (Відновити), дія підтверджується у діалоговому вікні, і після завершення процесу переглядається статус операції. Важливо зазначити, що відновлення GPO з резервної копії не відновлює зв’язки цих об’єктів. Зв’язки доведеться створювати та налаштовувати заново вручну, використовуючи інформацію зі звіту параметрів копії GPO [4].

Для заміни існуючого GPO домену на версію з резервної копії процедура дещо відрізняється. У консолі GPMC обирається потрібний GPO, на ньому виконується клацання правою кнопкою миші та обирається пункт Restore from Backup (Відновити з копії). Запускається майстер відновлення (Restore Group Policy Object Wizard), де після привітальної сторінки вказується шлях до резервної копії. Після вибору конкретної копії та перегляду її параметрів натискається кнопка Next, перевіряється зведення параметрів і натискається кнопка Finish для запуску процесу. Завершується операція переглядом статусу відновлення.

У GPMC наявна функція Group Policy Modeling (Моделювання групових політик), яка дозволяє адміністраторам виконувати тестування для визначення результатів обробки GPO за різних умов: застосування нових політик, зміна статусу GPO, переміщення об’єкта комп’ютера або користувача, а також зміна членства у групах. Цей інструментарій дозволяє прогнозувати вплив змін на інфраструктуру без безпосереднього втручання в робоче середовище. Детальний розгляд цієї функції винесено в окремий розділ курсу.

Ефективне адміністрування вимагає навичок отримання звітів та усунення несправностей. Якщо групові політики обробляються не так, як було заплановано, може знадобитися увімкнення запису в журнал (логування) для виявлення причин проблем. За замовчуванням фіксація попереджень та помилок увімкнена для всіх розширень на стороні клієнта. Зміна параметрів журналювання рекомендується лише тоді, коли інформації у стандартних журналах подій недостатньо. Наприклад, для діагностики проблем із розширенням GPP Drive Maps (Відображення дисків) можна змінити параметри запису в журнал саме для цього розширення. Процес передбачає створення нового GPO (наприклад,

GPOLogSettings), перехід до вузла Computer Configuration \ Administrative Templates \ System \ Group Policy \ Logging and tracing [3].

На сторінці налаштувань необхідно відкрити параметр Configure Drive Maps Preference Logging and Tracing, обрати Enabled, а у списку Tracing встановити значення On. У полі User Trace Form слід запам’ятати шлях до файлу трасування. Після збереження параметрів GPO прив’язується до відповідної організаційної одиниці (OU), і виконується примусове оновлення політик через GPMC (пункт Group Policy Update). Оскільки розширення Drive Maps є налаштуванням користувача, для оновлення обробки необхідно вийти та повторно увійти в систему. Результати трасування можна переглянути у файлі, що зазвичай знаходиться за шляхом %COMMONAPPDATA%\GroupPolicy\Preference\Trace\User.log. Слід пам’ятати, що якщо GPO не застосовується (наприклад, через фільтри безпеки), файл трасування створено не буде.

Для перевірки фактичної обробки політик на конкретній системі або для певного користувача використовується інструмент Group Policy Results (Результуючий набір політик — RSoP). У консолі GPMC для Windows Server цей інструмент має розширені можливості звітування. Запуск майстра здійснюється через контекстне меню контейнера Group Policy Results (Мастер результатів групових політик). На етапах роботи майстра обирається цільовий комп’ютер (поточний або інший) та користувач, що входив у цю систему. Після завершення збору даних результати відображаються у вікні GPMC на вкладках Summary (Зведення), Details (Детально) та Policy Events (Події політики), що дозволяє комплексно проаналізувати застосування політик.

Адміністративне делегування GPO являє собою процес надання прав окремим користувачам або налаштування прав доступу для управління GPO у межах контейнерів Active Directory (сайтів, доменів, OU). Ця практика доцільна в організаціях із розділеними IT-групами (окремо для інфраструктури, серверів, робочих станцій). Делегування прав на створення GPO можливе лише в контейнерах Group Policy Objects та Starter GPOs. Для цього в GPMC обирається відповідний контейнер, здійснюється перехід на вкладку Delegation (Делегування), де через кнопку Add додається обліковий запис користувача або групи. Альтернативним методом є додавання користувача до групи Group Policy Creator Owners [3].

Щодо делегування прав на управління існуючими GPO, то за замовчуванням повні права мають адміністратори домену та підприємства, а також творці політики. Для надання прав редагування або управління безпекою іншим особам, необхідно обрати конкретний GPO, перейти на вкладку Delegation і додати користувача чи групу. У списку Permissions (Права доступу) можна обрати рівень повноважень: Read (Читання), Edit Settings (Редагування параметрів) або Edit Settings, Delete, Modify Security (Редагування, видалення,

зміна безпеки).

Консоль GPMC також дозволяє делегувати адміністративні завдання контейнерам Active Directory, такі як управління зв'язками GPO. Для цього обирається потрібний домен, сайт або OU, і на вкладці Delegation додається користувач із наданням специфічних прав: Link GPOs (Прив'язка GPO), Perform Group Policy Modeling Analyses (Виконання аналізу моделювання) або Read Group Policy Results Data (Читання результатів). При налаштуванні прав можна вказати область дії: тільки цей контейнер або контейнер із усіма дочірніми елементами [3].

Варто зауважити, що для виконання моделювання групових політик користувач, якщо він не працює на контролері домену, повинен бути членом групи Distributed COM Users домену.

Тема 6
Служба DNS

Поняття системи доменних імен DNS

Система доменних імен (DNS) виникла з проєкту ARPANET у 1960-х роках, вирішуючи потребу у зручному для користувача способі ідентифікації мережевих пристроїв, що виходить за межі числових IP-адрес. Ця концепція еволюціонувала в DNS у тому вигляді, в якому вона відома сьогодні, на початку 1980-х років із випуском фундаментальних специфікацій, задокументованих у запитах на коментарі (RFC). DNS організована в ієрархічну структуру, подібну до дерева, де коренева зона розгалужується на різні домени та піддомени, кожен з яких містить записи ресурсів, що надають важливу інформацію про мережеві ресурси [3].

Доменне ім’я конструюється з декількох сегментів, відомих як мітки, що розділені крапками – наприклад, packtpub.com. Ця система спирається на розподілену базу даних, що використовує архітектуру клієнт-сервер, де мережеві хости виступають у ролі серверів імен. Ці сервери відповідають за перетворення (розв’язання) доменних імен у відповідні IP-адреси, забезпечуючи безперебійну навігацію та з’єднання в інтернеті. Такий ієрархічний і розподілений підхід підвищує масштабованість, ефективність та надійність управління доменними іменами та мережевими ресурсами [3].

Для повного розуміння того, як функціонує DNS, доцільно простежити послідовність кроків, що відбуваються під час спроби доступу до вебсайту. DNS є необхідною для трансляції зручних для людини доменних імен у машинозчитувані IP-адреси, полегшуючи комунікацію між користувачами та вебсайтами. Процес розв’язання імен DNS, що описує механізм пошуку браузером коректної IP-адреси для з’єднання при введенні веб-адреси, такої як www.packtpub.com, складається з кількох етапів.

Процедура ініціюється введенням URL-адреси: коли адреса www.packtpub.com вводиться в адресний рядок браузера і натискається клавіша Enter, браузер надсилає запит на з’єднання з цим доменом. Цей запит спершу надходить до критично важливого компонента інфраструктури DNS, відомого як рекурсивний перетворювач (резолвер). Зазвичай керований інтернет-провайдером (ISP), цей резолвер відповідає за обробку запитів від імені клієнта. Далі рекурсивний резолвер комунікує з глобальними кореневими серверами, які зберігають інформацію про домени верхнього рівня (TLD), такі як .com. Ці сервери не володіють повною інформацією DNS, проте вони спрямовують резолвер до відповідних серверів TLD.

Сервери TLD, у свою чергу, відповідають наданням інформації, що спрямовує резолвер до авторитетних серверів імен для конкретного домену, наприклад, packtpub.com. Після цього резолвер опитує ці авторитетні сервери імен для знаходження точної IP-адреси, асоційованої з packtpub.com. Авторитетні сервери містять фактичні записи DNS, що

зіставляють доменні імена з IP-адресами. Як тільки резолвер отримує IP-адресу вебсервера, що хостить packtpub.com, він передає цю інформацію назад у браузер. Маючи IP-адресу, браузер може встановити з'єднання з вебсервером і отримати контент вебсайту для перегляду [3].

Цей поетапний процес ілюструє складні механізми роботи DNS, підкреслюючи її роль у перетворенні доменних імен в IP-адреси, що уможливлюють безперебійну комунікацію в інтернеті. Розуміння цього процесу підкреслює важливість правильного налаштування ролі DNS у мережі. Виконуючи це, забезпечується ефективне розв'язання доменних імен, що є критично важливим як для операцій внутрішньої мережі, так і для зовнішнього доступу до інтернету.

Структура простору імен

Структура системи доменних імен (DNS) нерозривно пов'язана з архітектурою мережі Інтернет, через що ці поняття часто ототожнюються. Така структура зарекомендувала себе як надзвичайно зручна, а той факт, що вона продовжує користуватися популярністю протягом тривалого часу, лише підтверджує її функціональність та надійність. Для формування більш широкого уявлення про те, яким чином служба DNS інтегрується в середовище Windows Server, необхідне детальне вивчення компонентів, з яких складається DNS, а також засобів їх об'єднання в єдину логічну структуру.

Обмежена область, що визначається іменем DNS, класифікується як простір імен DNS. Прикладами таких просторів можуть слугувати домени microsoft.com або marketing.companyabc.com. Простори імен поділяються на загальнодоступні (публічні) та внутрішні. Загальнодоступні простори імен публікуються в мережі Інтернет і функціонування їх залежить від дотримання низки стандартів. Усі простори імен доменів верхнього рівня, таких як .com, .net, .org тощо, є зовнішніми або загальнодоступними. Стосовно внутрішніх просторів імен, слід зазначити, що вони не публікуються в Інтернеті, а отже, не обмежуються жорсткими правилами реєстрації. Тобто внутрішній, не опублікований простір імен може мати будь-який вигляд, наприклад dnsname.local або companyabc.internal. Найчастіше внутрішні простори імен використовуються в службах Active Directory, оскільки це підвищує рівень безпеки середовища. Враховуючи, що такі простори імен не публікуються, пряме звернення до них із мережі Інтернет є неможливим [3].

У контексті концепції просторів імен DNS, простір імен являє собою обмежену логічну область, що утворюється іменем DNS та його піддоменами. Наприклад, імена europe.companyabc.com, asia.companyabc.com та companyabc.com розглядаються як частини одного й того ж безперервного простору імен DNS. Простір імен DNS у доменних службах Active Directory (AD DS) може бути опублікований в Інтернеті (на кшталт microsoft.com або

msn.com) або ж прихований від зовнішнього доступу, що залежить від обраної стратегії та вимог безпеки, які реалізуються адміністраторами системи.

Зовнішні (опубліковані) простори імен визначаються як імена DNS, що розпізнаються з будь-якої точки мережі Інтернет. Подібні простори імен раніше часто застосовувалися в організаціях, які з метою уніфікації прагнули, щоб їхнє доменне ім'я, яке зазвичай використовується в Інтернеті, представляло також і структуру AD DS. Однак практика демонструє, що така модель є недостатньо зручною та безпечною. Оскільки питання безпеки відіграють дедалі важливішу роль, систему DNS рекомендується встановлювати як окремий компонент: наявність внутрішніх зон AD DNS із можливістю доступу до них із мережі Інтернет не рекомендується [3].

Внутрішні (приховані) простори імен використовуються організаціями, для яких публікація внутрішньої доменної структури є неприпустимою з точки зору інформаційної безпеки. Такі організації можуть визначати схеми AD DS із внутрішнім простором імен, який не доступний для читання із зовнішньої мережі. Наприклад, компанія може володіти зовнішнім простором імен DNS cco.com, тоді як структура AD DS відповідатиме простору імен cco.internal або іншому подібному. Для внутрішніх просторів імен допускається будь-яка комбінація, адже в них відсутні обмеження на використання доменів .com, .net, .gov тощо. За потреби домен можна назвати навіть довільним чином, наприклад ilovemydomain.verymuch (хоча такий підхід не є рекомендованим). З практичних міркувань для приватної адресації спеціально зарезервовано простір імен .internal, використання якого у багатьох випадках є доцільним та зручним [3].

Слід звернути увагу на важливий аспект уникнення конфліктів імен. Якщо приймається рішення використовувати простір доменних імен, який теоретично може бути – на даний момент або в майбутньому – придбаний та застосований в Інтернеті, то для уникнення можливих колізій при перетворенні (розворот) імен рекомендується одразу набути права на це доменне ім'я. Наприклад, при виборі в якості внутрішнього простору імен companyabc.com доцільно перевірити його доступність і, за можливості, зареєструвати його. Якщо виявиться, що цим ім'ям домену вже володіє інша організація, рекомендується обрати для простору імен своєї AD DS інше доменне ім'я. Навіть якщо домен не публікується в Інтернеті, у користувачів домашніх або портативних комп'ютерів, яким потрібен доступ до домену через комутоване з'єднання або мережу VPN, можуть виникати конфлікти через помилкове спрямування запитів у простір імен DNS в Інтернеті, а не в локальний простір імен компанії.

Встановлення та налаштування служби DNS у Windows Server

В операційній системі Windows Server 2025 роль DNS є важливою для забезпечення

можливості трансляції доменних імен в IP-адреси, що сприяє безперебійній мережевій комунікації та доступу до ресурсів. Конфігурація цієї ролі може бути здійснена за допомогою інструменту Server Manager («Диспетчер серверів»). Як зображено на рисунку 6.1, процес розпочинається з доступу до Server Manager та вибору опції додавання ролей і компонентів.

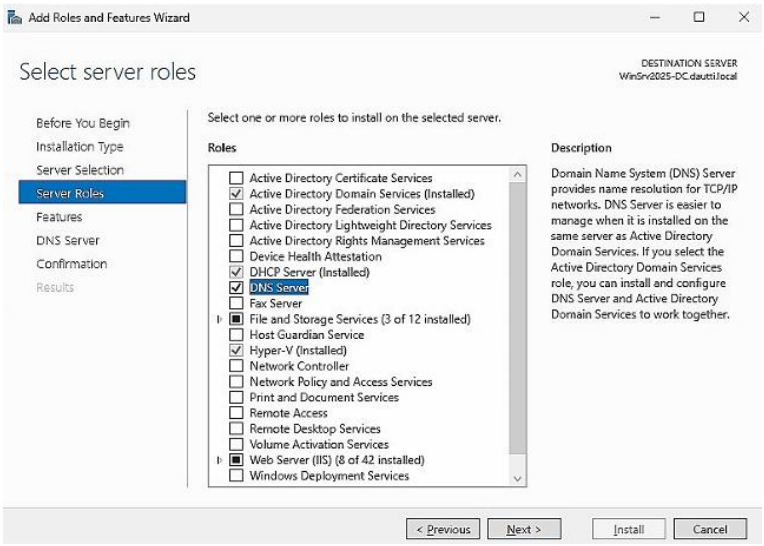

Рисунок 6.1 – Встановлення ролі DNS [3]

Встановлення ролі DNS може бути виконане як у вигляді незалежної служби, так і у поєднанні з доменними службами Active Directory (AD DS). У випадку окремого встановлення роль DNS функціонує автономно для обробки запитів на розв'язання доменних імен. Однак інтеграція DNS з AD DS, значно розширює загальну функціональність мережі, дозволяючи серверу DNS підтримувати операції Active Directory, такі як визначення розташування контролерів домену (DC) та пошук записів служб (рис. 6.2). Така інтеграція є особливо корисною для управління масштабними мережами, де AD та DNS взаємодіють для оптимізації операцій [29].

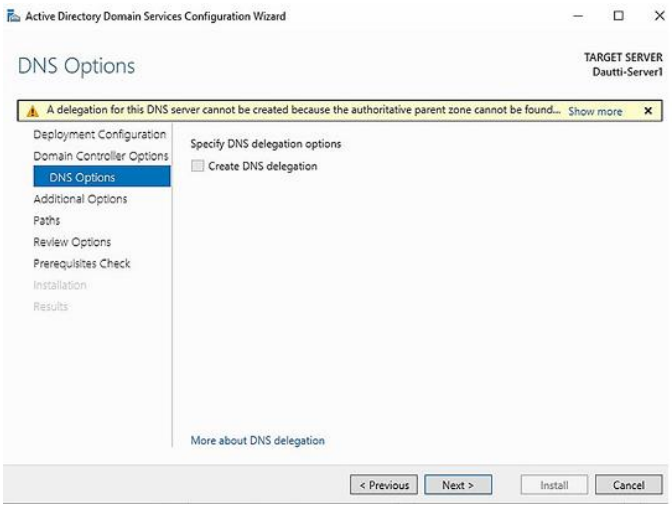

Рисунок 6.2 – Додавання DNS разом з AD DS [3]

Більше того, роль DNS часто включається як складова частина процесу встановлення AD DS, забезпечуючи цілісне налаштування, що підтримує розв'язання доменних імен у середовищі Active Directory. Такий підхід гарантує належну конфігурацію служб DNS для забезпечення потреб AD, включаючи автоматичне створення необхідних DNS-записів. Після успішного встановлення та налаштування ролі DNS з'являється можливість керувати розв'язанням доменних імен та підвищувати функціональність мережі.

Після інсталяції виконується подальша конфігурація сервера. Насамперед, здійснюється налаштування мережевих інтерфейсів. За замовчуванням сервер DNS прослуховує запити на всіх інтерфейсах IP-адрес. Існує можливість налаштувати сервер DNS на прослуховування лише визначеного інтерфейсу, використовуючи графічний інтерфейс користувача (GUI) або засоби PowerShell [29].

Для налаштування інтерфейсу, що використовується для прослуховування DNS-запитів через консоль DNS Manager, необхідно виконати наступні дії: у меню «Пуск» (Start) обирається пункт «Засоби адміністрування Windows» (Windows Administrative Tools), а потім – DNS. Далі обирається потрібний сервер, на якому (через утримання натискання або клік правою кнопкою миші) викликається контекстне меню та обирається пункт «Властивості» (Properties). Щоб обмежити сервер DNS використанням конкретної IP-адреси, вибирається опція «Лише вказані IP-адреси» (Only the following IP address), зазначається необхідна адреса, після чого натискається кнопка OK [3].

Наступним етапом є конфігурація кореневих посилань. Сервери кореневих посилань використовуються для допомоги у розв'язанні адресної інформації DNS у випадках, коли сервер DNS не в змозі розв'язати запит локально за допомогою розміщеної зони або кешу сервера. Сервери імен кореневих посилань заповнюються за замовчуванням під час нових інсталяцій. За необхідності список кореневих серверів імен можна редагувати, перейшовши на вкладку «Кореневі посилання» у діалоговому вікні властивостей сервера DNS або використовуючи PowerShell.

Важливо зазначити, що видалення всіх серверів кореневих посилань не підтримується. Замість цього сервер DNS налаштовується на відмову від використання серверів кореневих посилань шляхом вибору опції «Вимкнути рекурсію» (Disable recursion) на вкладці «Додатково» (Advanced) консолі DNS Manager. Вимкнення рекурсії також деактивує будь-які налаштовані сервери пересилання. Альтернативно, можна зняти позначку з пункту «Використовувати кореневі посилання, якщо сервери пересилання недоступні» (Use root hints if no forwarders are available) на вкладці «Сервери пересилання» (Forwarders).

Процедура редагування кореневих посилань через консоль DNS Manager виглядає наступним чином: відкривається консоль DNS, у властивостях сервера обирається вкладка «Кореневі посилання» (Root Hints), виділяється елемент для редагування та натискається

кнопка «Змінити» (Edit). Далі вводиться повне доменне ім’я (FQDN) та натискається «Розв’язати» (Resolve). Після перевірки та, за необхідності, редагування IP-адреси натискається OK. Після перегляду оновленого списку серверів кореневих посилань підтверджується завершення операції натисканням OK. Варто звернути увагу, що ім’я сервера має завершуватися крапкою.

Також передбачена можливість налаштування серверів пересилання. Сервер пересилання конфігурується опціонально для розв’язання адресної інформації DNS замість пересилання трафіку до кореневих серверів DNS. Додавання серверів пересилання здійснюється через GUI або за допомогою командлета PowerShell Set-DNSServerForwarder. Слід зауважити, що кореневі посилання DNS не використовуються, доки сервери пересилання відповідають на запити. Для налаштування серверів пересилання через консоль DNS Manager у властивостях сервера обирається вкладка «Сервери пересилання» (Forwarders) та натискається кнопка «Змінити» (Edit). Вводиться IP-адреса DNS-сервера, до якого будуть пересилатися запити. Цей крок повторюється необхідну кількість разів. Після натискання OK та перегляду списку серверів DNS конфігурація завершується натисканням кнопок OK або «Застосувати» (Apply).

Створення зон і записів

У контексті адміністрування служби DNS ключовим етапом є створення зон, які виступають логічними контейнерами для зберігання записів ресурсів. Основна зона (Primary Zone) містить головну копію даних, доступну для читання та запису. У середовищі Windows Server існує два механізми зберігання даних основної зони: інтеграція з Active Directory (AD) та файлове зберігання.

Інтеграція зон DNS із Active Directory забезпечує низку переваг, зокрема використання механізмів мульти-майстерної реплікації, посилену безпеку та спрощене адміністрування. Для створення такої зони використовується консоль управління DNS (DNS Manager) або засоби автоматизації PowerShell. Процедура створення через графічний інтерфейс передбачає виконання наступних кроків.

У консолі DNS Manager здійснюється підключення до цільового сервера, після чого у контекстному меню обирається пункт «New Zone» (Нова зона), що ініціює запуск «Майстра створення нових зон» (New Zone Wizard) (рис. 6.3). На етапі вибору типу зони (Zone Type) необхідно обрати «Primary zone» (Основна зона) та переконатися, що активовано опцію «Store the zone in Active Directory» (Зберігати зону в Active Directory). Слід зазначити, що дана опція доступна виключно у випадку, коли сервер DNS функціонує як контролер домену AD DS [3].

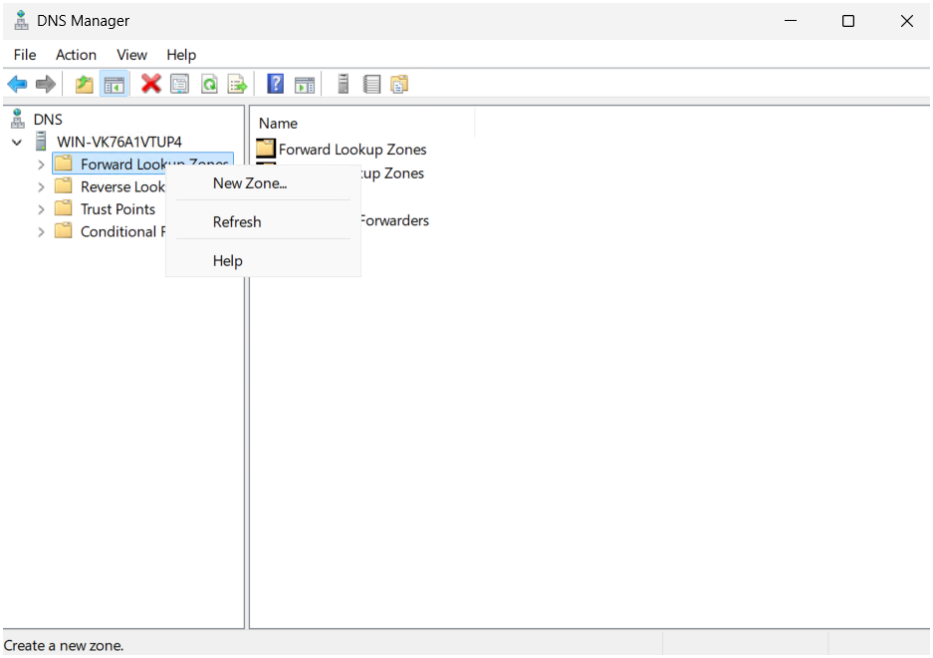

Рисунок 6.3 – Початок створення прямої зони DNS [3]

Критично важливим етапом є визначення області реплікації зони (Active Directory Zone Replication Scope). Адміністратору пропонуються наступні варіанти розповсюдження даних:

– Усі сервери DNS, що працюють на контролерах домену в даному лісі.
– Усі сервери DNS, що працюють на контролерах домену в даному домені.
– Усі контролери домену в даному домені (опція для сумісності з Windows 2000).
– Усі контролери домену, включені до специфічного розділу каталогу.

Далі визначається тип перегляду: зона прямого перегляду (Forward lookup zone) для перетворення імен в IP-адреси або зона зворотного перегляду. Після введення імені зони (наприклад, north.contoso.com) налаштовується режим динамічних оновлень (Dynamic Update). Для інтегрованих зон Active Directory рекомендується вибір опції «Allow only secure dynamic updates» (Дозволяти тільки безпечні динамічні оновлення), що гарантує автентифікацію комп'ютерів перед внесенням змін до записів. Інші варіанти включають дозвіл будь-яких оновлень (що знижує рівень безпеки) або повну заборону динамічних оновлень [30].

У сценаріях, де інтеграція з AD неможлива або недоцільна, створюється стандартна основна зона, дані якої зберігаються у текстовому файлі. Процес створення аналогічний попередньому, проте на етапі вибору типу зони опція «Store the zone in Active Directory» має бути деактивованою (знятою).

При конфігуруванні такої зони системі необхідно вказати ім'я файлу зони. За замовчуванням пропонується створити новий файл з іменем зони та розширенням .dns (наприклад, east.contoso.com.dns), який буде розміщено у системній директорії

%SystemRoot%\system32\dns. Також існує можливість імпорту існуючого файлу зони, попередньо скопійованого у зазначену директорію. Важливою відмінністю від інтегрованих зон є налаштування динамічних оновлень: опція безпечних оновлень (Secure dynamic updates) у даному випадку недоступна, тому вибір обмежується дозволом небезпечних і безпечних оновлень або їх забороною. Завершується процедура натисканням кнопки «Finish» [3].

Вторинна зона (Secondary Zone) являє собою копію основної зони, доступну лише для читання. Вона використовується для розподілу навантаження, забезпечення відмовостійкості та зменшення трафіку запитів у глобальній мережі [3].

Для створення вторинної зони у «Майстрі створення нових зон» обирається тип «Secondary zone». На етапі іменування необхідно вказати ім’я, яке точно відповідає імені основної зони, з якої буде здійснюватися реплікація (наприклад, south.contoso.com). Ключовим налаштуванням є визначення головних DNS-серверів (Master DNS Servers) [3].

У відповідному діалоговому вікні вводяться IP-адреси одного або декількох серверів, що містять копію основної зони (рис. 6.4). Необхідною умовою успішного розгортання вторинної зони є налаштування дозволу на передачу зон (Zone Transfer) на стороні основного сервера для IP-адреси вторинного сервера. Після валідації введених адрес процес завершується натисканням кнопки «Finish».

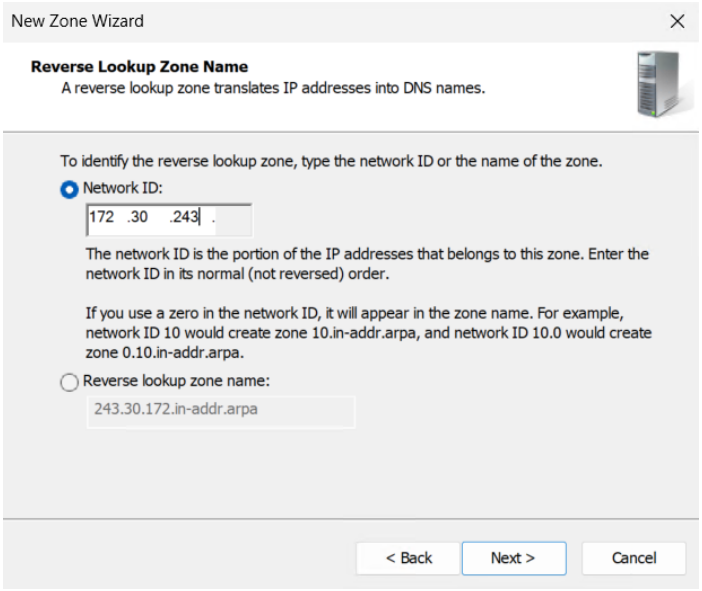

Рисунок 6.4 – Надання ідентифікатора мережі для вторинної зони DNS [3]

Делегування зон є фундаментальним механізмом ієрархічної структури DNS, що дозволяє передати відповідальність за частину простору імен (піддомен) іншому DNS-серверу. Це забезпечує децентралізацію управління та підвищення ефективності розв’язання імен.

Процедура делегування виконується через консоль DNS Manager шляхом вибору

батьківської зони та активації пункту «New Delegation» (Нове делегування) у контекстному меню. У діалоговому вікні «Delegated Domain Name» вводиться ім’я делегованого піддомену (наприклад, для south.west.contoso.com вводиться south), при цьому повне доменне ім’я (FQDN) формується автоматично.

Наступним кроком є визначення серверів імен, які будуть авторитетними для делегованої зони. Необхідно натиснути кнопку «Add» та вказати FQDN або IP-адресу відповідного DNS-сервера. Система автоматично намагається розв’язати введене ім’я в IP-адресу (Resolve). Після успішної валідації та додавання необхідної кількості серверів натискається кнопка «OK» та «Finish» для завершення роботи майстра. У результаті в батьківській зоні створюються записи NS (Name Server), які вказують на сервери, що обслуговують делегований піддомен, а також, за необхідності, записи прив’язки (Glue records) [3].

В основі функціонування системи доменних імен лежать записи ресурсів (Resource Records – RR), які слугують фундаментальними ідентифікаторами об’єктів у мережі. Кожен такий запис є унікальним у межах свого домену і використовується для виконання пошукових запитів, пов’язуючи зрозумілі імена з технічними ресурсами. Враховуючи розподілену природу та ієрархічність DNS, ідентичні записи можуть існувати на різних рівнях структури, проте в конкретній зоні вони виконують чітко визначену роль. У більшості сучасних реалізацій, зокрема інтегрованих зі службами Active Directory в Windows Server, адміністраторам доводиться працювати зі спеціалізованим набором записів, розуміння яких є критичним для забезпечення стабільності мережевої інфраструктури.

Ключовим елементом будь-якої зони є запис початку повноважень (Start of Authority – SOA), який визначає сервер, що виступає первинним джерелом інформації та відповідає за оновлення даних у цій зоні. Цей запис містить життєво важливі параметри: час життя (TTL) для кешування, контактні дані відповідального адміністратора та серійний номер зони. У середовищі Windows Server запис SOA створюється автоматично під час ініціалізації ролі DNS для Active Directory, заповнюючись стандартними значеннями, які згодом можна адаптувати до політик організації через консоль управління [3].

Найбільш масовим типом записів, що становить основу адресації в інтернеті, є записи хостів типу A, які прямо зіставляють доменне ім’я з IPv4-адресою пристрою (рис. 6.5). Саме ці записи дозволяють користувачам знаходити ресурси за іменами. Варто зазначити, що окрім базового зіставлення, записи можуть містити додаткові метадані, такі як точний час створення або індивідуальні налаштування TTL. Однак, щоб переглянути або змінити ці розширені параметри в консолі DNS Management, адміністратору необхідно увімкнути режим розширеного перегляду (View – Advanced), оскільки в стандартному режимі відображається лише базова інформація [4].

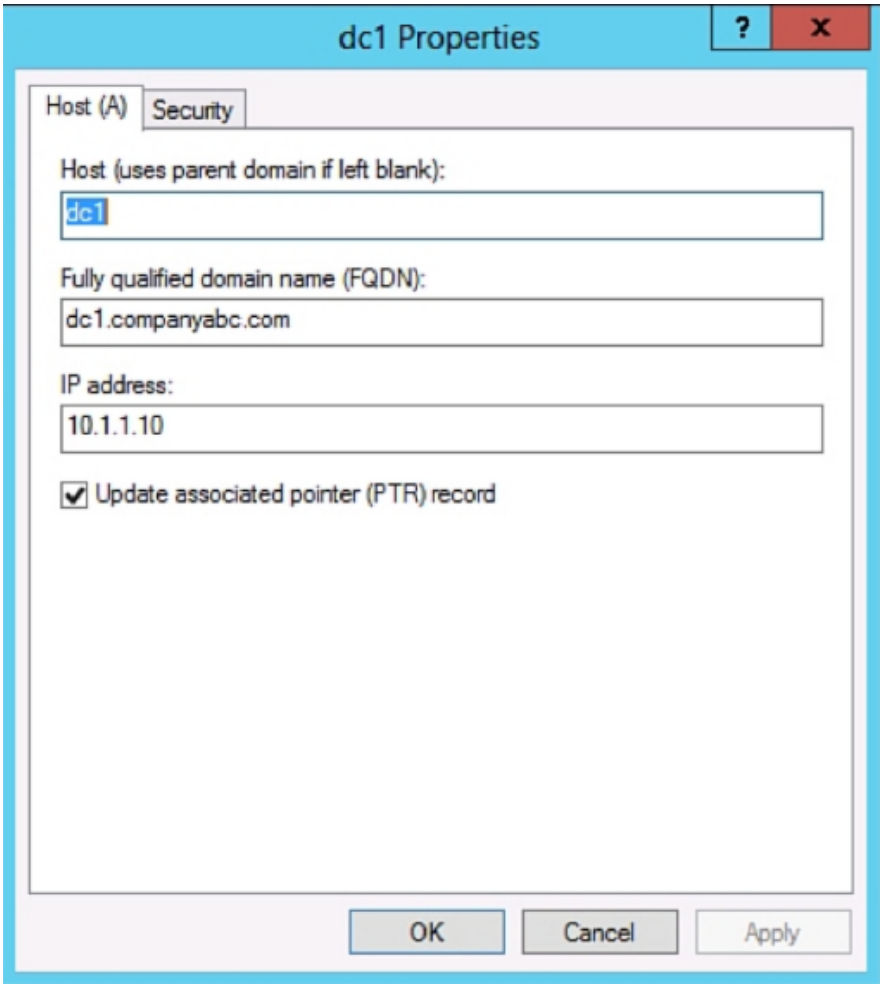

Рисунок 6.5 – Записи хостів типу A [4]

Для забезпечення доступності зони використовуються записи серверів імен (Name Server – NS), які вказують на те, які саме сервери уповноважені обробляти запити для даного домену. На відміну від запису SOA, який є єдиним для зони, записів NS зазвичай створюють декілька для забезпечення відмовостійкості. Важливо розуміти технічний нюанс: запис NS вказує не на IP-адресу, а на доменне ім’я сервера, тому для коректної роботи механізму розв’язання імен необхідна наявність відповідного A-запису для кожного сервера імен, на який посилається запис NS.

Особливе значення для інфраструктури Microsoft Active Directory мають записи служб (Service – SRV), які дозволяють клієнтам локалізувати сервери, що надають специфічні сервіси, такі як LDAP, Kerberos або глобальний каталог. Цей тип запису містить детальну технічну інформацію, включаючи порт, пріоритет та вагу служби, що дозволяє ефективно розподіляти навантаження між контролерами домену (рис. 6.6). Оскільки підтримка SRV-записів з’явилася в стандартах DNS не відразу, при використанні сторонніх DNS-серверів (наприклад, на базі UNIX BIND) критично важливо переконатися, що версія програмного забезпечення (8.1.2 або вище) підтримує цей стандарт, інакше коректна робота домену Windows буде неможливою [4].

Рисунок 6.6 – Приклад запису SRV для елемента глобального каталога Active Directory [4]

Окрім інфраструктурних записів, існують спеціалізовані типи для маршрутизації пошти та керування псевдонімами. Записи обміну поштою (MX) визначають сервери, що приймають SMTP-трафік для домену, причому пріоритет обробки пошти регулюється числовим значенням у записі. Для створення альтернативних імен вузлів використовуються записи канонічних імен (CNAME), які діють як псевдоніми, перенаправляючи запит на основний A-запис хоста. Це особливо зручно при міграції сервісів або для створення простих імен на кшталт mail.company.com замість складних технічних ідентифікаторів серверів.

Завершують екосистему DNS записи, що виконують специфічні або допоміжні функції. Для зворотного перетворення IP-адрес в імена використовуються записи покажчиків (PTR), які розміщуються виключно в зонах зворотного перегляду і є необхідними для багатьох механізмів безпеки. Також, з огляду на поступовий перехід мереж на новий протокол, зростає значення записів AAAA, які виконують ту ж функцію, що й записи A, але для 128-бітних адрес IPv6. Серед більш рідкісних типів можна виділити записи ISDN для телефонії, KEY для зберігання ключів шифрування та інші спеціалізовані формати, що застосовуються для вузьких задач адміністрування.

Забезпечення відмовостійкості

Архітектура системи доменних імен проектується з урахуванням вимог високої доступності, оскільки відмова служби DNS призводить до фактичної недоступності мережевих ресурсів для кінцевих користувачів, навіть за умови працездатності каналів зв'язку. Базовим механізмом забезпечення надійності є розгортання вторинних серверів DNS, які зберігають копію зон, отриману від первинного сервера. Синхронізація даних між цими серверами здійснюється за допомогою механізму передачі зони. При проектуванні відмовостійкої топології критично важливо розуміти різницю між повним (AXFR) та інкрементальним (IXFR) типами передачі даних. Якщо AXFR передбачає передачу всього файлу зони, що створює значне навантаження на мережу, то IXFR дозволяє передавати лише змінені записи, оптимізуючи трафік та пришвидшуючи конвергенцію даних.

У корпоративних середовищах, побудованих на базі Windows Server та Active Directory, підхід до відмовостійкості реалізується інакше – через використання зон, інтегрованих в Active Directory. У такій конфігурації відмовляються від класичної моделі «Головний-Ведений» (Primary-Secondary) на користь мультимайстерної реплікації. Це означає, що кожен контролер домену з роллю DNS-сервера зберігає доступну для запису копію зони, а зміни реплікуються засобами AD DS разом з іншими об'єктами каталогу. Такий підхід усуває єдину точку відмови, характерну для стандартних файлових зон, де вихід з ладу первинного сервера блокує можливість внесення змін до записів. Крім того, це дозволяє використовувати захищені динамічні оновлення, що підвищує загальний рівень безпеки інфраструктури [3].

Для забезпечення доступності самих мережевих сервісів на рівні DNS застосовується механізм циклічного розподілу навантаження, відомий як DNS Round Robin. Суть методу полягає у створенні декількох записів типу A з однаковим доменним іменем, але різними IP-адресами, що вказують на кластер серверів. При надходженні запитів DNS-сервер відповідає перестановкою списку IP-адрес, завдяки чому клієнти розподіляються між доступними вузлами. Хоча цей метод не є повноцінною заміною апаратним балансувальникам навантаження (оскільки не враховує реальний стан завантаженості хостів), він є ефективним інструментом базової відмовостійкості на прикладному рівні.

На глобальному рівні, особливо для обслуговування кореневих зон та високонавантажених публічних сервісів, впроваджується технологія Anycast DNS. Вона дозволяє анонсувати одну й ту ж IP-адресу з багатьох географічно рознесених точок присутності. Маршрутизація BGP (Border Gateway Protocol) автоматично спрямовує запит клієнта до топологічно найближчого сервера. У разі виходу з ладу одного вузла або сегмента мережі, маршрути динамічно перебудовуються, і трафік автоматично перенаправляється на наступний доступний вузол, забезпечуючи безперервність обслуговування без необхідності

зміни налаштувань на стороні клієнта.

Розуміння DNS-зон

Зони становлять основу ієрархічної структури DNS, яка регулює процеси розв'язання доменних імен у мережевому середовищі. Зони DNS є невід'ємною частиною простору імен Active Directory, який тісно узгоджується із глобальним простором імен DNS, забезпечуючи структурований та масштабований підхід до управління даними, пов'язаними з доменами. Шляхом сегментації зон DNS адміністратори отримують можливість більш ефективно зберігати інформацію про конкретні домени та управляти нею, що гарантує точність та ефективність процесу розв'язання доменних імен.

В архітектурі DNS виділяють три основні типи зон, кожен з яких виконує чітко визначену функцію.

Першим типом є первинна зона (Primary zone), яка виступає авторитетним джерелом DNS-інформації для домену. Вона містить остаточну, доступну для редагування копію бази даних DNS і відповідає за підтримку всіх записів ресурсів у межах своєї області дії. Ця зона є центральним органом управління для розв'язання імен у домені, забезпечуючи коректність та послідовність відповідей на DNS-запити [3].

Другим типом є вторинна зона (Secondary zone), яка діє як резервна копія первинної зони та містить копію DNS-записів, призначену лише для читання. Ця зона має критичне значення для забезпечення надлишковості, оскільки вона дозволяє процесу розв'язання імен продовжуватися безперервно навіть у випадку недоступності первинної зони. Вторинна зона синхронізується з первинною, що гарантує відображення в ній найбільш актуальної інформації DNS [3].

Третім спеціалізованим варіантом є зона-заглушка (Stub zone), яка є різновидом вторинної зони. На відміну від стандартної вторинної зони, що містить повну копію бази даних DNS, зона-заглушка зберігає лише мінімально необхідний обсяг інформації – зокрема, IP-адреси авторитетних DNS-серверів для даної зони – для перенаправлення запитів до відповідного авторитетного сервера. Така архітектура робить зони-заглушки корисними для спрощення адміністрування DNS та оптимізації мережевого трафіку шляхом зменшення потреби у повній реплікації даних DNS [3].

Ключову роль в управлінні цими зонами відіграють DNS-сервери. Авторитетний DNS-сервер, який оперує записами DNS для конкретного домену, є критично важливим елементом цієї структури. Конфігурація такого сервера може здійснюватися системним адміністратором вручну, що дозволяє забезпечити точний контроль над записами DNS, або динамічно іншими DNS-серверами за допомогою передачі зон та оновлень. Авторитетний сервер виступає кінцевим арбітром для DNS-запитів у своєму домені, гарантуючи точність та актуальність

відповідей. На противагу цьому, неавторитетний DNS-сервер покладається на кешовані дані, отримані в результаті попередніх пошуків DNS, і не зберігає оригінальних записів. Хоча неавторитетні сервери можуть надавати швидкі відповіді на основі кешованої інформації, вони не є остаточним джерелом для розв'язання імен, що іноді може призводити до отримання застарілих або неточних відповідей у разі неналежного обслуговування кешу [30].

Поза межами розгляду зон DNS важливо також розуміти роль WINS – застарілої служби, яка здійснює розв'язання імен NetBIOS. Хоча в сучасних мережах DNS значною мірою витіснила WINS, ця служба залишається актуальною в середовищах, де старіші системи та додатки все ще покладаються на NetBIOS для розв'язання імен. Ознайомлення з принципами роботи WINS може бути особливо важливим у мережах, що підтримують застарілу інфраструктуру, оскільки це забезпечує ефективну комунікацію між усіма системами, як старими, так і новими.

Виконання передачі зон

Копіювання бази даних DNS з одного сервера на інший здійснюється за допомогою спеціалізованого процесу, відомого як передача зони (або трансфер зони). Ця процедура є обов'язковою для будь-якої зони, що не інтегрована в Active Directory, відповідальність за вміст якої покладено більш ніж на один сервер імен. Хоча механізм виконання цієї операції може варіюватися залежно від версії програмного забезпечення DNS, фундаментальний принцип залишається незмінним: інформація про передачу зон завжди ініціюється та витягується вторинними серверами з первинних.

Первинні DNS-сервери можуть бути налаштовані таким чином, щоб автоматично повідомляти вторинні сервери про внесення змін до зони, ініціюючи тим самим процес передачі. Альтернативним підходом є налаштування передачі зони за розкладом, що дозволяє адміністраторам контролювати навантаження на мережу [4].

Для налаштування вторинного сервера на отримання оновлень із зони прямого перегляду необхідно виконати ряд послідовних дій. Процес починається із запуску диспетчера сервера (Server Manager) у середовищі Windows Server з повним графічним інтерфейсом, після чого здійснюється перехід до розділу DNS, де відображається перелік доступних серверів. Через контекстне меню обраного сервера запускається консоль DNS Manager, у якій необхідно розгорнути вузол Forward Lookup Zones (Зони прямого перегляду). Для активації механізму передачі у властивостях цільової зони на вкладці Zone Transfers слід встановити прапорець Allow Zone Transfers, обравши опцію дозволу передачі лише на сервери, зазначені у списку серверів імен (Name Servers). На вкладці Name Servers за допомогою кнопки Add додається FQDN-ім'я сервера, який прийматиме зміни. Під час додавання система виконає спробу перевірки сервера і, оскільки на цьому етапі він ще не є

авторитетним для даної зони, може з’явитися попередження про відсутність авторитетності, яке на даному етапі налаштування можна ігнорувати (рис. 6.7).

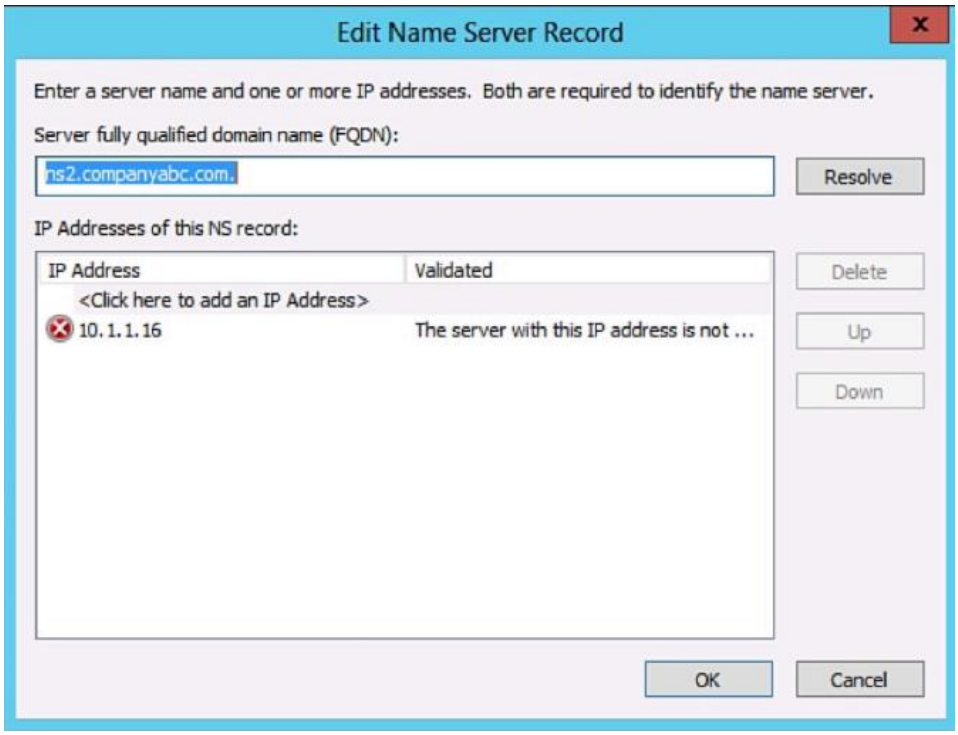

Рисунок 6.7 – Налаштування серверів для передачі зони [4]

Після того, як дозвіл на передачу налаштовано на первинному сервері, наступним кроком є створення та конфігурація вторинної зони на відповідному вторинному DNS-сервері. У консолі DNS Manager через меню Action обирається команда New Zone, що запускає майстер створення нових зон. У списку типів зон необхідно обрати Secondary Zone (Вторинна зона) [4].

Важливо зазначити, що оскільки вторинні зони не підтримують інтеграцію з Active Directory, відповідні опції будуть недоступними. Далі вводиться ім’я зони, яке має бути ідентичним імені первинної зони, та вказується IP-адреса або FQDN-ім’я первинного сервера, з якого здійснюватиметься реплікація записів. Після завершення роботи майстра зона буде автоматично передана з первинного сервера на вторинний, забезпечуючи синхронізацію даних.

Існує два основних методи виконання передачі зон: повний та інкрементальний. Стандартний метод, при якому весь вміст зони DNS повністю копіюється з первинного сервера на вторинний, називається асинхронною передачею зони (Asynchronous Zone Transfer – AXFR) або повним перенесенням. У цьому режимі кожен елемент бази даних DNS передається заново, незалежно від того, чи він вже існує на вторинному сервері. Хоча в ранніх реалізаціях DNS використовувався виключно цей метод, у сучасних системах він застосовується переважно для первинної синхронізації або у випадках значної

розсинхронізації даних. Більш ефективним підходом є інкрементальна передача зони (Incremental Zone Transfer – IXFR), під час якої реплікуються лише ті записи, що були змінені.

Механізм IXFR базується на використанні серійного номера, що зберігається в записі SOA первинної зони і збільшується на одиницю при кожній модифікації даних. Процес синхронізації передбачає порівняння серійних номерів: якщо вторинний сервер має версію зони з номером 45, а первинний – 55, передаватися будуть лише зміни, внесені в інтервалі між цими версіями. Це дозволяє суттєво економити пропускну здатність мережі [4].

Однак, якщо різниця між серійними номерами стає занадто великою, інформація на вторинному сервері вважається застарілою, і система автоматично ініціює повну передачу методом AXFR.

Розуміння DNS-запитів

Оскільки основним призначенням системи доменних імен (DNS) є перетворення імен для запитуючих клієнтів, механізм обробки запитів розглядається як один із найбільш фундаментальних елементів архітектури системи. У переважній більшості випадків до бази даних DNS надходять запити двох основних типів: рекурсивні та ітеративні.

Рекурсивні запити найчастіше ініціюються розпізнавачами – клієнтськими компонентами, які потребують розв’язання конкретного доменного імені сервером DNS. Крім того, такі запити можуть генеруватися самим DNS-сервером у випадках, коли налаштовано використання ретрансляторів на певний визначений сервер імен. Суть рекурсивного запиту полягає у з’ясуванні можливості конкретного сервера імен виконати повне перетворення для специфічного запису, при цьому відповідь може бути або остаточно позитивною, або негативною [3].

При виконанні ітеративних запитів до DNS-сервера ставиться вимога або здійснити перетворення імені, або надати посилання на інший DNS-сервер, який з високою ймовірністю володіє точнішою інформацією щодо місця обробки даного запиту. Після отримання посилання ініціюється наступний ітеративний запит до зазначеного сервера, і цей процес повторюється циклічно до моменту отримання позитивного або негативного результату розв’язання імені. Ці функції лежать в самій основі функціонування DNS, враховуючи її розподілену природу, і дозволяють ефективно виконувати процеси пошуку.

Розуміння еволюції Microsoft DNS

Реалізація доменних служб Active Directory (AD DS), що пропонується в Windows Server 2025, розширює спектр додаткових компонентів, який був впроваджений ще у версії Windows 2000 Server DNS та згодом удосконалювався у Windows Server 2003 і Windows Server 2008, Windows Server 2012 та Windows Server 2022.

У систему AD DS додано низку важливих функціональних покращень, проте вони не є настільки радикальними, щоб суттєво змінити стратегічні рішення щодо архітектури DNS. У цьому контексті розглядаються можливості, які були перенесені у Windows Server 2025 DNS із попередніх версій платформи, і які допомагають відрізняти дану реалізацію від інших систем DNS [3].

Найбільш вагомою зміною в реалізації DNS у Windows 2000 Server стало впровадження концепції зон, вбудованих у каталог, які отримали назву інтегрованих в Active Directory зон. Такі зони зберігалися безпосередньо в базі даних Active Directory, а не у стандартних текстових файлах, як у традиційній DNS. Під час реплікації Active Directory здійснювалася також і реплікація зони DNS. Такий підхід уможливив виконання безпечних оновлень, використання протоколу аутентифікації Kerberos та реалізацію мультимайстерної моделі DNS, за якої жоден із серверів не виступає єдиним еталоном, а на кожному вузлі міститься доступна для запису копія зони. У версіях Windows Server 2012 та пізніших, як і в Windows Server 2008, інтегровані в AD зони DNS продовжують використовуватися, проте з однією суттєвою модифікацією: для зниження навантаження, пов'язаного з реплікацією, інформація таких зон тепер зберігається не в контекстах іменування Active Directory, а у розділі додатків [4].

Механізм динамічних оновлень, що реалізується за допомогою Dynamic DNS (DDNS), надає клієнтам можливість автоматично реєструвати, оновлювати та скасовувати реєстрацію записів хостів під час підключення до мережі. Ця концепція, вперше представлена у Windows 2000 Server DNS, була перенесена у Windows Server 2025 без змін.

Окрім того, введена у Windows 2000 Server та збережена у Windows Server 2025 підтримка розширених наборів символів Unicode дозволяє службі DNS зберігати записи, що складаються із символів Unicode, фактично охоплюючи декілька наборів символів із безлічі різних мов. Це дозволяє DNS-серверу оперувати записами, що містять нестандартні символи, такі як підкреслення, літери різних алфавітів тощо [3].

Незважаючи на наявну підтримку символів Unicode в реалізації Microsoft DNS, у будь-якій інфраструктурі DNS рекомендується застосовувати стандартний набір символів. Дотримання цієї рекомендації забезпечує можливість обміну даними зон із реалізаціями DNS, що не підтримують Unicode, наприклад, із серверами Unix BIND. До стандартного набору входять символи латинського алфавіту (a-z, A-Z), цифри (0-9) та дефіс (-).

DNS у середовищі служб доменів Active Directory

Системи DNS та Active Directory Domain Services (AD DS) є нерозривно пов'язаними компонентами мережевої інфраструктури, які часто ототожнюються через схожість їхніх логічних структур. В основі Active Directory лежить ієрархічна структура стандарту X.500,

яка була спеціально спроектована для відображення на ієрархію DNS, чим і пояснюється їхня структурна подібність.

Служба DNS використовується в середовищі Active Directory для виконання всіх внутрішніх пошукових операцій – від запитів, необхідних клієнтам для автентифікації та входу в систему, до пошуку інформації в глобальному каталозі. Саме тому при плануванні розгортання або модернізації інфраструктури AD DS критично важливо враховувати аспекти інтеграції зі службою DNS. Будь-які порушення в роботі DNS можуть мати руйнівний вплив на функціонування середовища Active Directory, оскільки постійна взаємодія серверів та клієнтів залежить від безперебійної роботи служби перетворення імен [3].

З огляду на це, у будь-якій реалізації AD DS рекомендується розгортати резервну інфраструктуру DNS, розглядаючи можливість дублювання первинної зони навіть у невеликих мережах. Окрім забезпечення відмовостійкості, особливу увагу слід приділяти заходам безпеки: налаштуванню безпечних динамічних оновлень для зон, інтегрованих в Active Directory, відокремленню DHCP-серверів від контролерів домену та обмеженню адміністративного доступу для запобігання несанкціонованому перегляду даних.

Архітектура Active Directory Domain Services розроблена з урахуванням можливості співіснування та інтеграції зі сторонніми реалізаціями DNS, за умови підтримки ними динамічних оновлень та записів SRV (наприклад, UNIX BIND версії 8.1.2 і новіших).

Проте організаціям, які інтенсивно використовують технології Microsoft, рекомендується розміщувати зони Active Directory на серверах під управлінням Windows Server 2025, оскільки ця операційна система забезпечує покращені можливості захисту та інтеграції. У середовищах, де використовуються застарілі версії DNS або де розміщення клієнтів Active Directory у наявних базах даних є неможливим чи небажаним, доцільно виділити простір імен Active Directory в окрему зону, делегувавши повноваження відповідним серверам. Для забезпечення зворотного перетворення імен ресурсів із вихідної зони в системах Windows Server 2025 можуть бути налаштовані відповідні ретранслятори [4].

У певних архітектурних конфігураціях виникає необхідність застосування вторинних зон для забезпечення специфічних сценаріїв розв’язання імен. Історично, наприклад, у моделях з виділеним коренем, де два окремих дерева формують різні простори імен в межах одного лісу, для синхронізації в Windows Server було необхідне створення вторинних зон. Оскільки кожне дерево складається з незалежних доменів, що можуть не мати повноважень безпеки щодо інших доменів, для пошуку між деревами потрібен спеціальний механізм (рис. 6.8). У Windows Server 2025 впроваджено можливість реплікації окремих дерев на всі DNS-сервери в лісі, що знижує потребу у вторинних зонах, проте їх використання залишається актуальним для реплікації за межі лісу. Альтернативою для досягнення аналогічних результатів без повної реплікації даних може слугувати використання умовного

пересилання та зон-заглушок.

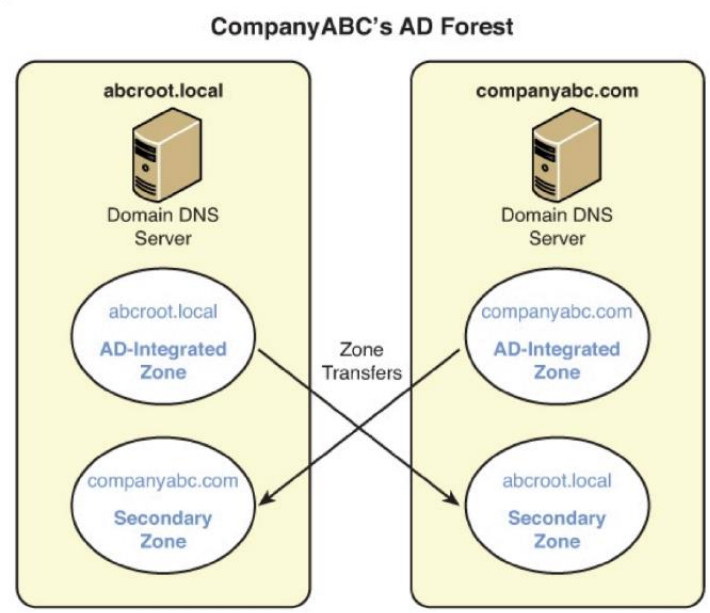

Рисунок 6.8 – Вторинні зони DNS доменів з виділеним коренем [4]

Механізм локалізації сервісів клієнтами AD DS повністю базується на DNS і використанні записів служб (SRV). Під час входу в систему клієнти здійснюють пошук спеціальних записів SRV, які вказують на розташування контролерів домену та серверів глобального каталогу.

У Windows Server 2025 ці записи розміщуються в окремій зоні, що реплікується на всі контролери домену з роллю DNS. Структура цієї зони передбачає створення піддоменів для кожного сайту Active Directory, у яких перелічуються ресурси, доступні саме в цьому сайті (рис. 6.9).

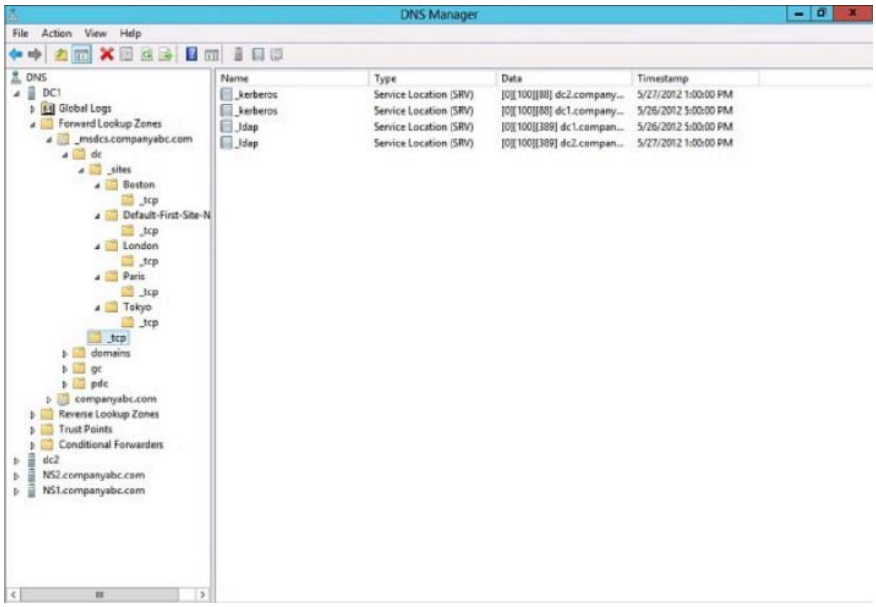

Рисунок 6.9 – Записи SRV рівня сайту [4]

Коректність цих записів є критичною: якщо запис SRV у піддомені сайту вказує на сервер з іншого сайту, клієнти будуть змушені проходити автентифікацію через повільні канали WAN. Поширена проблема виникає, коли створюється сайт Active Directory без серверів, і в його DNS-піддомен автоматично додається запис SRV з центрального вузла (концентратора). Після додавання нових серверів у цей сайт старі записи не видаляються автоматично, що призводить до неефективної маршрутизації запитів. Для забезпечення відмовостійкості в кореневому вузлі контейнерів сайтів також міститься повний список контролерів домену, який використовується для випадкового вибору сервера у разі недоступності локальних ресурсів [4].

Для вирішення проблеми зручності використання імен та відмови від застарілої служби WINS у Windows Server 2025 (як і в попередній версії 2022) пропонується використання зони GlobalNames (GNZ). Використання повністю визначених доменних імен (FQDN) часто є незручним для користувачів, тоді як односкладові імена (наприклад, http://intranet) традиційно вимагали використання WINS. Впровадження IPv6 стимулює відмову від WINS на користь DNS, яка пропонує менші витрати на адміністрування та вищу безпеку. Зона GlobalNames дозволяє перетворювати односкладові імена засобами DNS: якщо сервер не знаходить адресу в локальних зонах, він звертається до GNZ. Ця зона є звичайною зоною прямого перегляду зі спеціальним зарезервованим ім’ям GlobalNames, що повинна зберігатися в Active Directory.

Процес налаштування зони GlobalNames передбачає виконання чіткої послідовності дій через консоль диспетчера DNS. Створюється нова первинна зона, інтегрована в Active Directory, з областю реплікації на всі DNS-сервери в лісі. Зоні присвоюється ім’я GlobalNames, і для неї дозволяються динамічні оновлення. Після створення зони критично важливим етапом є активація її підтримки на рівні сервера. Для цього в командному рядку PowerShell необхідно виконати команду Set-DnsServerGlobalNameZone -Enable $true. Цю команду слід виконати на кожному сервері, який використовуватиме зону GlobalNames для перетворення імен, незалежно від статусу реплікації самої зони. Перевірити стан функції можна за допомогою командлета Get-DnsServerGlobalNameZone (значення Enable повинно дорівнювати True). Після активації до зони додаються записи типу CNAME (псевдоніми), що зіставляють односкладові імена з відповідними FQDN ресурсів, забезпечуючи коректне розв’язання імен без використання NetBIOS.

Виправлення неполадок DNS

Структура DNS є логічною, і за умови правильного вибору засобів та технологій процес усунення неполадок є зрозумілим та структурованим. Для успішного вирішення проблем при перетворенні імен у DNS необхідне глибоке знання діагностичних інструментів

та їхніх можливостей. Першим етапом діагностики для будь-якого адміністратора є використання програми Event Viewer (Перегляд подій). У середовищі Windows Server 2025 цей процес значно спрощено: всі події DNS, які реєструє Event Viewer, стають одразу доступними безпосередньо в консолі диспетчера DNS. Аналіз цього набору журналів дозволяє виявляти та усувати проблеми, що виникають у DNS під час реплікації, обробки запитів та в інших ситуаціях.

Для більш точної діагностики проблем на основі журналів подій на кожному сервері можна додатково активувати запис налагоджувальної інформації (Debug Logging). Включати цю функцію рекомендується лише за нагальної потреби, оскільки вона впливає на продуктивність системи та призводить до швидкого переповнення файлів журналів.

Процедура активації цієї функції складається з чіткої послідовності дій: спочатку виконується запуск диспетчера сервера (Server Manager) на сервері Windows Server 2025 з повним графічним інтерфейсом, після чого здійснюється перехід у розділ DNS, де відображається список серверів у серверному пулі з встановленою роллю DNS. Далі необхідно клацнути правою кнопкою миші на потрібному сервері та вибрати пункт DNS Manager (Диспетчер DNS). У консолі, що відкрилася, вибирається ім’я сервера, на якому проводиться налаштування, після чого через контекстне меню (права кнопка миші) обирається пункт Properties (Властивості). У вікні властивостей слід перейти на вкладку Debug Logging (Ведення журналу налагодження), відмітити прапорець Log Packets for Debugging (Реєструвати інформацію про пакети для налагодження), налаштувати інші необхідні параметри та підтвердити зміни натисканням кнопки ОК [3].

За замовчуванням файл журналу має назву dns.log і розміщується в каталозі c:\windows\system32\dns\.

Журнал DNS може бути дуже деталізованим і складним для читання, проте він надає вичерпну інформацію про точні дії DNS-сервера. Якщо відмітити прапорець Details (Подробиці) на вкладці Debug Logging, можна переглядати також і дані, що повертаються. Варто пам’ятати, що ведення журналу суттєво збільшує навантаження на DNS-сервер, тому його слід включати лише на час виявлення неполадок і негайно відключати після їх усунення.

Також для спостереження за роботою DNS використовується Монітор продуктивності (Performance Monitor) – вбудована утиліта, яка дозволяє глибоко вникнути в роботу мережі. Для DNS у цій утиліті пропонується безліч важливих лічильників, які дозволяють стежити за обробкою запитів, перенесенням зон, використанням пам’яті та іншими важливими показниками.

На стороні клієнтів (Windows 2000 Server і вище) функціонує вбудований клієнтський кеш для перетворення імен, де зберігається вся інформація, отримана від серверів імен. При надходженні пошукового запиту розпізнавач спочатку аналізує вміст цього кешу замість

звернення до сервера імен. Елементи залишаються в ньому до закінчення терміну їхнього життя (TTL), перезавантаження комп'ютера або скидання вмісту кешу. Якщо в клієнтський кеш потрапить помилкова інформація, її легко видалити за допомогою команди ipconfig /flushdns. Також за замовчуванням усі клієнти мають файл HOSTS, який дозволяє виконувати просте порядкове перетворення імен в IP-адреси. Зазвичай цей файл знаходиться в каталозі \%systemroot%\System32\drivers\etc. Введені вручну записи можуть суперечити DNS, тому при усуненні неполадок завжди перевіряється відсутність конфліктів між файлом HOSTS і базою даних DNS [4].

Найбільш корисним інструментом для пошуку та усунення проблем, пов'язаних із клієнтами DNS, є утиліта командного рядка NSLOOKUP.

Незважаючи на простоту, отримана з її допомогою інформація надає допомогу у виявленні проблем. У найпростішому випадку утиліта nslookup зв'язується зі стандартним DNS-сервером клієнта і намагається перетворити введене ім'я (наприклад, команда nslookup www.companyabc.com для тестування пошуку імені www.companyabc.com) [4].

В NSLOOKUP можна вводити й інші типи запитів, наприклад, створювати запити для перегляду записів MX або SOA, пов'язаних із певним доменом. Процедура виконання таких запитів включає наступні кроки: відкриття вікна командного рядка через меню Start (Пуск) – All Programs (Усі програми) – Accessories (Стандартні) – Command Prompt (Командний рядок). Введення команди nslookup і натискання клавіші Enter, введення команди set query=mx, введення імені домену, введення команди set query=soa та введення імені домену, продемонстровано на рисунку 6.10.

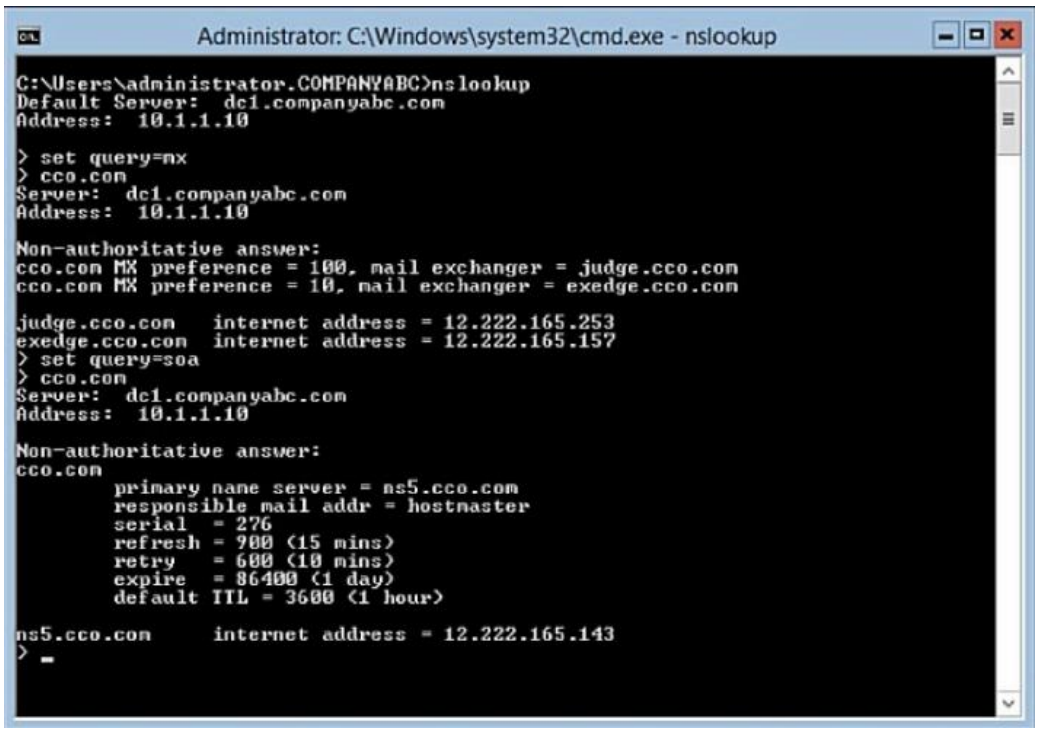

Рисунок 6.10 – Використання утиліти NSLOOKUP [4]

Можливості цієї утиліти не обмежуються тільки такими простими пошуками. За допомогою команди nslookup /? можна переглянути повний перелік доступних функцій. Загалом, утиліта NSLOOKUP є чудовим інструментом для вирішення багатьох завдань і повинна обов'язково входити в арсенал будь-якого фахівця, який займається виявленням і усуненням неполадок.

Ще одним важливим інструментом для пошуку та усунення проблем, пов'язаних із перетворенням імен у DNS, є утиліта IPCONFIG, яка зручна і для вирішення питань із TCP/IP.

Стосовно DNS утиліта IPCONFIG дозволяє виконувати кілька важливих операцій, що запускаються з командного рядка за допомогою відповідних параметрів. Параметр ipconfig /flushdns використовується при виникненні проблем із кешем на стороні клієнта для скидання його вмісту. Цей прапорець дозволяє видалити всі поміщені раніше в кеш запити, які може зберігати клієнт, і особливо корисний, якщо на сервері імен тільки-но змінилися IP-адреси, і певні клієнти тепер не можуть звернутися до нього. Параметр ipconfig /registerdns змушує клієнта динамічно перереєструвати себе в DNS, якщо відповідна зона підтримує динамічні оновлення. Цікавий і маловідомий прапорець ipconfig /displaydns дозволяє переглянути вміст клієнтського кешу і допомагає у виявленні певних проблем з окремими записами [4].

Також цінним джерелом інформації є утиліта TRACERT, що дозволяє отримати уявлення про шлях, який проходить DNS-запит при його пересиланні мережею. Наприклад, вказавши як параметр TRACERT адресу www.microsoft.com, можна побачити, через скільки маршрутизаторів і DNS-серверів доводиться проходити пакету.

Принцип роботи даної утиліти простий: спочатку відправляється DNS-запит із TTL-значенням 1. Оскільки всі маршрутизатори повинні зменшувати TTL кожного оброблюваного пакета на 1, перший же маршрутизатор відмовиться переадресовувати даний пакет і поверне відправнику повідомлення з відмовою. Після цього комп'ютер збільшує TTL-значення на 1 і відправляє пакет знову. Цього разу пакет пройде через перший маршрутизатор, але отримає відмову від другого. Цей процес триває доти, доки пакет не досягне місця призначення. Ця утиліта надає простий, але дуже ефективний спосіб для перегляду шляху, який DNS-запит проходить при його передачі через Інтернет [4].

Утиліта DNSCmd являє собою командну версію консолі диспетчера DNS. Вона встановлюється у вигляді частини ролі DNS Server у Windows Server 2025 і дозволяє адміністраторам створювати зони, змінювати записи і виконувати інші важливі адміністративні операції з командного рядка. Повний список усіх її можливостей можна переглянути, ввівши команду dnscmd /? [4].

Альтернативою є командлети PowerShell, модуль яких також встановлюється у вигляді частини ролі DNS Server у Windows Server 2025 і дозволяє виконувати аналогічні функції

точно так само, як і за допомогою традиційного засобу DNSCmd. У Windows PowerShell значно покращено можливості налаштування та управління DNS, у тому числі: дотримано паритет інтерфейсу користувача та команди DNSCmd; забезпечено встановлення та видалення ролі DNS Server за допомогою Windows PowerShell; реалізовано клієнтські запити Windows PowerShell із результатами перевірки DNSSEC; можливе налаштування сервера для комп'ютерів зі старими операційними системами. Усі можливості цієї утиліти можна побачити, виконавши команду Get-Command -Module DnsServer у вікні командного рядка PowerShell.

Тема 7
Служба DHCP

Призначення та принцип роботи DHCP

У складі операційної системи Windows Server служба DHCP (Dynamic Host Configuration Protocol) реалізована як опціональна мережева серверна роль, яка розгортається для управління розподілом IP-адрес та надання іншої інформації про оренду клієнтам DHCP. Варто зазначити, що всі клієнтські операційні системи на базі Windows містять клієнтську частину DHCP як невід'ємний компонент стека протоколів TCP/IP, причому цей клієнт активовано в системі за замовчуванням.

Протокол динамічної конфігурації хоста (DHCP) – це протокол архітектури «клієнт-сервер», який автоматично забезпечує хост Інтернет-протоколу (IP) його IP-адресою та іншою супутньою конфігураційною інформацією, такою як маска підмережі та шлюз за замовчуванням. У регламентуючих документах RFC 2131 та 2132 протокол DHCP визначено як стандарт IETF (Internet Engineering Task Force), що базується на протоколі початкового завантаження (BOOTP) – протоколі, з яким DHCP має значну кількість спільних деталей реалізації, що дозволяє хостам отримувати необхідну конфігурацію TCP/IP від сервера DHCP [1].

Для забезпечення доступу до мережі та її ресурсів кожен пристрій у мережі на базі TCP/IP повинен володіти унікальною одноадресною (unicast) IP-адресою. За відсутності служби DHCP налаштування IP-адрес для нових комп'ютерів або комп'ютерів, що переміщуються з однієї підмережі в іншу, повинно виконуватися вручну. Аналогічним чином вручну повинно здійснюватися вивільнення IP-адрес для комп'ютерів, які вилучаються з мережі. Запровадження DHCP дозволяє повністю автоматизувати цей процес та здійснювати його централізовано. Сервер DHCP підтримує пул IP-адрес і надає адресу в оренду будь-якому клієнту з підтримкою DHCP під час його ініціалізації в мережі. Оскільки IP-адреси є динамічними (надаються в оренду), а не статичними (призначаються на постійній основі), адреси, що більше не використовуються, автоматично повертаються до пулу для подальшого перерозподілу [1].

Адміністратором мережі встановлюються сервери DHCP, які підтримують інформацію про конфігурацію TCP/IP і надають налаштування адреси клієнтам із підтримкою DHCP у формі пропозиції оренди. Сервер DHCP зберігає інформацію про конфігурацію в базі даних, яка включає дійсні параметри конфігурації TCP/IP для всіх клієнтів у мережі, а також дійсні IP-адреси, що утримуються в пулі для призначення клієнтам, та адреси, що були виключені. Окрім того, база даних містить зарезервовані IP-адреси, асоційовані з конкретними клієнтами DHCP, що дозволяє забезпечити послідовне призначення однієї IP-адреси одному клієнту. Також визначається тривалість оренди, тобто проміжок часу, протягом якого IP-адреса може

використовуватися до моменту, коли вимагатиметься подовження оренди. Клієнт із підтримкою DHCP після прийняття пропозиції оренди отримує дійсну IP-адресу для підмережі, до якої він підключається, та запитані параметри DHCP. Останні являють собою додаткові параметри, які налаштовані на сервері DHCP для призначення клієнтам, наприклад, адреса маршрутизатора (шлюз за замовчуванням), DNS-сервери та доменне ім'я DNS [3].

Використання сервера DHCP забезпечує низку переваг, зокрема надійну конфігурацію IP-адрес. DHCP мінімізує помилки конфігурації, викликані ручним налаштуванням IP-адрес, такі як друкарські помилки або конфлікти адрес, спричинені призначенням однієї IP-адреси більш ніж одному комп'ютеру одночасно. Також досягається зменшення навантаження на адміністрування мережі завдяки таким функціям, як централізована та автоматизована конфігурація TCP/IP, можливість визначати конфігурації TCP/IP з центрального розташування та можливість призначати повний спектр додаткових значень конфігурації TCP/IP за допомогою параметрів DHCP [31].

Додатково забезпечується ефективна обробка змін IP-адрес для клієнтів, які потребують частого оновлення (наприклад, портативних пристроїв у бездротовій мережі), та пересилання початкових повідомлень DHCP за допомогою агента ретрансляції DHCP, що усуває потребу в розгортанні сервера DHCP у кожній підмережі.

Сервер DHCP у середовищі Windows Server включає розширені функціональні можливості, серед яких політики DHCP, що дозволяють створювати правила застосування параметрів на основі характеристик клієнта (наприклад, MAC-адреси або класу виробника), та журналювання аудиту DHCP для відстеження активності сервера, включаючи призначення та подовження оренди [31].

Керування серверами DHCP здійснюється за допомогою Windows PowerShell, консолі DHCP або Windows Admin Center. Важливими функціями є авторизація сервера DHCP в Active Directory для запобігання наданню адрес неавторизованими серверами, а також інтеграція з DNS, де динамічний DNS автоматично оновлює записи при зміні оренди. Передбачена інтеграція з протоколами IPv4 та IPv6 для підтримки обох стандартів адресації, функція відмовостійкості, що дозволяє двом серверам спільно використовувати одну область для надлишковості та балансування навантаження, а також інтеграція з IPAM (IP Address Management) для централізованого керування призначеннями IP-адрес та орендою.

Типи повідомлень протоколу

Функціонування служби DHCP у середовищі Windows Server 2025 базується на суворо регламентованому обміні службовими повідомленнями, які інкапсулюються в дейтаграми транспортного протоколу UDP.

Архітектура взаємодії клієнта та сервера реалізується через кінцевий автомат станів,

переходи між якими ініціюються отриманням або відправленням специфічних пакетів. Ключовим елементом ідентифікації типу повідомлення є поле опції 53 (DHCP Message Type), яке міститься в заголовку кожного пакета. Хоча базовий стандарт протоколу залишається незмінним (згідно з RFC 2131), реалізація стека TCP/IP у Windows Server 2025 забезпечує оптимізовану обробку цих повідомлень, підтримку розширених політик безпеки та інтеграцію з протоколом IPv6. Розрізняють вісім основних типів повідомлень для IPv4 та аналогічний, але термінологічно відмінний набір для IPv6, кожен з яких виконує критичну функцію в життєвому циклі оренди адреси [2].

Процес отримання мережевих налаштувань ініціюється повідомленням DHCPDISCOVER. Це широкомовний запит, що генерується клієнтом для локалізації доступних DHCP-серверів у межах фізичного сегмента мережі або за його межами через агенти ретрансляції. У Windows Server 2025 обробка цього повідомлення включає перевірку на відповідність політикам фільтрації MAC-адрес та наявність дозволів у списку дозволених/заборонених клієнтів (Allow/Deny) ще до моменту формування відповіді. Пакет надсилається на широкомовну адресу 255.255.255.255 із використанням порту джерела 68 та порту призначення 67. У структуру повідомлення часто включається опція 61 (Client Identifier – Ідентифікатор Клієнта) та запит на певні параметри (Опція 55), що дозволяє серверу заздалегідь визначити необхідну конфігурацію для конкретного пристрою [2].

У відповідь на валідний запит DHCPDISCOVER сервером генерується повідомлення DHCPOFFER. Цей пакет містить попередню пропозицію оренди, яка включає вільну IP-адресу з відповідної області, маску підмережі, тривалість оренди та ідентифікатор сервера. Варто зазначити, що у Windows Server 2025 механізм пропозиції адреси тісно інтегрований із службою захисту доступу до мережі, що дозволяє динамічно змінювати пропоновані параметри залежно від стану «здоров'я» клієнта. На цьому етапі запропонована IP-адреса тимчасово резервується сервером, щоб уникнути її видачі іншому клієнту до завершення транзакції. Повідомлення може надсилатися як unicast, так і broadcast, залежно від прапорця Broadcast у заголовку початкового запиту клієнта.

Важливим етапом узгодження параметрів є надсилання клієнтом повідомлення DHCPREQUEST. Цей тип повідомлення використовується в трьох різних сценаріях: для вибору конкретного сервера після отримання пропозиції DHCPOFFER (при цьому пропозиції інших серверів імпліцитно відхиляються), для підтвердження раніше отриманої адреси після перезавантаження системи, а також для періодичного подовження терміну дії оренди (Renewal). У середовищі Windows Server 2025, при налаштованій відмовостійкості, вміст цього повідомлення синхронізується між партнерами по відмовостійкості, що забезпечує безперервність обслуговування навіть у разі виходу з ладу основного вузла. При початковому виборі сервера повідомлення надсилається широкомовно, щоб повідомити всі інші сервери

про те, що їхні пропозиції не були прийняті, що дозволяє їм повернути зарезервовані адреси до пулу доступних.

Успішне завершення процесу конфігурації фіксується відправленням повідомлення DHCPACK (від англ. Acknowledgement). Цей пакет містить фінальне підтвердження надання IP-адреси та повний набір опцій DHCP, таких як адреси DNS-серверів, шлюзу за замовчуванням, доменне ім’я та інші специфічні. Отримання цього повідомлення переводить клієнта у стан «Bound». У випадку неможливості задоволення запиту клієнта (наприклад, якщо запитувана адреса вже зайнята або клієнт перемістився в іншу логічну підмережу), сервер Windows Server 2025 генерує повідомлення DHCPNAK (Negative Acknowledgement). Це змушує клієнта негайно припинити використання адреси та ініціювати процес отримання налаштувань заново (повернутися до стадії Discover) [2].

Окрім основного циклу DORA (DISCOVER – OFFER – REQUEST – ACK), протокол передбачає механізми діагностики та коректного завершення роботи. Повідомлення DHCPDECLINE надсилається клієнтом, якщо він виявляє конфлікт IP-адрес (наприклад, за допомогою ARP-запитів) перед використанням запропонованої адреси. Windows Server 2025 позначає таку адресу як «BAD_ADDRESS» і тимчасово вилучає її з обігу до втручання адміністратора або автоматичного очищення [3].

Для звільнення адреси використовується повідомлення DHCPRELEASE, яке дозволяє серверу негайно повернути адресу в пул. Також підтримується повідомлення DHCPINFORM, що застосовується клієнтами зі статичними адресами для отримання додаткових опцій без виділення IP-адреси.

Окремо слід виділити повідомлення протоколу DHCPv6, підтримка якого є важливою для сучасних мереж на базі Windows Server 2025. Це такі повідомлення, як Solicit (аналог Discover), Advertise (аналог Offer), Request (аналог Request) та Reply (аналог Ack), які забезпечують аналогічний функціонал у мережах з використанням IPv6.

Основні поняття DHCP: DHCP-сервер, DHCP-клієнт

Служба DHCP-сервера являє собою останню реалізацію сучасної системи автоматизованої мережевої адресації. Функціонал даної служби включає виконання всіх тих же операцій, що й служба BOOTP, проте додатково забезпечується можливість надання розширеної інформації клієнтам, які ініціюють запит на отримання IP-адреси.

Сервером DHCP видача IP-адреси клієнту реалізується за допомогою процедури, що складається з трьох етапів. На першому етапі клієнт DHCP завантажується та здійснює розсилку DHCP-запиту на отримання IP-адреси всім вузлам у локальній мережі. На другому етапі DHCP-сервер, що знаходиться в локальній мережі, отримує цей запит і виконує підготовку до відправлення IP-адреси даному клієнту у формі DHCP-оренди. На

завершальному етапі, після визначення DHCP-сервером необхідної інформації із запиту клієнта, здійснюється видача клієнту DHCP-оренди IP-адреси, яка включає також додаткові параметри оренди, такі як маска підмережі, шлюз за замовчуванням та, найімовірніше, IP-адреса самого сервера [4].

Клієнтська служба DHCP – це служба на стороні клієнта, що виконує запит IP-адреси з мережі. Залежно від конфігурації мережевого адаптера системи, клієнтська служба DHCP може перебувати в активному стані або бути відключеною. У випадках, коли клієнтом використовується мережеве завантаження, служба може набувати вигляду клієнта BOOTP або PXE, керованого системою [4].

У середовищі Windows керування клієнтською службою DHCP здійснюється на основі конфігурації, що зберігається в операційній системі Microsoft, а також безпосередньо на кожному адаптері. У разі виявлення адаптером підключення до мережі та за умови налаштування IP-конфігурації на автоматичну адресацію, клієнтською службою ініціюється розсилка запиту IP-адреси. Коли з сервера буде отримано відповідь, інформація про оренду застосовується до відповідного адаптера, після чого стає можливим повноцінний мережевий обмін даними.

Одночасно з DHCP-орендою IP-адреси клієнтом отримується важлива додаткова інформація – термін дії оренди. Цей параметр визначає часовий проміжок, протягом якого клієнт має право використовувати видану IP-адресу до моменту необхідності повторного звернення до DHCP-сервера з метою подовження існуючої або отримання нової оренди.

Клієнтом DHCP здійснюється кешування цієї інформації. У ситуаціях, коли термін оренди наближається до завершення, або під час перезапуску системи чи нової ініціалізації мережі, клієнт DHCP встановлює зв’язок із DHCP-сервером для перевірки дійсності оренди або необхідності її подовження чи заміни.

Окрім зазначеного, у системах Microsoft на клієнтську службу DHCP покладається функція керування реєстрацією клієнта в динамічній DNS за умови доступності відповідного сервера динамічної DNS. Однак цей алгоритм не застосовується у випадку, коли служба DHCP-сервера передає реєстрацію DHCP-оренди в динамічній DNS безпосередньо самому серверу.

Розподіл адрес

Процес розподілу IP-адрес сервером DHCP не є хаотичним, а підпорядковується суворому детермінованому алгоритму, основою якого є концепція «Області» (англ. Scope).

У термінології Windows Server область – це адміністративне групування IP-адрес для комп’ютерів у підмережі, що використовують службу DHCP.

Адміністратором спочатку проектується діапазон дійсних IP-адрес, після чого

визначаються діапазони виключень (Exclusions) – адреси, які не підлягають динамічному розподілу (наприклад, адреси шлюзів, принтерів або серверів зі статичною конфігурацією). Сукупність адрес, що залишаються після застосування виключень, формує так званий «пул доступних адрес».

Існує три основні методи розподілу адрес, які реалізуються DHCP-сервером: динамічний, автоматичний та ручний (резервування).

При динамічному розподілі, який є найбільш поширеним, адреса надається клієнту на обмежений час (термін оренди). Сутність цього підходу полягає у тимчасовому наданні клієнту IP-адреси з визначеного адміністратором пулу вільних адрес на обмежений проміжок часу, який називається терміном оренди. На відміну від автоматичного розподілу, де адреса закріплюється за клієнтом перманентно, динамічний механізм спроектовано для забезпечення ефективної ротації адрес, що дозволяє обслуговувати кількість клієнтів, яка перевищує розмір доступного адресного простору, за умови, що не всі вони підключені до мережі одночасно. Цей процес регулюється станом бази даних сервера, де кожному запису про активну оренду відповідає часова мітка закінчення її дії [33].

Автоматичний розподіл передбачає призначення постійної IP-адреси вільному клієнту без обмеження часу, що доцільно для стабільних мереж з низькою мобільністю вузлів. Механізм автоматичної приватної IP-адресації (Automatic Private IP Addressing – APIPA) спроектовано для забезпечення можливості системам під управлінням ОС Windows, що функціонують у межах єдиного мережевого сегмента, автоматично встановлювати мережеві з’єднання та здійснювати обмін інформацією навіть за умови повної недоступності серверів DHCP. Дана технологія позиціонується як ефективне рішення для розгортання в мережевих інфраструктурах малого масштабу, де виникає потреба у спільному використанні ресурсів та обміні даними між декількома обчислювальними вузлами за умови мінімального технічного супроводу з боку IT-персоналу або повної його відсутності. IP-адреси, що автоматично присвоюються мережевим адаптерам у такій конфігурації, генеруються із зарезервованого діапазону підмережі 169.254.0.0/16. Слід зазначити, що функціонал адресації APIPA активовано за замовчуванням на всіх клієнтських системах сімейства Windows. У ситуаціях, коли клієнт Windows не може локалізувати DHCP-сервер і ініціює процедуру самопризначення автоматичної приватної IP-адреси, існує вірогідність, що система не одразу виявить подальшу появу DHCP-сервера в мережі, що може призвести до надто тривалого перебування вузла поза межами основного мережевого середовища. Варто також враховувати архітектурну особливість, згідно з якою службу APIPA неможливо деактивувати в операційних системах Windows та Windows Server інакше, ніж шляхом повного відключення протоколу DHCP [4].

Третій метод – це резервування – він забезпечує прив’язку конкретної IP-адреси до

унікального ідентифікатора клієнта (MAC-адреси). У Windows Server 2025 механізм резервування вдосконалено: окрім традиційної прив'язки за MAC-адресою, підтримується ідентифікація за DHCP Unique Identifier (DUID), що є критично важливим для підтримки клієнтів IPv6 та складних гетерогенних середовищ [3].

Загалом, алгоритм вибору адреси сервером при отриманні запиту DHCPDISCOVER від клієнта виконується у чіткій послідовності. Спочатку сервером здійснюється пошук запису резервування в базі даних, що відповідає апаратному ідентифікатору клієнта. Якщо такий запис знайдено, клієнту пропонується саме зарезервована адреса. У разі відсутності резервування сервер перевіряє, чи мав цей клієнт раніше призначену активну оренду (яка ще не минула). Якщо попередню адресу знайдено і вона доступна, вона пропонується повторно. Якщо ж клієнт є новим або термін його попередньої оренди сплив, сервер обирає першу доступну адресу з пулу. У Windows Server 2025 цей процес оптимізовано завдяки використанню бітових карт для швидкого пошуку вільних слотів у базі даних, що мінімізує затримку відповіді.

Важливим аспектом надійності розподілу адрес у Windows Server 2025 є вбудований механізм виявлення конфліктів. Перед тим як запропонувати клієнту IP-адресу, сервером може виконуватися перевірка її доступності шляхом надсилання ICMP-запиту (Ping). Якщо на запит отримано відповідь, це свідчить про те, що адреса несанкціоновано використовується іншим вузлом у мережі (наприклад, налаштована вручну). У такому випадку сервер позначає цю адресу як «BAD_ADDRESS» і переходить до вибору наступної доступної адреси з пулу. Кількість спроб виявлення конфліктів налаштовується адміністратором, проте слід враховувати, що кожна перевірка вносить додаткову затримку в процес отримання адреси [31].

Особливістю реалізації розподілу адрес у сучасних версіях Windows Server, включаючи версію 2025, є застосування політик DHCP (Policy Based Assignment). Це дозволяє адміністраторам змінювати стандартну логіку розподілу, призначаючи IP-адреси з певних діапазонів або з певними опціями на основі критеріїв, таких як клас виробника, клас користувача або MAC-адреса.

Політики оренди та резервування

Впровадження політик DHCP (Policy Based Assignment – PBA) у сучасних серверних операційних системах, зокрема у Windows Server 2025, дозволяє перейти від лінійної моделі розподілу адрес до гнучкої, умовно-залежної архітектури керування мережевими клієнтами. Політики DHCP визначаються як набір правил, що дозволяють адміністратору класифікувати запити клієнтів на основі специфічних критеріїв та застосовувати до них диференційовані налаштування. Основними критеріями, що використовуються для формування умов

політики, є MAC-адреса клієнта (з підтримкою шаблонів та масок), клас виробника, клас користувача, ідентифікатор клієнта та інформація агента ретрансляції (Relay Agent Information). Цей механізм надає можливість сегментувати єдину фізичну підмережу на логічні групи пристроїв (наприклад, IP-тефони, принтери, гостьові пристрої, корпоративні робочі станції) без необхідності створення окремих областей або VLAN, забезпечуючи при цьому кожній групі унікальний набір мережевих опцій.

Процес обробки політик сервером Windows Server 2025 здійснюється у суворій ієрархічній послідовності, яка визначається порядком обробки, встановленим адміністратором. При надходженні запиту DHCPDISCOVER або DHCPREQUEST сервер послідовно перевіряє відповідність атрибутів пакета умовам налаштованих політик. Перша політика, критерії якої задовольняються клієнтським запитом, вважається активною, і подальший перебір зупиняється (якщо не налаштовано інакше). Це дозволяє реалізувати складні сценарії конфігурації, де для специфічних пристроїв застосовуються виняткові налаштування, а для всіх інших – загальні правила. Важливою особливістю реалізації у Windows Server 2025 є можливість використання логічних операторів «AND» та «OR» при комбінуванні умов, що дозволяє створювати високоточні фільтри, наприклад, застосовувати політику лише до пристроїв певного виробника, що підключаються через конкретний комутатор [3].

У контексті керування часом оренди, політики відіграють ключову роль в оптимізації використання адресного простору та безпеки мережі. За допомогою політик можна встановити відмінні терміни оренди для різних категорій пристроїв у межах однієї області. Наприклад, для стаціонарних робочих станцій та серверного обладнання може бути встановлено тривалий час оренди (наприклад, 8 днів або більше), що зменшує обсяг службового трафіку та навантаження на сервер. Водночас для мобільних пристроїв або гостьових клієнтів, ідентифікованих за класом користувача або діапазоном MAC-адрес, термін оренди може бути скорочено до кількох годин. Такий підхід забезпечує швидке повернення невикористовуваних адрес до пулу, запобігаючи вичерпанню адресного простору в сегментах з високою ротацією клієнтів, що є критичним для бездротових мереж у великих корпоративних середовищах.

Взаємодія політик із механізмом резервування адрес у Windows Server 2025 характеризується системою пріоритетів, де налаштування, визначені на рівні індивідуального резервування, традиційно мають найвищий пріоритет. Проте політики дозволяють групувати резервування або застосовувати специфічні опції до групи зарезервованих клієнтів без необхідності ручного налаштування кожного запису. Крім того, політики дозволяють виділяти окремі діапазони IP-адрес всередині області для ексклюзивного використання певною групою клієнтів. Якщо клієнт відповідає умовам політики, він отримує IP-адресу

виключно з визначеного для цієї політики діапазону. Це дозволяє гарантувати, що критично важливі пристрої (наприклад, медичне обладнання або системи безпеки) завжди отримають адресу з пріоритетного пулу, навіть якщо основний пул адрес для загальних клієнтів буде вичерпано.

Окрему увагу в Windows Server 2025 приділено інтеграції політик із повним життєвим циклом оренди, включаючи підтримку FQDN (Fully Qualified Domain Name). Політики дозволяють керувати поведінкою реєстрації DNS для різних типів клієнтів. Наприклад, можна налаштувати політику, яка забороняє динамічне оновлення DNS-записів для пристроїв із класу «Guest», підвищуючи рівень безпеки інфраструктури імен. Керування цими складними конфігураціями у Windows Server 2025 реалізовано через консоль DHCP, Windows Admin Center, а також за допомогою розширених командлетів PowerShell, що дозволяє автоматизувати створення та реплікацію політик у масштабних відмовостійких кластерах DHCP, забезпечуючи ідентичність логіки обробки запитів на всіх вузлах мережі [3].

Налаштування DHCP-сервера на базі Active Directory засобами ОС Windows Server

Перед початком інсталяції сервера DHCP необхідно забезпечити виконання низки обов'язкових попередніх умов. До таких вимог належать: налаштована статична IPv4-адреса мережевого інтерфейсу, попередньо визначений діапазон IP-адрес для створення області DHCP, а також наявність облікового запису, що входить до групи адміністраторів або має еквівалентні повноваження.

Процес встановлення сервера DHCP передбачає додавання ролі DHCP Server до існуючого сервера Windows Server. Інсталяція може бути виконана як за допомогою PowerShell, так і через графічний інтерфейс диспетчера серверів (Server Manager).

У разі використання диспетчера серверів на робочому столі Windows відкривається меню «Пуск», обирається «Server Manager», після чого в меню «Manage» (Управління) ініціюється команда «Add Roles and Features» (Додати ролі та компоненти). У майстрі налаштування на сторінці «Before you begin» (Перед початком) натискається «Next», обирається тип встановлення «Role-based or feature-based installation» (Встановлення на основі ролей або компонентів), залишаються параметри за замовчуванням на сторінці вибору цільового сервера, а на сторінці вибору ролей встановлюється прапорець «DHCP Server» (рис. 7.1). Після підтвердження додавання необхідних компонентів та ознайомлення з описом ролі, на сторінці підтвердження натискається кнопка «Install» (Встановити). Завершення інсталяції не вимагає перезавантаження системи [32].

Після успішної інсталяції ролі DHCP Server критично важливим етапом є авторизація та конфігурація сервера.

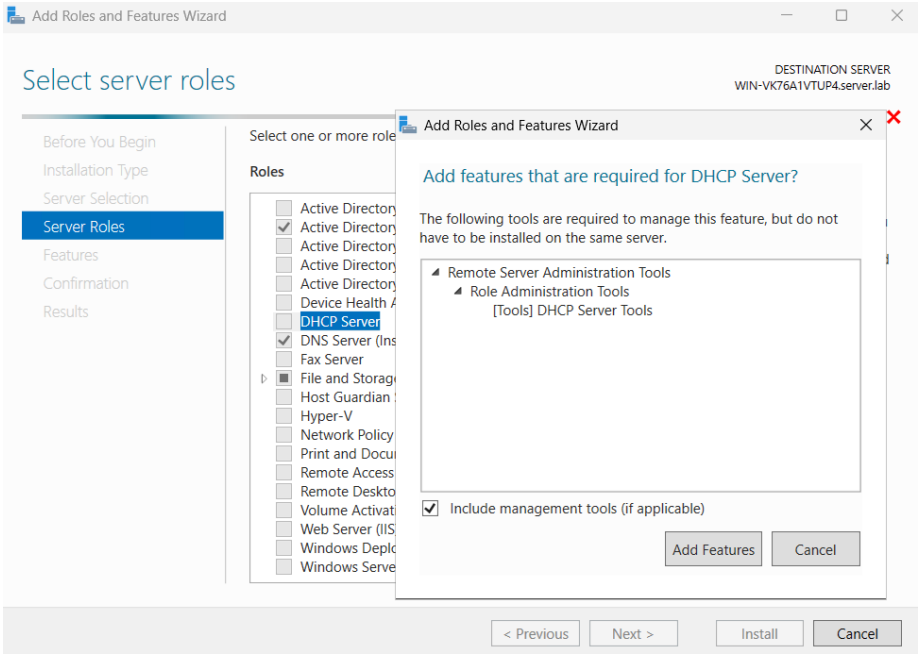

Рисунок 7.1 – Додавання ролі «DHCP-сервер» [32]

При розгортанні DHCP у доменному середовищі Active Directory необхідно виконати авторизацію сервера для його легітимного функціонування в домені. Слід зазначити, що неавторизовані сервери DHCP, встановлені в доменах Active Directory, не можуть функціонувати належним чином і не здійснюють оренду IP-адрес клієнтам. Автоматичне відключення неавторизованих серверів є механізмом безпеки, спрямованим на запобігання призначенню некоректних IP-адрес клієнтам у мережі несанкціонованими серверами. Процедура авторизації через графічний інтерфейс виконується шляхом відкриття консолі DHCP через меню «Administrative Tools» (Адміністрування), де у контекстному меню сервера обирається пункт «Authorize» (Авторизувати) (рис. 7.2). Після оновлення списку серверів успішна авторизація підтверджується появою зеленого індикатора на піктограмі сервера.

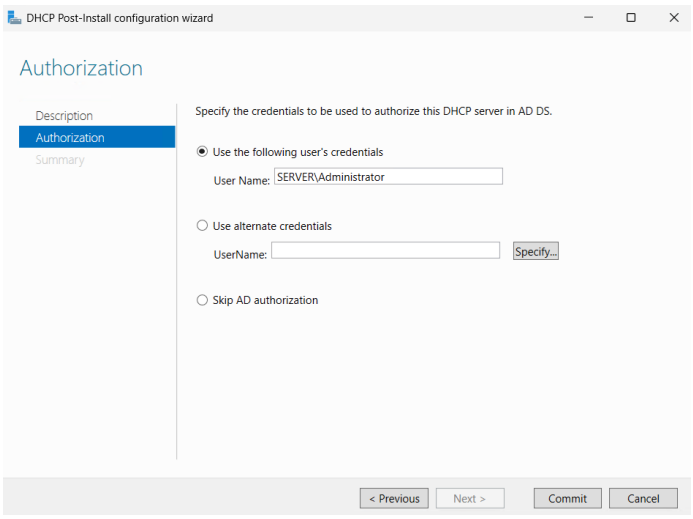

Рисунок 7.2 – Виконання авторизації для DHCP-сервера [32]

Наступним кроком після авторизації є створення нової області IPv4, яка визначає діапазон IP-адрес для обслуговування клієнтів. У консолі DHCP розгортається ім’я сервера, у контекстному меню вузла IPv4 обирається пункт «New Scope» (Нова область), що запускає відповідний майстер. У ході роботи майстра задається ім’я області, визначається діапазон IP-адрес та маска підмережі (рис. 7.3).

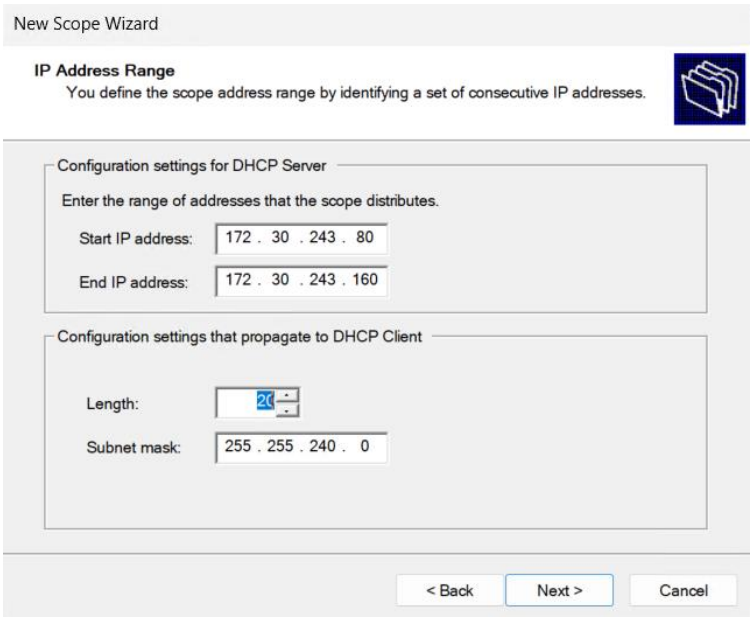

Рисунок 7.3 – Визначення діапазону IP-адрес та маски підмережі для DHCP-сервера [32]

На етапі «Add Exclusions and Delay» (Додавання виключень та затримки) можна вказати адреси, які не підлягають розподілу (рис. 7.4). Далі визначається тривалість оренди (Lease Duration), тобто термін дії призначеної IP-адреси (рис. 7.5).

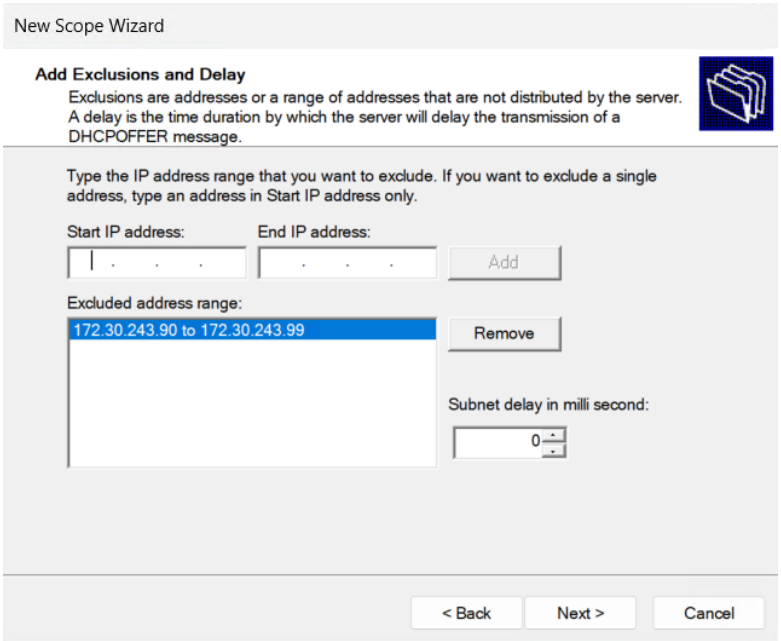

Рисунок 7.4 – Додавання виключень IP-адрес [32]

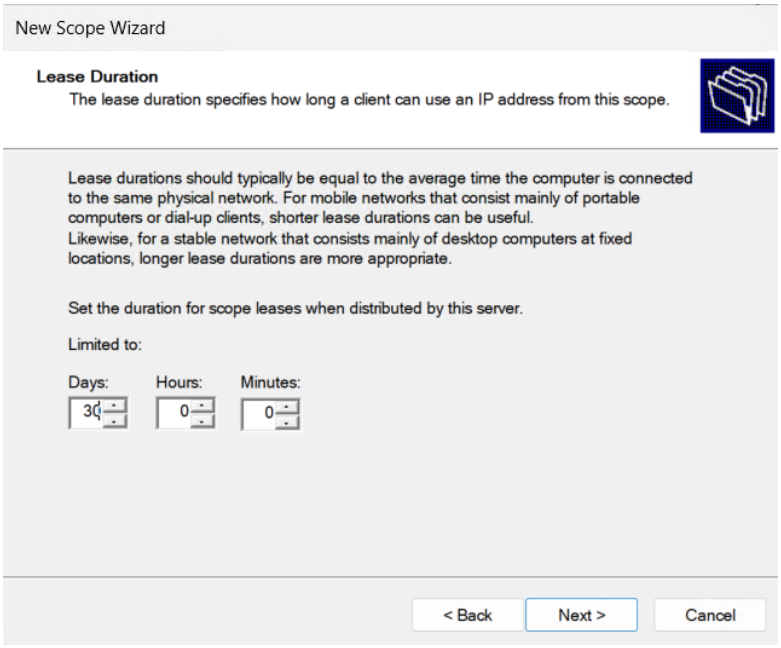

Рисунок 7.5 – Налаштування часу оренди для області DHCP [32]

На сторінці «Configure DHCP Options» (Налаштування параметрів DHCP) рекомендується обрати негайне налаштування опцій, таких як адреса маршрутизатора (шлюз за замовчуванням), доменне ім’я та сервери DNS, необхідні для розпізнавання імен, а також сервери WINS за їх наявності. Завершується процес активацією області шляхом вибору опції «Yes, I want to activate this scope» (Так, я хочу активувати цю область) (рис. 7.6).

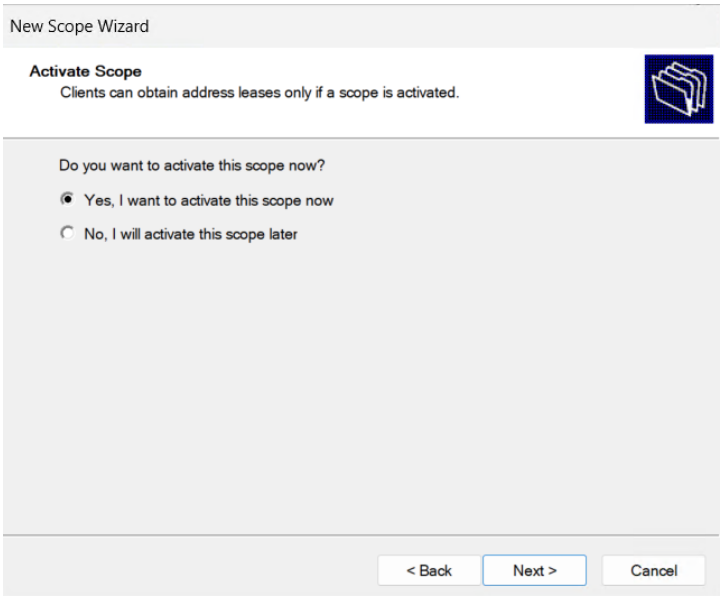

Рисунок 7.6 – Вибір опції активації області DHCP [32]

Після створення області управління її параметрами здійснюється через консоль DHCP або PowerShell. Для модифікації опцій області в консолі розгортається вузол IPv4 та відповідна область, обирається вузол «Scope Options» (Опції області), де через контекстне

меню та пункт «Configure Options» (Налаштувати опції) можна активувати, деактивувати або змінювати властивості параметрів. Окрім опцій, адміністратор може керувати резервуванням адрес (Reservations), що гарантує закріплення конкретної IP-адреси за MAC-адресою мережевого інтерфейсу клієнта. Створення резервування можливе шляхом конвертації існуючої оренди через контекстне меню запису в «Address Leases» (Оренда адрес) або створення нового резервування вручну у вузлі «Reservations», де вказуються ім’я, IP-адреса та MAC-адреса. Також здійснюється керування виключеннями (Exclusions) через вузол «Address Pool» (Пул адрес), де через пункт «New Exclusion Range» (Новий діапазон виключення) задаються початкова та кінцева адреси діапазону, що вилучається з розподілу [32].

Важливим компонентом безпеки є захист імен DHCP (DHCP Name Protection), який при використанні реєстрації в динамічній DNS забороняє клієнту DHCP реєструвати або перезаписувати існуюче ім’я, якщо воно вже знаходиться в доменній зоні DNS і не належить цьому клієнту. Це запобігає атакам типу спуфінг (підміна) та пошкодженню записів статично налаштованих систем. Активація захисту можлива на рівні сервера або області. Для налаштування на рівні області у властивостях області обирається вкладка DNS, натискається кнопка «Configure» (Налаштувати) у розділі «Name Protection» та встановлюється прапорець «Enable Name Protection» (Увімкнути захист імен). Аналогічні дії виконуються для активації захисту на рівні вузла IPv4 сервера, що застосує налаштування до всіх областей [34].

Для підвищення надійності сервера після налаштування реєстрації DNS та захисту імен необхідно виконати конфігурацію взаємодії DHCP та динамічної DNS. Рекомендується створити спеціальний обліковий запис служби в Active Directory (наприклад, DHCP-SVC) із секретним паролем, для якого встановлено параметр відсутності вимоги зміни пароля при першому вході. У консолі DHCP у властивостях вузла IPv4 на вкладці DNS слід переконатися, що дозволено динамічне оновлення DNS. Далі на вкладці «Advanced» (Додатково) через кнопку «Credentials» (Облікові дані) вводяться ім’я створеного облікового запису, домен та пароль, після чого зміни зберігаються, а служба DNS перезапускається.

Служба DHCP у Windows Server підтримує інтеграцію зі службою захисту мережевого доступу (Network Access Protection – NAP). Політики NAP містять критерії, дотримання яких (наприклад, наявність антивірусного ПЗ та оновлень) дозволяє системі працювати в мережі. Для інтеграції на рівні області у властивостях області на вкладці «Network Access Protection» обирається «Enable for This Scope» (Увімкнути для цієї області) та визначається профіль NAP. Для активації на всіх областях це налаштування виконується у властивостях вузла IPv4, що призводить до перезапису параметрів NAP у всіх існуючих областях [34].

Також адміністраторам надається доступ до журналів дій та подій DHCP для моніторингу роботи служби (рис. 7.7). Журнал дій зберігається у текстовому форматі в папці

C:\Windows\System32\DHCP і перезаписується щотижня. Розширені журнали подій (Admin, Operational, FilterNotifications) доступні для перегляду через засіб перегляду подій (Event Viewer) у вузлі Applications and Services Logs/Microsoft/Windows/DHCP-Server.

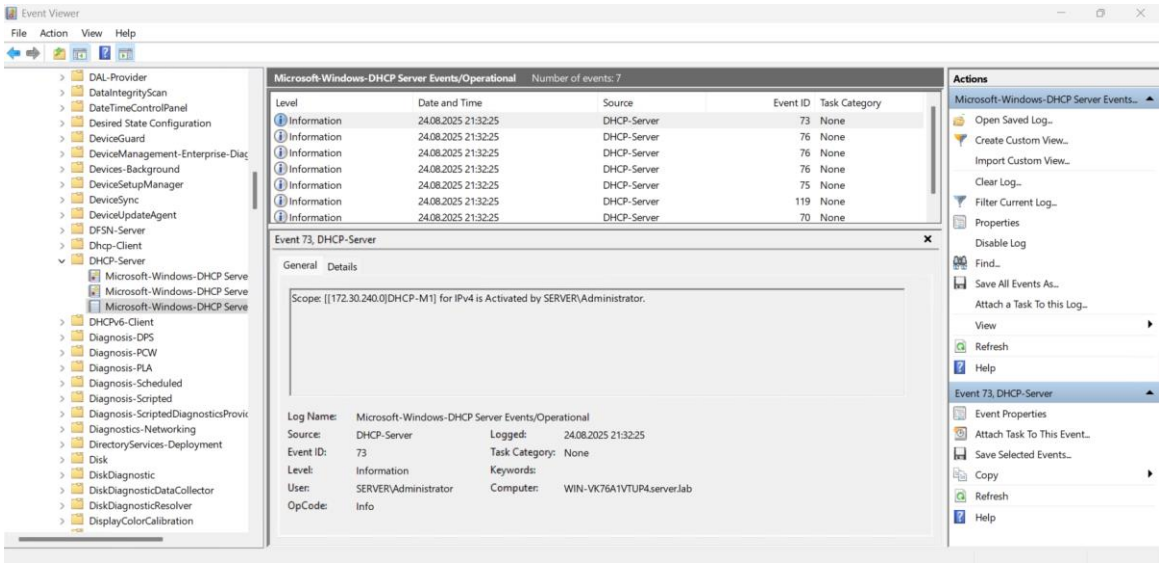

Рисунок 7.7 – Журнали DHCP-сервера [3]

Тема 8
RDS в Active Directory

Поняття та призначення RDS у корпоративних мережах

Служба віддалених робочих столів (Remote Desktop Services – RDS) відіграє ключову роль у функціонуванні операційних систем Windows Server, забезпечуючи користувачам можливість доступу до графічних інтерфейсів комп'ютерів та застосунків із віддалених локацій, незалежно від того, чи перебувають вони в тій самій мережі, чи підключаються через мережу Інтернет. Раніше відома як служби терміналів (Terminal Services – TS) до моменту її ребрендингу в Windows Server 2008 R2, RDS надає надійний функціонал, що дозволяє користувачам запускати віртуалізовані застосунки безпосередньо на своїх робочих столах. Ця функція є надзвичайно цінною в корпоративних середовищах, де централізоване управління застосунками та робочими столами визначається як критично важливе завдання [4].

За замовчуванням у Windows Server дозволяється два одночасних сеанси віддаленого робочого столу без необхідності придбання додаткового ліцензування. Це обмеження є достатнім для виконання базових адміністративних завдань, однак у випадках, коли виникає необхідність одночасного підключення більше ніж двох користувачів, для керування додатковими ліцензіями має бути налаштований сервер ліцензування RDS. Для активації та належного налаштування RDS у середовищі Windows Server 2025 роль RDS повинна бути додана через інтерфейс управління сервером, як зображено на рисунку 8.1.

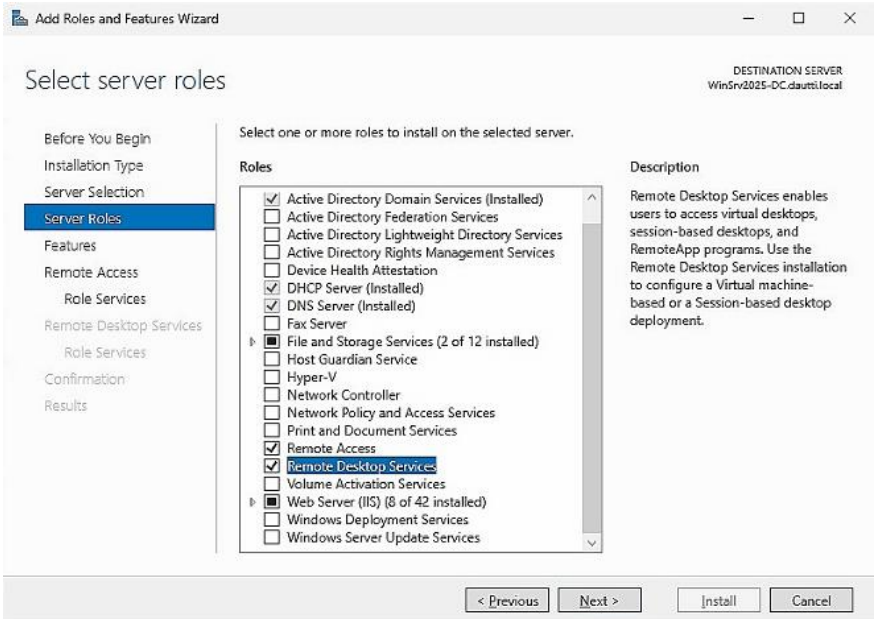

Рисунок 8.1 – Додавання ролі RDS у Windows Server 2025 [3]

Служба RDS являє собою універсальний продукт, впровадження якого дозволяє задовольнити різноманітні виробничі вимоги. У певних сценаріях адміністраторами дана

служба застосовується для дистанційного адміністрування сервера, групи серверів або окремих застосунків. Вона також надає користувачам можливість звертатися до застосунків та мережевих ресурсів за допомогою термінального сеансу. Нарешті, службу RDS може бути реалізовано постачальниками хмарних служб: це дозволяє створювати служби керованих застосунків, що усуває необхідність придбання апаратного та програмного забезпечення сервера, а також необхідність його супроводу.

Незалежно від причин розгортання RDS, її впровадження забезпечує низку переваг.

По-перше, забезпечується централізоване розгортання застосунків. При використанні RDS програмне забезпечення розміщується виключно на серверах RDS, що уможливлює централізоване управління, а також дозволяє швидко виконувати як розгортання, так і оновлення.

По-друге, реалізується дистанційний доступ до застосунків. RDS дозволяє користувачам звертатися до застосунків як через локальну мережу, так і дистанційно. Підключення до застосунків може здійснюватися навіть за наявності обмеженої пропускної здатності каналу зв'язку – наприклад, через телефонну лінію або через розподілені канали глобальної мережі (WAN) – з використанням захищеного протоколу HTTPS.

По-третє, реалізується концепція доступності середовища Windows («Всюди ОС Windows»). Служба RDS дозволяє користувачам звертатися до потужних Windows-застосунків із безлічі різноманітних пристроїв, серед яких пристрої зі слабким апаратним забезпеченням, комп'ютери, що працюють не під управлінням ОС Windows, тонкі клієнти (термінали) та навіть мобільні пристрої.

По-четверте, підтримуються віртуальні робочі столи. Використовуючи RDS із віртуалізацією робочих столів, користувачі можуть створити власний персональний робочий стіл або отримати визначений доступ до екземпляра віртуального робочого столу з пулу віртуальних робочих столів.

Слід зазначити, що для дистанційного доступу до систем можуть використовуватися Windows XP, Windows Vista, Windows 7, Windows 8, Apple Mac та інші системи, які підтримують службу клієнтів віддалених робочих столів (Remote Desktop Client – RDC) [4].

Архітектура служби Remote Desktop Services і взаємодія з Active Directory

У контексті засобів дистанційного адміністрування технологія RDS дозволяє здійснювати керування сервером безпосередньо із серверної консолі, або ж із будь-якого іншого сервера чи робочої станції за допомогою клієнта RDS, який у попередніх версіях мав назву клієнта служби терміналів (Terminal Services Client). За замовчуванням функціонал віддаленого робочого столу встановлюється в системі, проте не активується. Його застосування дозволяє суттєво спростити процедуру адміністрування серверів для IT-

підрозділів, надаючи персоналу можливість виконувати роботу практично з будь-якої консолі, підключеної до корпоративної мережі. Такий підхід сприяє зменшенню часу реакції IT-персоналу на запити, пов’язані з доступом до мережевих ресурсів або управлінням обліковими записами користувачів. Задачі супроводу серверів, такі як перегляд журналів подій або збір телеметричних даних про продуктивність, можуть бути виконані безпосередньо через цього клієнта. Також під час сеансу віддаленого робочого столу може бути здійснено встановлення застосунків та їх оновлень.

Служба Remote Desktop Services характеризується високою корисністю для користувачів з багатьох причин, серед яких виділяються можливість зниження витрат компанії на апаратне забезпечення, спрощення доступності застосунків та управління ліцензіями, а також підвищення загальної продуктивності мережі. Оскільки сеанс Remote Desktop фактично є віддаленим сеансом, що виконується на хості сеансів віддаленого робочого столу, всі користувачі виконують застосунки безпосередньо на цьому сервері Windows, використовуючи його обчислювальну потужність, що зменшує навантаження на локальні робочі станції. Це дозволяє продовжити термін експлуатації застарілого обладнання шляхом використання процесорних потужностей, оперативної пам’яті та дискової підсистеми сервера [19].

З точки зору супроводу робочих середовищ, хост сеансів віддаленого робочого столу може бути встановлений та застосований як вторинний засіб для забезпечення доступу користувачів до необхідних застосунків у разі виникнення проблем на локальних робочих станціях. Хоча такий сценарій потрібен не завжди, він може виявитися критично важливим для підтримки продуктивної роботи та стабільності доходу компанії у випадках, коли персонал супроводу відсутній або не може оперативно усунути проблеми на стороні кінцевих пристроїв. Надання централізованих застосунків за допомогою служби RDS спрощує управління програмним забезпеченням, зменшуючи кількість машин, на яких необхідно проводити модернізацію, оновлення безпеки та впровадження оперативних виправлень. Оскільки всі застосунки виконуються на хості сеансів, зміни вносяться лише на ньому, стаючи одночасно доступними для всього колективу користувачів.

Служба RDS також може застосовуватися для підтримки застосунків кінцевих користувачів безпосередньо у сеансі віддаленого робочого столу. Під час роботи користувачів адміністратором можуть бути налаштовані можливості дистанційного управління або спостереження для перегляду або повної взаємодії із сеансом користувача. Ця функціональність застосовується для навчання персоналу, супроводу застосунків або внесення змін у конфігурацію, таких як встановлення принтерів або підключення до спільних мережевих файлових ресурсів. Це суттєво знижує потребу в фізичній присутності адміністраторів, оскільки допомога багатьом користувачам може надаватися з єдиного

центру. Слід зазначити, що для забезпечення сумісності з політиками безпеки та конфіденційності багатьох організацій, у службі RDS передбачено можливість повного відключення функції дистанційного управління. Альтернативно, службу можна сконфігурувати так, щоб користувачі самостійно надавали дозвіл на взаємодію адміністратора з їхнім сеансом.

Встановлення ролі служби RDS забезпечує доступ до застосунків та служб користувачам незалежно від їхнього місцезнаходження. Це особливо актуально для постачальників хмарних служб та компаній, що пропонують послуги через власні застосунки, дозволяючи стандартизувати роботу виключно через RDS. Додатковою перевагою є зниження витрат на доставку носіїв із ПЗ кожному клієнту та можливість надання кваліфікованої підтримки. Постачальники хмарних служб за допомогою RDS можуть обслуговувати тисячі користувачів з різних організацій, стягуючи плату за використання застосунків або час сеансу [3].

Механізм роботи віддаленого робочого столу дозволяє користувачам підключатися до віддаленої машини та отримувати доступ до застосунків або всього робочого столу. Для ініціювання сеансу зв’язку між клієнтом і сервером призначений клієнт підключення до віддаленого робочого столу (Remote Desktop Connection – RDC).

Клієнт RDC використовує багатоканальний протокол Remote Desktop Protocol (RDP), який є розширенням сімейства протоколів ITU T.120. За замовчуванням підключення RDP використовують TCP-порт 3389, а при використанні шлюзу віддалених робочих столів (Remote Desktop Gateway) – TCP-порт 443 (HTTPS) [3].

Під час роботи з RDP події миші та клавіатури перенаправляються з клієнта на віддалену машину, де RDP використовує власний драйвер для отримання цих подій. Для відображення дій користувача RDP застосовує свій відеодрайвер, який оформлює зображення у мережеві пакети для відправки назад клієнту RDC, де вони перетворюються на відповідні виклики API інтерфейсу графічних пристроїв (GDI) Microsoft Win32 [3].

RDP підтримує багатоканальний режим, використовуючи окремі віртуальні канали для передачі повідомлень пристроїв, візуальних даних та зашифрованих даних вводу, підтримуючи до 64 000 окремих каналів. Також підтримується групова передача даних для трансляції інформації кільком клієнтам у реальному часі без дублювання трафіку [4].

Віддалений робочий стіл може функціонувати у двох режимах: Remote Desktop for Administration (для адміністрування) та Remote Desktop Services (служба віддалених робочих столів). Режим адміністрування підтримується операційними системами Windows Server (зокрема версією 2025) і встановлюється разом із ними, потребуючи лише активації. Це полегшує розгортання автоматизованих серверів без локальної консолі та віртуальних гостьових сеансів, зменшуючи потребу в периферійному обладнанні (моніторах, клавіатурах)

на користь додаткової оперативної пам’яті. Цей режим обмежує кількість сеансів до двох паралельних підключень (плюс консольний сеанс) і доступний лише локальним адміністраторам, не вимагаючи додаткових ліцензій. Режим адміністрування можна увімкнути через групову політику, PowerShell або вручну, і він доступний у всіх версіях Windows Server та клієнтських системах професійних редакцій.

Режим Remote Desktop Services дозволяє будь-якому авторизованому користувачеві підключитися до сервера для запуску застосунків або повного сеансу. Для функціонування цього режиму необхідно придбати ліцензію клієнтського доступу (Client Access License – CAL) RDS для кожного одночасного підключення. Управління цими ліцензіями здійснюється через сервер ліцензування віддалених робочих столів (Remote Desktop Licensing), який може бути встановлений на редакціях Windows Server Standard, Enterprise або Datacenter. Перед впровадженням застосунків у середовищі RDS необхідно провести ретельну перевірку їхньої роботи у багатосеансовому режимі для виявлення проблем сумісності та необхідності застосування спеціальних сценаріїв налаштування [3].

На стороні клієнта операційні системи Windows (Vista, 7, 8, 10, 11) містять усічену версію служби Remote Desktop, що дозволяє дистанційне керування робочою станцією та виконання програм, які зазвичай працюють локально. Це також використовується як засіб адміністрування для налаштування параметрів профілю користувача. Крім того, компонент «Віддалений помічник» (Remote Assistance), що з’явився у Windows Server 2003, дозволяє користувачам надсилати запит на допомогу адміністратору. При цьому користувач керує рівнем доступу помічника (чат, перегляд, повне управління). Обидві сторони можуть мати контроль над клавіатурою та мишею, використовуючи протокол RDP. Клієнт підключення до віддаленого робочого столу (Remote Desktop Connection) надає кінцевому користувачеві можливість керувати параметрами сеансу, такими як перенаправлення локальних дисків, аудіо та портів, а також зберігати конфігурацію підключення для подальшого використання [4].

Основні ролі RDS: RD Session Host, RD Connection Broker, RD Web Access, RD Gateway, RD Licensing

Хост сеансів віддалених робочих столів (Remote Desktop Session Host, або RD Session Host) використовується для розміщення Windows-застосунків або повного робочого столу Windows для користувачів, які підключаються до RD Session Host, використовуючи клієнт RDC або застосунок RemoteApp.

Функціональні можливості ролі RD Session Host включають механізм справедливого використання розподілених ресурсів. У попередніх версіях термінальної служби політика планування у планувальнику Windows розподіляла час процесора порівну між усіма

потоками одного рівня пріоритету. Така методика запобігала монопольному захопленню ресурсів процесора будь-яким користувачем, однак вона не могла рівномірно розподіляти час процесора на основі динамічних навантажень. Для оптимізації роботи з динамічними навантаженнями компонент Fair Share CPU Scheduling (Справедливе планування розподілених ресурсів процесора) у службі RDS використовує механізм планування Windows Server рівня ядра для динамічного розподілу процесорного часу між сеансами залежно від кількості сеансів та їхнього навантаження. Окрім засоби розподілу процесорного часу, в системі наявні засоби справедливого розподілу мережі та дискового приводу [4].

Засіб розподілу мережі динамічно розподіляє пропускну здатність мережі між гостьовими сеансами на основі кількості активних гостьових сеансів. Засіб розподілу дискового приводу рівномірно розподіляє операції дискового введення-виведення між сеансами для запобігання монополізації диска одним або кількома сеансами.

У Windows Server управління розгортанням та конфігуруванням здійснюється централізовано з консолі диспетчера серверів. Замість налаштування окремих серверів диспетчер серверів дозволяє налаштувати одночасно всі ролі RDS – це називається колекцією сеансів (раніше – ферма RDS). Централізація розгортання та налаштування забезпечує зв’язок між серверними ролями, такими як RD Web, RD Connection Broker та RD Session Hosts. Крім того, при налаштуванні кількох серверів для хостів сеансів, брокерів тощо створюються зв’язки для балансування навантаження, резервування та колективного налаштування. Налаштування, на яке адміністратори раніше витрачали кілька годин, тепер виконується за хвилини з диспетчера серверів у межах однієї системи [3].

Спрощено не лише створення сеансу RDS, а й адміністрування та управління серверами RDS. Управління загальними налаштуваннями серверів брокерів, веб-серверів тощо виконується з однієї консолі диспетчера серверів, що значно полегшує супровід однотипних конфігурацій у однотипних серверних системах.

Окрім централізованого розгортання та адміністрування, у RDS реалізовано можливість централізації параметрів профілів користувачів та налаштувань персоналізації за допомогою дисків профілів користувачів (User Profile Disks). Раніше параметри налаштовувалися конкретно в локальних профілях на термінальному сервері або сервері RDS, і кожен сервер мав власні параметри. Завдяки дискам профілів конфігурації слідують за користувачами незалежно від того, до якого сервера RDS підключено користувача.

Служба хоста віртуалізації віддалених робочих столів (Remote Desktop Virtualization Host) у поєднанні із сервером Hyper-V забезпечує розміщення віртуальних машин для сеансів клієнтів Windows. Користувачі можуть підключатися до віртуальної машини за допомогою технології RemoteApp and Desktop Connection або Remote Desktop Web Access. Такі віртуальні машини можуть бути розгорнуті як персональний віртуальний робочий стіл

(кожному користувачеві призначається унікальна віртуальна машина) або як частина загального пулу віртуальних робочих столів (віртуальна машина виділяється динамічно). При використанні служби ролі для хоста віртуалізації RD також встановлюється сервер Hyper-V [3].

Персональні віртуальні робочі столи призначаються індивідуальним користувачам за допомогою диспетчера підключень (Remote Desktop Connection Manager). Користувачеві може призначатися лише один віртуальний робочий стіл, а віртуальний робочий стіл може бути призначений лише одному користувачеві. Зберігаючи відношення «один до одного», всі налаштування, виконані користувачем на персональному робочому столі, зберігаються і доступні для майбутнього використання.

На противагу цьому, пул віртуальних робочих столів призначений для збереження одних і тих самих налаштувань користувача для всіх віртуальних робочих столів, незалежно від того, до якого з них користувач підключений у даний момент. Для цього всі віртуальні машини з пулу мають бути сконфігуровані ідентично. У пулах можна задати відкат змін до попереднього стану після виходу користувача.

Для перенаправлення користувача на коректну віртуальну машину вузол RD Virtualization Host використовує брокер підключень (Remote Desktop Connection Broker). Якщо користувачеві призначено персональний робочий стіл, брокер перенаправляє запит на відповідну віртуальну машину (запускаючи її за потреби). При підключенні до розділюваного пулу брокер виконує наступні дії: якщо користувач вже має відключений сеанс, запит перенаправляється до цього сеансу; якщо ні – динамічно призначається машина з пулу.

Служба ролі шлюзу віддалених робочих столів (Remote Desktop Gateway) дозволяє користувачам звертатися до мережевих ресурсів (хости сеансів RD, віртуальні машини або комп’ютери з RDS), розташованих за брандмауерами у приватній мережі, з будь-якого клієнта в Інтернеті (або внутрішніх клієнтів, якщо TCP-порт 3389 обмежено). Для цього шлюз застосовує SSL-ретрансляцію (SSL VPN), дозволяючи клієнтам підключатися через захищене шифроване з’єднання HTTPS (TCP-порт 443), всередині якого передається трафік RDP [3].

Шлюз RD був впроваджений компанією Microsoft у відповідь на практику блокування трафіку RDP (TCP 3389) підрозділами інформаційної безпеки. Рішення SSL VPN, вбудоване в служби RDS, дозволяє користувачам отримувати доступ незалежно від їхнього розташування. Оскільки сервер шлюзу RD використовує HTTPS, потрібне встановлення сертифіката автентифікації сервера, випущеного центром сертифікації (CA), якому довіряють клієнти (публічний або внутрішній довірений CA) [3].

При використанні шлюзу RD необхідно враховувати наступні вимоги.

Має бути встановлена служба віддаленого виклику процедур через HTTP-проксі (RPC over HTTP Proxy).

Для функціонування RPC over HTTP Proxy необхідна служба Internet Information Services (IIS).

На існуючому сервері NPS, який використовується шлюзом, має бути встановлена служба мережевих політик (Network Policy Server – NPS).

Сервери та клієнти можуть бути налаштовані на використання захисту мережевого доступу (NAP).

Для політик авторизації необхідна служба Active Directory Domain Services (AD DS).

Компонент RD Gateway підтримується на клієнтах під управлінням Windows XP SP2 / Windows Server 2003 SP1 або новіших версій із встановленим клієнтом RDC.

Служба ролі веб-доступу до віддалених робочих столів (Remote Desktop Web Access) дозволяє користувачам (внутрішнім та дистанційним) звертатися з веб-сайту до застосунків RemoteApp, робочих столів на основі сеансів або віртуальних робочих столів. Використовуючи RD Web Access, користувач отримує єдиний консолідований список опублікованих ресурсів з хоста або ферми хостів. Ця роль особливо корисна для централізованого розгортання програм зі спеціальної веб-сторінки або сайту SharePoint. Для використання RD Web Access клієнти повинні мати браузер Internet Explorer 6.0 або новіший та службу RDC, що підтримує протокол RDP версії 6.1 або вище [4].

Еволюція цього компонента почалася з засобу Session Directory (Каталог сеансів) у Windows Server 2003, який згодом був перейменований у TS Session Broker у Windows Server 2008 з додаванням балансування навантаження. У Windows Server 2012 і пізніших версіях компонент отримав назву RD Connection Broker. Ця служба ролі виконує балансування навантаження та гарантує підключення користувачів до правильних сеансів (робочих столів на основі сеансів, віртуальних робочих столів та програм RemoteApp). При встановленні ролі RD Connection Broker також автоматично встановлюється служба RD Web Access [4].

Сервер брокера зберігає у локальній базі даних інформацію про всі сеанси (розташування, стан, ID сеансу, ім’я користувача). Використовуючи цю інформацію, брокер перенаправляє користувачів до вже існуючих сеансів на коректному сервері. При нових підключеннях брокер намагається адекватно розподіляти навантаження між серверами ферми залежно від їхніх вагових коефіцієнтів та реального навантаження.

Для конфігурування балансування навантаження необхідно створити запис типу A або AAAA для кожного хоста RD у фермі (Round Robin DNS). Ім’я хоста встановлюється за іменем ферми. Після початкового підключення та аутентифікації на одному з хостів, сервер надсилає запит брокеру для прийняття рішення про перенаправлення. Остаточний хост обирається на основі двох рішень: наявність існуючого сеансу (перенаправлення до нього) або вибір найменш завантаженого сервера для нового сеансу.

Ліцензії клієнтського доступу до служб віддалених робочих столів (RDS CALs)

необхідні користувачам та пристроям для доступу до сервера RD Session Host (RDSH), який дозволяє віддалені підключення до робочих столів та застосунків. Сервер ліцензування RDS відіграє ключову роль в управленні цими ліцензіями, їх видачі та відстеженні використання в мережі. За замовчуванням Windows Server дозволяє два одночасних сеанси віддаленого робочого столу без додаткового ліцензування (режим адміністрування). Для організацій, яким потрібно більше двох підключень, необхідно придбати додаткові RDS CAL.

Доступні такі типи ліцензій:

RDS Device CAL (Ліцензія клієнтського доступу пристрою RDS), яка допускає використання одного пристрою (будь-яким користувачем) для звернення до функцій служби.

RDS User CAL (Ліцензія клієнтського доступу користувача RDS), що дозволяє одному користувачеві (з будь-якого пристрою) звертатися до функцій служби.

RDS External Connector (Зовнішній з'єднувач RDS) – дозволяє кільком зовнішнім користувачам звертатися до єдиного сервера.

SPLA (Лицензійна угода постачальників служб) – надає постачальнику послуг гнучке рішення для ліцензування ряду організацій.

Для налаштування сервера ліцензування RDS у середовищі Windows Server 2025 спочатку необхідно встановити роль RDS на сервері. Після цього слід вибрати «Remote Desktop Licensing» (Ліцензування віддалених робочих столів) як службу ролі, як зображено на рисунку 8.2. Це налаштування гарантує, що сервер зможе видавати відповідну кількість ліцензій для забезпечення потреб організації у віддаленому доступі.

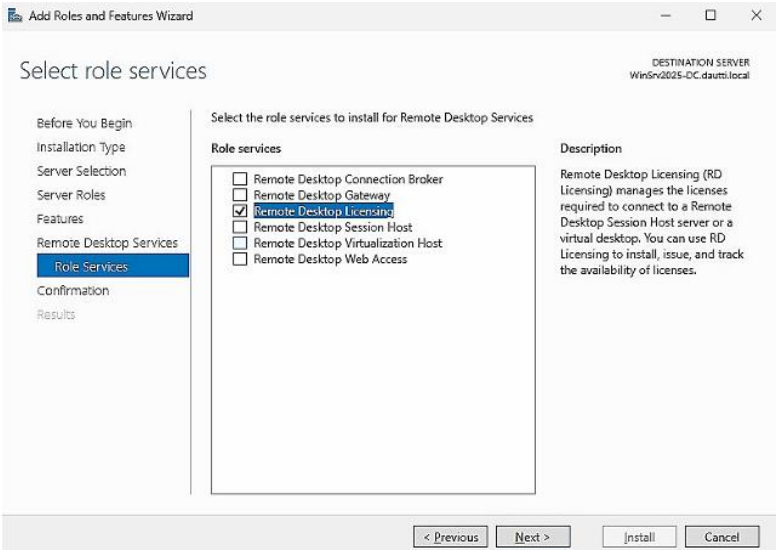

Рисунок 8.2 – Додавання служб ролі ліцензування віддалених робочих столів у Windows Server 2025 [3]

Крім того, критично важливо регулярно переглядати та керувати RDS CAL для забезпечення відповідності ліцензійним угодам та уникнення перебоїв у наданні послуг.

Процес автентифікації користувачів через Active Directory та авторизація доступу до віддалених сесій

Забезпечення захищеного доступу до корпоративних ресурсів у середовищі Windows Server 2025 базується на інтегрованій взаємодії служби віддалених робочих столів (RDS) із службою каталогів Active Directory (AD DS). Ця взаємодія розгортається у двох послідовних площинах: автентифікації – процесі верифікації цифрової ідентичності суб'єкта, та авторизації – процедурі перевірки прав підтвердженого суб'єкта на доступ до конкретного об'єкта системи. Архітектура безпеки RDS спроектована таким чином, щоб винести процес перевірки облікових даних за межі графічного сеансу сервера, що реалізується через механізм автентифікації на рівні мережі.

У сучасних версіях Windows Server стандартним є використання автентифікації на рівні мережі (Network Level Authentication – NLA). Ця технологія вимагає успішного завершення процедури автентифікації користувача ще до моменту виділення сервером ресурсів для створення графічного інтерфейсу сеансу. Технічна реалізація NLA покладається на протокол CredSSP (Credential Security Support Provider), який забезпечує інкапсуляцію облікових даних та їх безпечну передачу через захищений канал [3].

Процес автентифікації проходить наступні етапи.

Перше – це ініціалізація з'єднання. На цьому етапі клієнтське програмне забезпечення (MSTSC) ініціює запит на підключення до сервера RDS. На цьому етапі між клієнтом і сервером встановлюється захищений тунель TLS (Transport Layer Security) для запобігання перехопленню даних.

Друге – це делегування облікових даних. Клієнт вводить облікові дані на локальному пристрої. CredSSP шифрує ці дані та передає їх серверу RDS через встановлений TLS-тунель. Важливо зазначити, що сервер RDS ще не створює сеанс RDP.

Третє – це верифікація в Active Directory. Сервер RDS, отримавши зашифровані дані, виступає в ролі посередника і звертається до контролера домену Active Directory. Використовуючи протокол Kerberos (або NTLM як резервний варіант), сервер перевіряє валідність наданої пари логін/пароль та статус облікового запису.

І останній – четвертий етап – це підтвердження, під час якого контролер домену повертає серверу RDS відповідь про успішність автентифікації. Лише після отримання позитивного підтвердження сервер RDS дозволяє подальше встановлення RDP-з'єднання та завантаження профілю користувача.

У доменному середовищі Active Directory пріоритетним протоколом автентифікації є Kerberos версії 5. Його критичною перевагою для RDS є забезпечення взаємної автентифікації. Це означає, що не лише сервер перевіряє користувача, але й клієнтський комп'ютер перевіряє справжність сервера RDS перед передачею йому будь-якої інформації.

Клієнт звертається до центру розподілу ключів (KDC) на контролері домену із запитом на отримання службового квитка для конкретного SPN (Service Principal Name) сервера RDS. Якщо сервер є підробленим (атака типу спуфінг), клієнт не зможе отримати коректний квиток або розшифрувати відповідь сервера, і з'єднання буде розірвано автоматично [3].

Після успішної автентифікації (підтвердження, що користувач є тим, за кого себе видає) система переходить до етапу авторизації (визначення, чи має цей користувач право на вхід). У Windows Server 2025 авторизація базується на списках контролю доступу (ACL) та членстві у групах безпеки.

Основним бар'єром авторизації є локальна група безпеки «Користувачі віддаленого робочого столу» (Remote Desktop Users) на сервері хоста сеансів (RD Session Host). Операційна система перевіряє ідентифікатор безпеки (SID) користувача або груп, до яких він належить. Якщо SID користувача не знайдено в ACL слухача RDP або в локальній групі дозволених користувачів, доступ відхиляється із відповідним повідомленням, навіть якщо пароль був правильним [3].

У сценаріях розгортання ферми серверів із використанням брокера підключень (RD Connection Broker), авторизація набуває додаткового рівня – рівня колекції сеансів. Брокер підключень перевіряє конфігурацію колекції, щоб з'ясувати, чи дозволено конкретному користувачеві доступ до цього логічного об'єднання ресурсів. Це дозволяє розмежувати доступ різних департаментів до різних пулів серверів у межах одного домену.

Адміністрування процесів автентифікації та авторизації виконується через стандартні графічні інтерфейси Windows Server 2025. Для забезпечення належного рівня безпеки адміністратор повинен виконати наступні налаштування на кожному хості сеансів або централізовано через диспетчер серверів.

Для активації NLA адміністратор використовує панель «Властивості системи» (System Properties). Необхідно відкрити вкладку «Віддалений доступ» (Remote). У секції «Віддалений робочий стіл» (Remote Desktop) здійснюється вибір опції «Дозволяти підключення тільки з комп'ютерів, на яких працює віддалений робочий стіл з автентифікацією на рівні мережі» (Allow connections only from computers running Remote Desktop with Network Level Authentication). Встановлення цього прапорця змушує сервер відхиляти будь-які спроби підключення від клієнтів, що не підтримують CredSSP, або спроби анонімного ініціювання сеансу [3].

Налаштування авторизації на рівні локального хоста здійснюється за наступним алгоритмом. Надання прав доступу конкретним користувачам Active Directory здійснюється шляхом їх додавання до локальної групи безпеки сервера. Використовуючи оснастку «Керування комп'ютером» (compmgmt.msc), адміністратор переходить у розділ «Локальні користувачі та групи» – «Групи» та відкриває властивості групи «Remote Desktop Users».

Згідно з кращими практиками, до цієї локальної групи додаються не окремі облікові записи користувачів, а глобальні групи безпеки домену (наприклад, «Domain RDS Access Group»). Це забезпечує масштабованість управління: при появі нового співробітника його достатньо додати до групи в Active Directory, і він автоматично отримає доступ до всіх серверів ферми.

Якщо розгорнуто роль RD Connection Broker, управління доступом здійснюється через консоль «Диспетчер серверів» (Server Manager). У розділі «Служби віддалених робочих столів» – «Колекції» адміністратор обирає необхідну колекцію і у меню «Властивості» переходить до вкладки «Групи користувачів» (User Groups). Тут вказуються групи Active Directory, яким дозволено підключатися до цієї колекції. Брокер підключень використовує цей список як фільтр. Якщо користувач успішно пройшов автентифікацію NLA, але не входить до зазначених груп колекції, брокер відмовить у перенаправленні сеансу на хост [3].

Інтеграція політик групової безпеки для контролю доступу й обмеження ресурсів

У масштабних корпоративних інфраструктурах ручне налаштування параметрів безпеки та продуктивності на кожному хості сеансів (RD Session Host) розглядається як неефективний підхід, що є потенційно небезпечним через ризик виникнення «дрейфу конфігурації». Для забезпечення уніфікації налаштувань, централізованого керування доступом та оптимізації використання системних ресурсів у середовищі Windows Server 2025 застосовується механізм об’єктів групових політик (GPO) служби каталогів Active Directory. Інтеграція RDS з GPO дозволяє адміністраторам формувати детерміноване середовище, де права користувачів, параметри сеансів та рівень доступу до периферійних пристроїв чітко регламентовані на рівні організаційних одиниць (OU).

Важливим аспектом налаштування GPO для термінальних ферм є розуміння режиму обробки замикання. За стандартною логікою Active Directory, політики конфігурації користувача застосовуються залежно від того, в якій організаційній одиниці знаходиться об’єкт облікового запису користувача. Однак у контексті RDS часто виникає потреба застосовувати специфічні обмеження, наприклад, заборону доступу до панелі керування або приховування дисків, лише тоді, коли користувач входить на термінальний сервер, залишаючи його права на локальному пристрої без змін. Для вирішення цієї задачі в Windows Server 2025 використовується режим «Налаштування режиму обробки замикання політики групи користувача» (Configure user Group Policy loopback processing mode). Ця політика активується в розділі «Конфігурація комп’ютера» для об’єкта GPO, прив’язаного до OU з серверами RDS [3].

Згадана політика передбачає два режими функціонування, вибір між якими залежить від архітектурних вимог до системи. Перший режим, «Режим злиття» (Merge), передбачає об’єднання списків політик користувача: спочатку застосовуються політики з OU

користувача, а потім – політики з OU сервера, причому в разі конфлікту пріоритет надається політикам сервера. Другий варіант, «Режим заміни» (Replace), ігнорує політики, визначені для об’єкта користувача в його рідній OU, і застосовує виключно налаштування користувача, визначені в GPO, що прив’язаний до сервера RDS. Саме «Режим заміни» є рекомендованим для ізольованих термінальних середовищ, оскільки він забезпечує повну передбачуваність поведінки системи та усуває вплив налаштувань локальних робочих станцій на серверне середовище [3].

Однією з головних проблем використання спільних ресурсів сервера є накопичення «завислих» або неактивних сеансів, які продовжують споживати оперативну пам’ять та процесорний час. Засоби GPO в Windows Server 2025 надають гранулярний контроль над життєвим циклом RDP-сеансу через адміністративні шаблони компонентів Windows у розділі обмеження сеансів за часом. Ключові параметри налаштування включають встановлення обмеження часу для відключених сеансів, що визначає період збереження сеансу в пам’яті після розриву з’єднання, після чого сеанс примусово завершується для вивільнення ресурсів. Також налаштовується обмеження часу для активних, але бездіяльних сеансів, яке регулює допустимий час відсутності активності користувача перед автоматичним відключенням. Параметр завершення сеансу при досягненні ліміту часу визначає кінцеву дію системи: просте відключення з можливістю відновлення або повне завершення процесів користувача, що є рекомендованим для серверів з високим навантаженням.

З точки зору інформаційної безпеки, канал RDP може використовуватися для несанкціонованого виведення корпоративних даних на локальні пристрої користувача, тому Windows Server 2025 дозволяє адміністраторам жорстко обмежити можливості перенаправлення (Redirection) через відповідний розділ GPO. Найважливіші політики обмеження включають заборону перенаправлення буфера обміну, що блокує копіювання даних між сервером та локальним комп’ютером, створюючи ізольований контур. Дуже важливою є також заборона перенаправлення дисків, яка унеможливлює відображення локальних дисків клієнта у сеансі сервера, запобігаючи завантаженню шкідливого програмного забезпечення та вивантаженню конфіденційних документів. Додатково рекомендується відключати перенаправлення портів COM та LPT для мінімізації поверхні атаки через застарілі інтерфейси.

Окрім адміністративних шаблонів, групові політики керують базовими правами безпеки через призначення прав користувача в локальних політиках. Адміністратор повинен сконфігурувати параметр «Дозволити вхід через службу віддалених робочих столів» (Allow log on through Remote Desktop Services). На практиці реалізується наступний алгоритм: створюється спеціалізована група безпеки в Active Directory (наприклад, RDS_Access_Users), після чого створюється об’єкт GPO, прив’язаний до OU з хостами сеансів. У політиці

дозволу входу явно вказується група Адміністраторів та новостворена цільова група, тоді як група «Користувачі» (Users) видаляється зі списку для запобігання неавторизованому доступу. Для створення ешелонованого захисту додатково може бути налаштована політика «Відхилити вхід через службу віддалених робочих столів» (Deny log on through Remote Desktop Services), куди додаються сервісні облікові записи та акаунти з високими привілеями. Такий підхід забезпечує централізований контроль, де надання доступу зводиться до маніпуляцій з групами AD, а безпека автоматично гарантується механізмами оновлення політик [3].

Переваги використання RDS у доменних середовищах, типові проблеми та методи їх усунення

Інтеграція служб віддалених робочих столів (RDS) у середовище Active Directory (AD) забезпечує фундаментальні архітектурні переваги, які є недосяжними при використанні моделі робочої групи. Ключовою перевагою є реалізація технології єдиного входу (Single Sign-On – SSO), яка базується на протоколі Kerberos.

У правильно спроектованій інфраструктурі Windows Server 2025, де клієнтські станції та сервери є членами одного домену, користувач проходить процедуру автентифікації лише один раз – при вході на локальний пристрій. Подальший доступ до віддалених застосунків або робочих столів відбувається шляхом прозорого обміну квитками Kerberos, що значно підвищує зручність роботи та зменшує ризик компрометації паролів через їх багаторазове введення. Крім того, доменна структура дозволяє використовувати централізований аудит подій безпеки, що забезпечує наскрізне відстеження активності користувача від моменту отримання квитка TGT (Ticket Granting Ticket) до завершення сесії на хості RDS [3].

Наступною важливою перевагою є можливість побудови відмовостійких конфігурацій високої доступності. Функціонування брокера підключень у режимі кластеризації можливе виключно за умови наявності доменної бази даних для зберігання інформації про сеанси, що у Windows Server 2025 часто реалізується через SQL Server. Це дозволяє системі балансувати навантаження між серверами та автоматично відновлювати доступ користувачів до розірваних сеансів навіть у разі виходу з ладу одного з вузлів брокера. Без інтеграції з Active Directory неможливе коректне функціонування механізмів перенаправлення користувачів та динамічного розподілу віртуальних робочих столів (VDI), оскільки відсутній єдиний простір імен та довірених сертифікатів.

Попри значні переваги, експлуатація складних інфраструктур RDS супроводжується низкою типових проблем, серед яких чільне місце займають помилки ліцензування. Часто спостерігається ситуація, коли після завершення 120-денного пільгового періоду користувачі втрачають доступ до системи з повідомленням про відсутність доступних ліцензій, навіть

якщо сервер ліцензування розгорнуто. Ця проблема зазвичай виникає через некоректну конфігурацію механізму виявлення сервера ліцензій. У доменному середовищі хости сеансів можуть автоматично шукати сервери ліцензій через об’єкти Service Connection Point (SCP) в Active Directory, проте в складних мережевих топологіях цей процес може давати збої. Для усунення цієї проблеми рекомендується явно задавати адресу сервера ліцензування та тип ліцензій (на користувача або на пристрій) через групові політики або командлети PowerShell, а також використовувати інструмент RD Licensing Diagnoser для перевірки зв’язку та наявності встановлених пакетів CAL.

Іншою поширеною категорією проблем є помилки сертифікатів та довіри при підключенні. Користувачі можуть отримувати попередження про те, що ідентичність віддаленого комп’ютера неможливо підтвердити, або про невідповідність імені сертифіката. Це явище часто зумовлене використанням внутрішніх доменних імен (наприклад, .local) для доступу з зовнішніх мереж, де очікується публічне ім’я (наприклад, .com).

У Windows Server 2025, де вимоги до безпеки посилено, такі невідповідності блокуються жорсткіше. Вирішення полягає у впровадженні інфраструктури розділеного DNS, що дозволяє внутрішнім та зовнішнім клієнтам звертатися до ресурсів за одним і тим самим повним доменним ім’ям (FQDN), на яке видано довірений сертифікат від публічного або корпоративного центру сертифікації. Також необхідно забезпечити, щоб сертифікат був коректно призначений на всіх рівнях: для ролей RD Connection Broker, RD Web Access та RD Gateway.

Проблеми з профілями користувачів, зокрема при використанні дисків профілів користувачів (User Profile Disks – UPD) або технології FSLogix, проявляються у завантаженні тимчасового профілю замість персонального. Це відбувається, коли віртуальний диск з профілем (VHDX) залишається заблокованим попереднім сеансом, який не був коректно завершений («завислий» процес logoff). В результаті система не може примонтувати диск для нового входу. Для діагностики та усунення таких збоїв адміністраторам необхідно використовувати моніторинг файлових дескрипторів на файловому сервері, де зберігаються профілі, та примусово закривати відкриті з’єднання до заблокованих файлів VHDX. Крім того, важливо налаштувати виключення антивірусного сканування для файлів контейнерів профілів, оскільки антивірус може блокувати доступ до диску під час сканування, викликаючи тайм-аут завантаження профілю [3].

Нарешті, проблеми з перенаправленням підключень часто виникають у фермах з балансуванням навантаження. Симптоматика проявляється у неможливості користувача повторно підключитися до свого існуючого відключеного сеансу, адже система створює новий сеанс на іншому сервері або видає помилку підключення. Причиною зазвичай є некоректне налаштування DNS або відсутність доступу клієнта до IP-адреси цільового хоста

сеансів. Алгоритм роботи брокера передбачає, що після первинного звернення клієнт отримує токен перенаправлення на конкретний IP хоста. Якщо клієнт знаходиться за межами корпоративної мережі і не використовує шлюз RD Gateway, він не зможе встановити пряме з'єднання з внутрішньою IP-адресою хоста. Вирішенням є обов'язкове використання шлюзу RD Gateway для зовнішніх підключень та налаштування параметра «Use Redirection Server Name» у властивостях колекції, що змушує клієнта використовувати FQDN замість IP-адреси при перенаправленні.

Тема 9
Реалізація нових удосконалень безпеки у Windows Server 2025

Базові механізми захисту ОС

Починаючи з випуску Windows Server 2003, корпорація Microsoft оголосила безпеку найважливішим пріоритетом для розробників продукту Windows Server, а також для багатьох інших команд розробників. Тому всі наступні версії операційної системи містили та містять численні зміни, покликані підвищити безпеку Windows Server, серед яких режим Core Edition, встановлення на основі ролей, служба оновлення Windows Server, AppLocker та багато інших. У Windows Server 2025 ця тенденція продовжується завдяки вдосконаленню функціональності таких засобів, як динамічне керування доступом та архітектура надійного завантаження.

Безпека на серверному рівні розглядається як одне з найважливіших понять для мережевого середовища. Сервери в інфраструктурі не тільки виконують критичні мережеві служби, на кшталт системи доменних імен (DNS), протоколу динамічного конфігурування хостів (DHCP), пошуку в каталогах та автентифікації, але й є централізованим місцем зберігання більшості, а то й усіх, критичних файлів у мережі організації. Тому так важливо скласти план забезпечення безпеки на серверному рівні та повністю розібратися в можливостях захисту Windows Server 2025 [3].

Після виявлення кількох вірусів, що набули широкого розповсюдження, та прогалин у безпеці, було розроблено ініціативу, що отримала назву Trustworthy Computing («Надійні обчислення»). Ця ініціатива вилилася у підвищену увагу до питань безпеки у всіх технологіях Microsoft. Кожен рядок коду Windows Server досліджується на предмет наявності можливих вразливих місць, а увага була перенесена з розробки нових можливостей на забезпечення безпеки. Про значення цієї ініціативи для користувачів технології Microsoft можна судити з того, що в самій корпорації безпека стала головним пріоритетом при розробці, а Windows Server 2025 продовжує вже майже десятилітню традицію застосування цієї концепції. Весь код продуктів перевіряється всередині процесу, який називається загальномовним виконуючим середовищем (Common Language Runtime – CLR). Це середовище виконує код програми, автоматично перевіряючи його на наявність прогалин у безпеці, які можуть бути викликані помилками програмування. Крім того, ретельно перевіряються повноваження, використовувані цими фрагментами, щоб переконатися, що код виконує тільки потрібні дії. Обмежуючи за допомогою цих технологій можливості зловживань та зменшуючи вразливість програмного забезпечення, середовище Common Language Runtime знижує загальний ризик безпеки Windows Server [3].

Заходи безпеки найбільш ефективні, коли вони застосовуються за рівнями. Наприклад, пограбувати будинок значно важче, якщо грабіжникові потрібно не тільки зламати парадні

двері, а й впоратися зі сторожовим собакою та відключити домашню охоронну систему. Це ж стосується і безпеки сервера: система безпеки повинна складатися з декількох рівнів, щоб складність її зламу зростала експоненціально.

У Windows Server 2025 органічно поєднуються безліч необхідних рівнів безпеки, в яких використовуються автентифікація Kerberos, захист файлів NTFS і вбудовані засоби безпеки, забезпечуючи таким чином готову систему безпеки. Для застосування додаткових компонентів безпеки необхідно розуміти особливості їх функціонування, а також встановити та сконфігурувати їх елементи. Система дозволяє додавати додаткові рівні безпеки та надає організаціям посилений захист без шкоди для функціональних можливостей.

Один з найбільш часто недооцінюваних, але, можливо, найбільш важливих компонентів безпеки сервера – реальна фізична безпека самого сервера. Найнадійніший веб-сервер, що не піддається зламу, безсилий, якщо зловмисник може просто відключити його від мережі. Ще гірше, якщо будь-хто, увійшовши в систему важливого файлового сервера, зможе скопіювати секретні файли або вивести комп'ютер з ладу.

Фізична безпека є обов'язковою умовою для будь-якої організації, оскільки саме з нею найчастіше пов'язана поява прогалин у системі безпеки. Незважаючи на це, у багатьох організаціях рівні фізичної безпеки важливих для виробничої діяльності серверів легко долаються або зовсім відсутні.

Отже, неодмінною умовою забезпечення безпеки є розуміння того, що потрібно для захисту фізичного та логічного доступу до сервера. Сервери повинні бути захищені фізично, тобто встановлені в приміщенні, що замикається, з контрольованим доступом. Критичні для виробничого процесу сервери не варто поміщати біля ніг адміністраторів або в інших ненадійних місцях. Ідеальним з точки зору безпеки сервера середовищем є спеціальне приміщення або постійно замкнена шафа. Більшість компаній-виробників обладнання постачають свої вироби механізмами для фізичного блокування деяких або всіх компонентів сервера. Залежно від застосування інших рівнів безпеки може бути доцільним використовувати такі механізми для захисту середовища сервера.

Всі сервери повинні конфігуруватися так, щоб тільки адміністратори мали фізичний доступ до консолі для входу в систему. За замовчуванням це обмеження використовується в контролерах доменів, але на інших серверах – файлових серверах, допоміжних серверах та аналогічному обладнанні – такі типи входу в систему повинні бути спеціально заборонені. Щоб обмежити вхід у систему, виконується певна послідовність дій. Спочатку відкривається Диспетчер серверів і обирається пункт меню Tools – Local Security Policy (Сервіс – Локальна політика безпеки). У панелі вузлів необхідно знайти вузол Security Settings – Local Policies – User Rights Assignment (Параметри безпеки – Локальні політики – Призначення прав користувачів). Далі двічі клацається на елементі Allow Log On Locally (Дозволити локальний

вхід у систему). На цьому етапі видаляються всі користувачі та групи, яким не потрібен доступ до сервера, після чого натискається кнопка ОК. Слід зауважити, що право доступу Allow Log On Locally можна встановити для всього домену або організаційної одиниці (OU) за допомогою групової політики домену, однак цей механізм дозволяє видавати права користувачам або групам, але не відбирати їх. Для заборони локального входу користувачам або групам за допомогою групової політики призначено право доступу Deny Log On Locally (Заборонити локальний вхід) [3].

У найбільш захищених інфраструктурах для дозволу входу в систему застосовуються так звані смарт-карти, які повністю підтримуються у Windows Server 2025. Смарт-карти бувають різної форми, зазвичай це пластикова картка розміром з візитівку з вбудованим у неї мікрочіпом і USB-роз'ємом. Кожному користувачеві видається унікальна картка і відповідний PIN-код. Вхід у робочу станцію зводиться до вставки картки в спеціальний зчитувальний пристрій і введення PIN-коду, який може бути комбінацією цифр і букв на зразок пароля. Безпеку можна підвищити ще більше, вимагаючи автоматичного виходу користувача з консолі при вилученні смарт-карти. У такій ситуації користувачі вставляють у зчитувальний пристрій смарт-карту, закріплену на одязі за допомогою ланцюжка або шнурка. Після введення PIN-коду вони входять у систему і виконують усі необхідні дії. Після цього користувачі просто витягують картку зі зчитувального пристрою, що призводить до автоматичного виходу із системи робочої станції. У такому випадку практично неможливо забути вийти з системи, оскільки користувач, відходячи від комп'ютера, повинен фізично від'єднатися від нього [3].

Забезпечення безпеки кабелів завжди було складним завданням, але тенденція використання бездротових мереж ускладнила її ще більше. Багато організацій були вражені тим, якої шкоди може завдати мережі особа, що має можливість підключитися через мережевий порт. Поява бездротових мереж ще більше спрощує доступ. Наприклад, зловмисник може просто під'їхати на автостоянку і отримати доступ до локальної мережі організації за допомогою ноутбука і звичайної карти бездротового зв'язку.

Стандартний спосіб захисту – Wi-Fi Protected Access (Захист доступу через Wi-Fi, WPA), що використовується в багатьох бездротових мережах – значно кращий, ніж початкові рішення, але він все одно ненадійний, як і будь-яке рішення на основі загальнодоступного пароля або ключа. Управління мережевими портами та захист мережевих комутаторів є частиною стратегії безпеки. В організаціях з бездротовими мережами необхідно вживати більш суворих заходів безпеки. Впровадження бездротових мереж, в яких використовується протокол 802.1x, значно підвищує рівень мережевої безпеки. Microsoft використовує цей протокол для захисту своєї бездротової мережі, і Windows Server повністю підтримує його. Організації, яким не вистачає часу або ресурсів для впровадження протоколу 802.1x, можуть

ефективно захистити бездротову мережу, просто розмістивши точки бездротового доступу зовні брандмауера і вимагаючи доступ по віртуальній приватній мережі (Virtual Private Network – VPN) через брандмауер. Навіть якщо зловмисник зможе роздобути спільний ключ, йому вдасться підключитися тільки до загальнодоступної мережі, що не має виходу в решту мережі.

Залежно від розмірів організації, сервер може бути призначений для виконання однієї або декількох мережевих ролей. Планування розгортання ролей – важливе і складне заняття, при якому слід враховувати доступне обладнання, сумісність ролей, очікувані навантаження, безліч корисних порад і рекомендацій та міркування безпеки. Одним з інструментів підвищення гнучкості та масштабованості в процесі проєктування є Hyper-V. Платформа віртуалізації, яка входить до складу клієнта і сервера Windows Server 2025, дозволяє забезпечити наявність декількох виділених гостьових систем на меншій кількості фізичних хостів. Оскільки будь-яка увімкнена служба підвищує ступінь загального ризику, важливо точно визначити, які ролі виконуватиме сервер, щоб належним чином сконфігурувати відповідні служби. Хоча ці компоненти можна встановити вручну, процес налаштування служб спрощується за допомогою майстра конфігурування сервера.

Після визначення переліку ролей, які виконуватиме сервер, ідеальним засобом активізації цих ролей та їх захисту може служити утиліта Server Manager (Диспетчер серверів). За замовчуванням, якщо сервер є DNS-сервером, але не виконує функції файлового сервера і сервера друку, Server Manager не тільки відкриває порти, потрібні для DNS, але й блокує всі спроби доступу до файлів або принтерів цього сервера. Вікно диспетчера серверів Windows Server 2025 дозволяє дозволити виконання на сервері окремих ролей. Після цього таким ролям дозволяється виконання, і на сервері відкриваються потрібні для їх виконання порти.

ОС Windows Server встановлюється з базовими можливостями та використовує модель управління серверними ролями для мінімізації площі вразливості системи, одночасно дозволяючи системі виконувати свої функції. Однак навіть у такому базовому варіанті є компоненти, які можуть розширити площу вразливості, і не є обов’язковими для роботи багатьох мережевих середовищ, на зразок файлових серверів або серверів DNS – це графічний інтерфейс, Internet Explorer і додатки .NET. Крім знайомої редакції з усіма можливостями, яка також називається Server Graphical Shell (Графічна оболонка сервера), у Windows Server є й кілька інших мінімалістських моделей роботи. Кожна така модель жертвує якимось аспектом функціональності для скорочення вразливості сервера. Для налаштування різних режимів роботи введено два компоненти: Server Graphical Shell (Графічна оболонка сервера) і Graphical Management Tools and Infrastructure (Інструменти та інфраструктура графічного управління). Видалення Server Graphical Shell переводить систему

в мінімальний серверний інтерфейс (Minimal Server Interface), в якому немає робочого столу і провідника Windows, але є PowerShell і багато різних засобів графічного управління. Деякі з них можна видалити для подальшого скорочення площі вразливості [4].

Щоб мінімізувати площу вразливості, ще в попередні версії операційної системи було введено режим Core Edition (Базова редакція), який можна вказати під час установки. У Windows Server є певна кількість керованого коду, в основному це PowerShell і підмножина .NET Framework. Важливим доповненням у Core Edition є можливість встановити в системі повний графічний інтерфейс на основі оболонки Server Graphical Shell. Для цього необхідно виконати такі команди PowerShell: Import-Module Dism, а потім Enable-WindowsOptionalFeature -online -Featurename ServerCore-FullServer, Server-Gui-Shell, Server-Gui-Mgmt. Режим Core Edition дуже зручний для серверних ролей – Hyper-V, доменної служби Active Directory, файлового сервера, сервера друку тощо. Це більш захищена платформа, яка не тільки скорочує площу вразливості, але й вимагає менше ресурсів і виправлень, а також простіше адмініструється за допомогою дистанційних інструментів і консолей.

Файли в Windows Server 2025 безпечні лише на стільки, на скільки для них визначені права доступу. Тому важливо зазначити, що Windows Server не надає групі Everyone (Всі користувачі) повний контроль над правами доступу рівня загальних ресурсів і рівня NTFS. Крім того, критичні файли та каталоги операційної системи захищені від їх несанкціонованого використання. Незважаючи на наявність загальних удосконалень, рекомендується ретельно розібратися в безпеці на файловому рівні, щоб не знизити безпеку сервера на цьому рівні. У Windows Server введена файлова система ReFS (Resilient File System – стійка файлова система), яка має зворотну сумісність з NTFS. Але оскільки ця нова файлова система також орієнтована на цілісність даних, масштабованість, надійність і легкість управління, механізми безпеки в ній не дуже відрізняються від попередніх версій продукту. Кожен об’єкт, на який є посилання в ReFS, зокрема файли та папки, помічається в списку контролю доступу (Access Control List – ACL), який фізично обмежує коло користувачів, що мають доступ до ресурсу. Права доступу файлів і папок використовують цю концепцію для жорсткого управління доступом на читання, запис та інші типи доступу до файлів [3].

Файлові сервери повинні обґрунтовано застосовувати права доступу рівня файлів і папок, і слід перевірити права доступу у всіх каталогах для виявлення можливих прогалин або незахищених ресурсів. Зміна прав доступу ReFS у Windows Server – простий процес. Для цього клацають правою кнопкою миші на папці або файлі, до якого потрібно застосувати налаштування безпеки, і вибирають у контекстному меню пункт Properties (Властивості). Далі переходять на вкладку Security (Безпека) і клацають на кнопці Advanced (Додатково).

Потім натискають кнопку Disable Inheritance (Скасувати успадкування). При появі повідомлення про застосування батьківських прав доступу вибирають варіант Remove All Inherited Permissions from This Object (Видалити всі успадковані права доступу у цього об'єкта). У діалоговому вікні Advanced Security Settings (Додаткові налаштування безпеки) натискають кнопку Add (Додати), щоб дозволити доступ групам та/або користувачам, яким потрібно звертатися до файлів або папок. Необхідно відзначити прапорець Replace All Child Object Permissions with Inheritable Permissions from This Object (Замінювати права у всіх об'єктах-нащадках на права, успадковані від цього об'єкта) і натиснути кнопку ОК. При появі запиту про заміну безпеки дочірніх об'єктів натискають кнопку Yes (Так), а потім підтверджують зміни, натискаючи ОК у відповідних вікнах.

Технологія BitLocker для шифрування дисків (BitLocker Drive Encryption) продовжує вдосконалюватися і в Windows Server 2025. Останні випуски містять кілька компонентів, які перетворюють цю технологію на зручний інструмент для серверів. Можливість додаткового захисту на фізичному рівні не завадить у середовищах із підвищеними вимогами до безпеки або в особливих умовах. Такі можливості BitLocker можуть бути цікаві адміністраторам серверів або захисту інформації: підтримка BitLocker для кластеризованих дисків (в тому числі для кластерів із підхопленням функцій і загальнодоступних кластерних томів); швидка підготовка (більш швидка початкова підготовка з можливістю шифрування лише зайнятої дискової пам'яті, більш швидке розгортання на основі інтеграції шифрованих томів у процес створення образів); мережеве розблокування (у поєднанні з технологією TPM дозволяє автоматично розблокувати сервер у корпоративній мережі, але вимагати введення пароля, якщо він не підключений до корпоративної мережі); а також покращені аудит і події BitLocker [35].

У нашому небезпечному світі сервер безпечний рівно настільки, наскільки безпечні виконувані на ньому програми. Тим не менш, Windows Server 2025 є найбільш безпечною операційною системою сімейства Windows і містить безліч вбудованих механізмів забезпечення безпеки сервера. Однак усі механізми захисту марні, якщо спеціально або випадково шкідливе ПЗ буде встановлено на сервер. Тому необхідні заходи щодо захисту сервера від такого ПЗ. Необхідно також ретельно продумувати політики безпеки та передбачати можливі наслідки від прогалин у безпеці. Реалізація ефективних і надійних процедур резервного копіювання та відновлення – ключова умова для відновлення та захисту даних.

Віруси – одна з найбільш серйозних небезпек для сервера. Багато вірусів написані спеціально для використання основних вразливостей в інфраструктурі сервера. Інші заражають файли, які можуть зберігатися на сервері, поширюючи інфекцію серед клієнтів, що завантажують ці файли. Тому вкрай важливо подумати над застосуванням засобів

антивірусного захисту всіх файлових серверів мережі підприємства. Всі основні виробники антивірусних програм включають у свої пакети надійні сканери файлового рівня, і ці сканери слід використовувати на всіх файлових серверах. Сама Microsoft випустила лінійку антивірусних продуктів, тісно інтегрованих із серією Windows Server. Їхньою перевагою є те, що в них одночасно працюють кілька антивірусних механізмів. Таким чином, якщо один із цих механізмів не зможе виявити вірус або користується не оновленою базою даних, то існує висока ймовірність, що цей вірус буде виявлений одним з інших механізмів. Для підтримки баз даних і засобів виявлення вірусів на сучасному рівні слід розробити чіткий план. Оскільки поява нового вірусу може призвести до хаосу в усьому світі за лічені дні і навіть години, доцільно перевіряти наявність оновлень як мінімум щодня [35].

У Windows Server з'явився новий набір компонентів із загальною назвою «Архітектура надійного завантаження» (Trusted Boot Architecture) або «Архітектура цілісності платформи» (Platform Integrity Architecture). Ці компоненти не вимагають втручання адміністратора, але надають значне поліпшення в захисті серверів проти шкідливого ПЗ, особливо низькорівневих загроз на кшталт руткітів і буткітів. Тепер у кожну інсталяцію Windows Server 2025 входять певні компоненти безпеки [3].

По-перше, це безпечне завантаження (Secure boot) – це означає, що операційна система завантажується тільки за допомогою підписаного надійного завантажувача. Цей завантажувач вимагає перевірку підпису від наступних компонентів. Така додаткова перевірка призначена для захисту від буткітів, які намагаються змінити процес завантаження.

По-друге, захисна передзагрузка (Anti-Malware preboot) – це означає, що спочатку завантажувач ОС завантажує сумісне захисне ПЗ, а вже потім будь-які сторонні драйвери і пакети. Як і інші завантажувальні компоненти, захисний драйвер повинен бути підписаний і надійний.

По-третє, зважене завантаження (Measured boot) – у процесі захищеного процесу завантаження в TPM записуються стан і метрики клієнта. Захисний клієнт може звернутися до цього запису і використовувати його для зміни процесу завантаження і вивантаження даних на спеціальний сервер для аналізу.

Процедура резервного копіювання є надзвичайно необхідною для файлового сервера і вимагає, щоб копіювання даних на пристрій зберігання даних виконував користувач, який має відповідні повноваження. Ця вимога гарантує, що ніхто сторонній не зможе скопіювати стан середовища і понести з собою резервну копію файлів чи системи. Тому всі пристрої, що містять резервні копії серверів, повинні охоронятися настільки ж ретельно, як і сам сервер.

Налаштування міжмережного екрану

Впровадження конфігурації з брандмауером підприємства визначається як обов'язкова

вимога в будь-якому середовищі, що має підключення до мережі Інтернет. Сервери або робочі станції, які безпосередньо підключені до глобальної мережі, розглядаються як першочергові об’єкти для спроб несанкціонованого втручання. Сучасні реалізації брандмауерів, подібні до Forefront Threat Management Gateway (TMG) від корпорації Microsoft, допускають застосування розширених налаштувань, таких як конфігурація проксі-сервера та демілітаризованої зони (DMZ). Правильне встановлення та конфігурування брандмауера, розміщеного між мережею під керуванням Windows Server 2025 та Інтернетом, є обов’язковою умовою забезпечення безпеки інформаційної інфраструктури [4].

До складу операційної системи Windows Server 2025 входить суттєво вдосконалений вбудований брандмауер, який за замовчуванням увімкнений у всіх інсталяціях продукту. Цей компонент, адміністрування якого здійснюється через оснастку MMC (Microsoft Management Console), шлях до якої пролягає через меню Server Manager – Tools – Windows Firewall with Advanced Security (Диспетчер серверів – Сервіс – Брандмауер Windows з посиленим захистом), забезпечує безпрецедентні можливості з управління та захисту сервера.

Брандмауер з посиленим захистом повністю інтегрований з утилітою Server Manager (Диспетчер серверів) та майстром додавання ролей і компонентів (Add Roles and Features Wizard) (рис. 9.1).

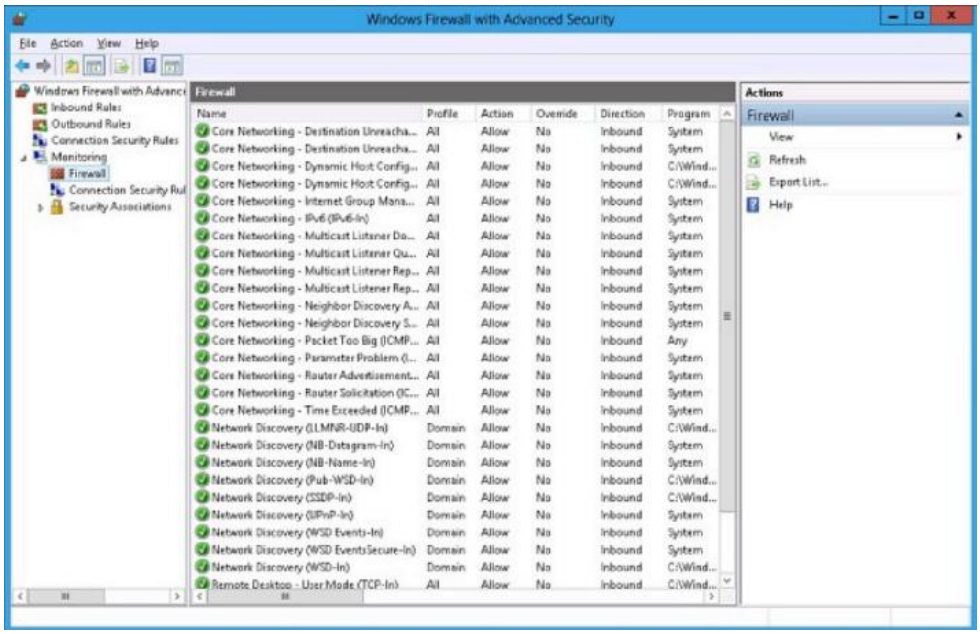

Рисунок 9.1 – Правила моніторингу в брандмауері Windows з посиленим захистом [4]

Наприклад, якщо адміністратор запустить майстер додавання ролей і компонентів та вкаже, що комп’ютер повинен функціонувати як файловий сервер, то після завершення процесу на сервері будуть автоматично відкриті лише ті порти та протоколи, які необхідні для забезпечення доступу до файлового сервера. Варто зазначити, що більшість адміністраторів раніше майже рефлекторно відключали на серверах програмні брандмауери,

оскільки в минулому їх використання супроводжувалося численними проблемами. Однак у середовищі Windows Server 2025 виконувати такі дії не рекомендується, оскільки сам продукт тісно інтегрований зі своїм брандмауером, який забезпечує значно вищий ступінь захисту порівняно з попередніми версіями операційної системи.

У деяких випадках, зокрема якщо сторонній додаток не інтегрований з брандмауером або виникає потреба відкрити конкретний порт, може знадобитися створення спеціальних правил брандмауера для забезпечення роботи окремих служб. Система дозволяє створювати як вхідні правила для трафіку, що надходить на сервер, так і вихідні правила для вихідних даних. Формування правил здійснюється на основі низки факторів.

По-перше, правило може базуватися на програмі. Можна створити правило, що дозволяє доступ конкретній виконуваній програмі (наприклад, вказати, що файл c:\Program Files\Custom Program\myprogram.exe під час виконання має повний вихідний доступ), при цьому брандмауер дозволить цій програмі виконувати будь-які типи підключень. Це корисно, якщо сервер додатків використовує кілька портів зі змінними номерами.

По-друге, правило може базуватися на порті. Підтримується вказівка традиційного порту UDP або TCP у майстрі додавання правил (Add Rules Wizard) для стандартних ситуацій, наприклад, відкриття порту 8787.

По-третє, існують попередньо визначені правила. У Windows Server наявні вбудовані правила для AD DS, DFS, BITS, HTTP тощо. Перевага їх використання полягає в тому, що розробники вже виконали роботу з налаштування, хоча деякі з них недоступні без встановлення відповідної ролі.

По-четверте, підтримується створення спеціальних типів правил, які не входять до інших категорій.

Як приклад процедури налаштування, розглядається створення вихідного правила, що дозволяє спеціалізованому додатку використовувати TCP-порт 8787 для вихідних повідомлень. Процес розпочинається з відкриття консолі управління брандмауером Windows з посиленим захистом за шляхом: Server Manager – Tools – Windows Firewall with Advanced Security. Далі у панелі вузлів обирається відповідний вузол правил (у контексті прикладу – для вихідного трафіку), а в панелі Actions (Дії) здійснюється перехід за посиланням New Rule (Створити правило). На сторінці Rule Type (Тип правила) майстра створення вихідного правила (New Outbound Rule Wizard) обирається варіант Port (Порт) для створення правила на основі порту, після чого виконується перехід до наступного кроку (рис. 9.2) [4].

На сторінці Protocol and Ports (Протокол і порти) вказується варіант TCP, а в полі Specific Local Ports (Конкретні локальні порти) вводиться номер 8787, після чого натискається кнопка Next (Далі) (рис. 9.3).

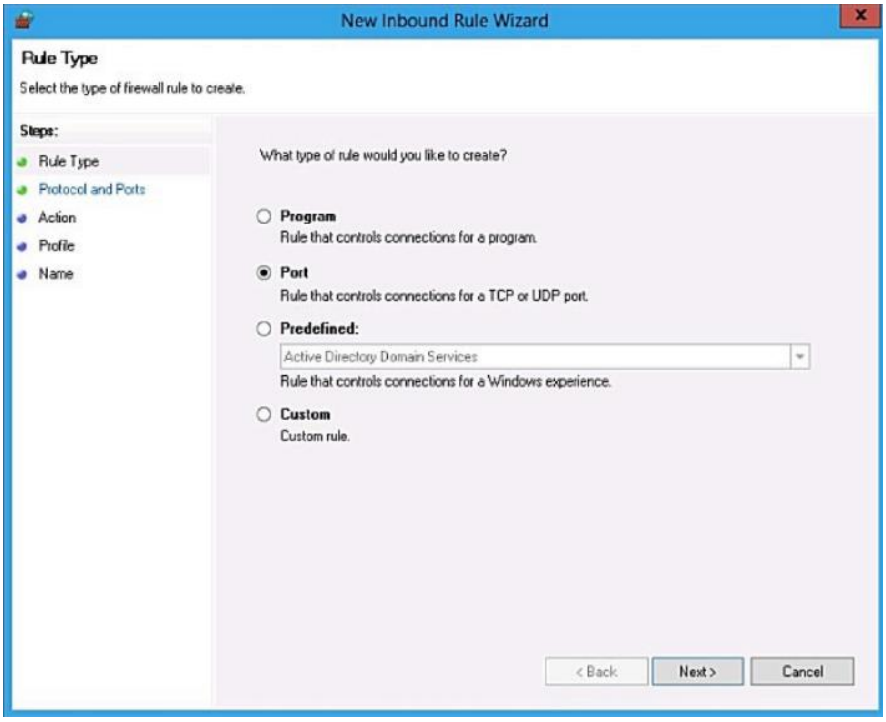

Рисунок 9.2 – Створення правила для брандмауера Windows [4]

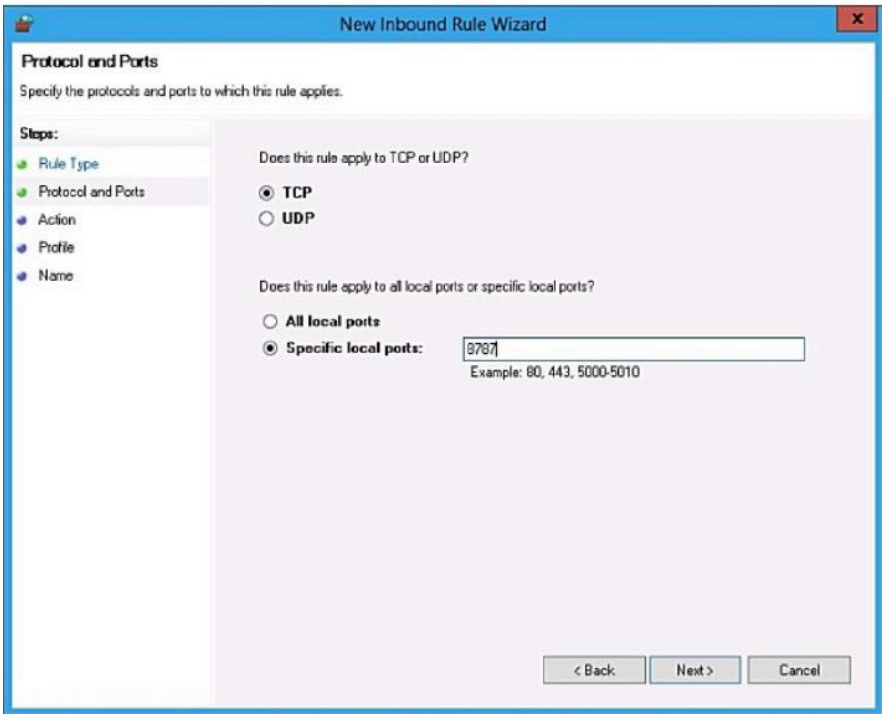

Рисунок 9.3 – Введення інформації про порт для правила брандмауера [4]

На наступній сторінці Action (Дія) обирається варіант Allow the Connection (Дозволити підключення) для активізації з'єднання. Слід зауважити, що сторінка Action майстра дозволяє також сконфігурувати правило, яке уможливлює підключення лише в тому випадку, якщо воно захищене за допомогою технологій IPSec. На сторінці Profile (Профіль) встановлюються всі три прапорці, що дозволяє адміністратору вказати застосування правила при підключенні до конкретних мереж [4].

Завершується процес введенням описового імені для правила та натисканням кнопки Finish (Готово). Параметри створеного правила можна переглянути у відповідному вузлі списку правил. Також існує можливість включити правило в групу правил, щоб об’єднати кілька правил для полегшення їх спільного дозволу або заборони.

Контроль облікових записів

У сучасному динамічному цифровому середовищі попит на передові системи автентифікації та авторизації для контролю облікових записів став критичнішим, ніж будь-коли. Оскільки організації дедалі більше покладаються на цифрові платформи для обробки конфіденційних даних та управління операціями, захист доступу до цих ресурсів є вкрай важливим. Впровадження складних механізмів автентифікації та авторизації не лише посилює безпеку, але й підвищує ефективність доступу користувачів та загальну якість обслуговування.

Біометрична автентифікація, яка є інноваційним аспектом сучасних стратегій безпеки, пропонує надійний та безвідмовний метод перевірки особи користувача, що значно перевершує традиційні системи. На відміну від паролів або PIN-кодів (які можна забути, викрасти або скомпрометувати), біометрична автентифікація використовує унікальні фізіологічні або поведінкові риси, такі як відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока та голосові патерни (рис. 9.4). Ці риси за своєю природою важко відтворити, що робить біометричні системи винятково ефективними у запобіганні несанкціонованому доступу та значному зниженні ризику крадіжки особистих даних [3].

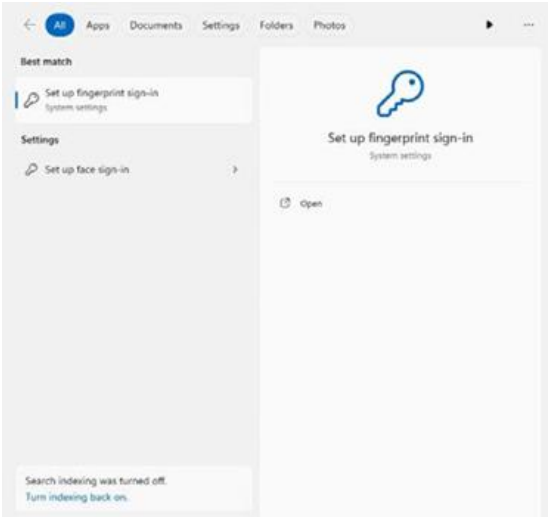

Рисунок 9.4 – Налаштування входу за відбитком пальця та розпізнаванням обличчя у Windows Server 2025 [3]

Інтеграція біометричної автентифікації у Windows Server 2025 являє собою значний

крок уперед у посиленні IT-безпеки. Використовучи біометричні модальності, адміністратори можуть гарантувати, що доступ до конфіденційних даних і систем обмежений лише авторизованими особами, забезпечуючи як посилену безпеку, так і користувацький досвід, який є не лише безшовним та інтуїтивно зрозумілим, але й зручним для користувача. Це усуває потребу запам'ятовувати складні паролі або покладатися на фізичні токени безпеки, спрощуючи процес автентифікації при збереженні суворих протоколів безпеки.

Однією з визначних особливостей біометричної автентифікації є її здатність забезпечувати безперервну перевірку в реальному часі. На відміну від статичних облікових даних, які можуть бути використані зловмисниками після їх отримання, біометричні дані залишаються прив'язаними до особи, що дозволяє проводити постійну валідацію під час активних сесій. Ця унікальна можливість є інструментальною у пом'якшенні інсайдерських загроз, коли зловмисні дії можуть виконуватися особами, які спочатку мали легітимний доступ.

Windows Server 2025 також вирішує питання конфіденційності та безпеки, пов'язані з біометричними даними, за допомогою передових методів шифрування. Захист біометричних шаблонів є критичним, оскільки будь-яка компрометація може мати далекосяжні наслідки. Використовуючи протоколи безпечного зберігання та передачі, платформа гарантує, що біометрична інформація залишається захищеною від перехоплення або втручання. Крім того, біометрична автентифікація безшовно інтегрується з багатофакторною автентифікацією (MFA), додатково посилюючи безпеку шляхом додавання ще одного рівня захисту. У поєднанні з іншими методами автентифікації, такими як смарт-карти або одноразові паролі, біометрія зміцнює захист організації навіть від найскладніших атак. Цей багаторівневий підхід гарантує, що якщо один фактор буде скомпрометовано, інші заходи безпеки залишаться неушкодженими [3].

З операційної точки зору біометрична автентифікація спрощує керування доступом для IT-адміністраторів. Централізовані консолі у Windows Server 2025 дозволяють легко реєструвати та керувати біометричними даними, забезпечуючи послідовне дотримання політик безпеки. Адміністратори можуть швидко відкликати або оновлювати біометричні облікові дані, підвищуючи реагування на потенційні загрози безпеці та гарантуючи гнучкість операцій безпеки. Прийняття біометричної автентифікації у Windows Server 2025 відображає перспективний підхід до IT-безпеки, поєднуючи передові технології зі зручністю використання. Оскільки кіберзагрози стають дедалі складнішими, розгортання біометричної автентифікації надає організаціям потужний інструмент для захисту цифрових активів, одночасно підвищуючи зручність для користувачів та операційну ефективність. Ця стратегічна інтеграція посилює загальну стійкість IT-середовищ, роблячи її вирішальним компонентом сучасних структур кібербезпеки.

Для забезпечення надійної безпеки та зручного контролю доступу впровадження біометричної автентифікації передбачає виконання кількох ключових кроків. Ці дії допомагають налаштувати необхідне обладнання, зареєструвати користувачів та інтегрувати біометричну автентифікацію з іншими заходами безпеки, такими як MFA. Дотримання цього процесу гарантує захист конфіденційних даних організації при забезпеченні безшовного користувацького досвіду.

Процес розпочинається з налаштування біометричних пристроїв, що передбачає встановлення та конфігурацію біометричного обладнання, сумісного з Windows Server 2025, наприклад сканерів відбитків пальців або камер розпізнавання обличчя. Наступним етапом є реєстрація користувачів за допомогою консолі управління Windows Server шляхом захоплення їхніх біометричних даних, що передбачає реєстрацію унікальних рис кожного користувача для уможливлення автентифікації. Завершальним етапом є інтеграція з MFA, що поєднує біометричну автентифікацію з багатофакторною автентифікацією для додавання додаткового рівня безпеки, гарантуючи, що користувачі повинні підтвердити свою особу кількома методами [3].

Політики умовного доступу у Windows Server 2025 пропонують динамічний та високозахищений метод управління доступом до організаційних ресурсів. Ці політики дозволяють IT-адміністраторам запроваджувати деталізований контроль на основі різноманітних факторів у реальному часі, включаючи ідентичність користувача, відповідність пристрою вимогам, географічне розташування та рівні ризику. Оцінюючи ці умови, система гарантує, що лише належним чином автентифіковані та авторизовані користувачі отримують доступ до конфіденційних систем та даних, що значно знижує ймовірність несанкціонованого входу та потенційних порушень безпеки. Ключовою перевагою політик умовного доступу є їхня здатність вибірково застосовувати MFA на основі контекстних факторів (рис. 9.5).

Рисунок 9.5 – Багатофакторна автентифікація в Azure [3]

Наприклад, якщо користувач намагається отримати доступ до ресурсів із пристрою,

що відповідає вимогам, у межах довіреної мережі, система може не вимагати додаткових етапів автентифікації. Однак, якщо спроба доступу здійснюється з невідомого пристрою або місця, може бути примусово застосована MFA для додавання додаткового рівня безпеки. Ця адаптивна модель підвищує загальну безпеку, зберігаючи при цьому безшовний досвід користувача шляхом коригування вимог автентифікації відповідно до рівня ризику, пов'язаного з кожною спробою доступу. Ці політики додатково посилюються завдяки їх інтеграції з іншими передовими функціями безпеки в Windows Server 2025, включаючи розвідку загроз та системи автоматизованого реагування. Ця інтеграція в реальному часі дозволяє приймати рішення про доступ на основі найновіших даних про загрози, дозволяючи системі автоматично коригувати контроль доступу у відповідь на виникаючі ризики. У сценаріях високого ризику політики умовного доступу можуть посилювати заходи безпеки, такі як вимога суворішої автентифікації або навіть блокування доступу, для проактивного захисту від потенційних загроз [3].

Адміністратори можуть легко налаштовувати та керувати цими політиками через централізовану консоль, що спрощує розгортання та забезпечення виконання в усій організації. Цей уніфікований підхід до управління забезпечує послідовне застосування стандартів безпеки. Водночас здатність генерувати детальні звіти про дії доступу та виконання політик надає цінну інформацію для оцінки безпеки та аудиту відповідності. Використовуючи політики умовного доступу, організації можуть впровадити інтелектуальну та високоадаптивну структуру контролю доступу, яка інтегрує контекстну інформацію з передовими функціями безпеки. Цей підхід не лише посилює захист критичних цифрових активів, але й покращує операційну ефективність та зручність для користувачів, роблячи його життєво важливим компонентом будь-якої сучасної стратегії кібербезпеки.

Налаштування політик умовного доступу передбачає створення правил, які забезпечують контроль доступу на основі даних у реальному часі. Визначаючи умови та встановлюючи політики, адміністратори можуть гарантувати, що доступ до конфіденційних систем надається лише за безпечних обставин, що відповідають вимогам. Цей підхід допомагає підтримувати баланс між безпекою та зручністю для користувача. Процес конфігурації розпочинається з визначення умов, за яких доступ має бути надано або обмежено, що може включати ролі користувачів, відповідність пристроїв вимогам та географічне розташування. Наступним кроком є створення політик за допомогою Windows Admin Center (WAC) для забезпечення виконання правил доступу на основі визначених умов, що гарантує доступ до чутливих систем і даних лише авторизованим користувачам. Завершальним етапом є моніторинг та коригування, що передбачає регулярний перегляд ефективності цих політик та внесення змін на основі нових даних розвідки загроз або змін в організаційних потребах.

OAuth, також відомий як Open Authorization (Відкрита Авторизація), є відкритим стандартом, розробленим для делегування доступу. Він часто використовується для надання веб-сайтам або додаткам обмеженого доступу до ресурсів користувача без розкриття їхніх облікових даних. Інтеграція OAuth 2.0 у Windows Server 2025 представляє значний стрибок у сучасних стандартах автентифікації, забезпечуючи високозахищену та гнучку структуру для управління авторизацією. Використовуючи OAuth 2.0, додатки можуть запитувати обмежений доступ до облікових записів користувачів через службу HTTP, забезпечуючи сильний контроль доступу без зайвої складності (рис. 9.6). Це налаштування дозволяє IT-адміністраторам ефективніше захищати організаційні ресурси, знижуючи ризики та спрощуючи взаємодію з користувачами [3].

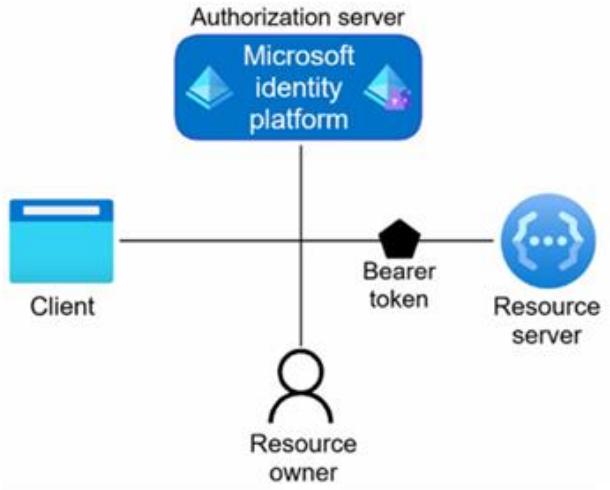

Рисунок 9.6 – Архітектура Oauth [3]

З OAuth 2.0 безпека посилюється через систему на основі токенів, яка усуває необхідність для додатків безпосередньо обробляти конфіденційні облікові дані. Цей підхід допомагає пом’якшити ризик розкриття або зловживання обліковими даними. Крім того, протокол підтримує різні методи авторизації – такі як код авторизації, неявний метод (implicit) та клієнтські облікові дані – надаючи адміністраторам гнучкість адаптувати процес автентифікації до своїх конкретних потреб. Здатність видавати тимчасові токени замість зберігання статичних облікових даних забезпечує додатковий рівень захисту від кібератак. У цьому контексті діаграма ілюструє потік автентифікації та авторизації з використанням платформи ідентичності Microsoft. Клієнт (додаток або користувач) проходить автентифікацію на сервері авторизації, який потім видає токен носія (bearer token). Цей токен пред’являється серверу ресурсів для отримання доступу до ресурсу, підтверджуючи, що клієнт був авторизований. Цей підхід на основі токенів гарантує, що лише автентифіковані та авторизовані клієнти можуть отримати доступ до захищених ресурсів, підвищуючи загальну безпеку.

Універсальність структури також сприяє взаємосумісності між різними службами та платформами, що є ключовою перевагою в сучасних взаємопов'язаних IT-середовищах. Забезпечуючи єдиний вхід (Single Sign-On – SSO), OAuth 2.0 дозволяє користувачам автентифікуватися один раз і отримувати безпечний доступ до кількох додатків без необхідності повторного введення облікових даних для кожної сесії. Ця можливість не лише підвищує ефективність, але й покращує загальну безпеку, зменшуючи кількість точок автентифікації, де можуть виникати вразливості. Підтримка OAuth 2.0 федеративного управління ідентичністю додатково дозволяє безпечну співпрацю із зовнішніми партнерами при збереженні жорсткого контролю доступу.

Прийняття OAuth 2.0 у Windows Server 2025 ілюструє перспективний підхід до захисту від сучасних кіберзагроз. Використання протоколом безпечних токенів замість традиційних постійних облікових даних зміцнює захист від атак, таких як фішинг або підбір паролів. Крім того, адміністратори отримують можливість відкликати токени та динамічно коригувати права доступу у відповідь на зміну потреб безпеки або еволюцію ризиків, забезпечуючи гнучкіше середовище безпеки. Вбудовуючи OAuth 2.0 в інфраструктуру Windows Server, IT-адміністратори отримують можливість створювати більш цілісну та безпечну екосистему. Ця інтеграція не лише підвищує безпеку через передові механізми авторизації, але й сприяє більш плавному та інтегрованому користувацькому досвіду [3].

Впровадження OAuth 2.0 передбачає налаштування структури для безпечної та ефективної обробки авторизації. Налаштовуючи OAuth 2.0 та інтегруючи його з додатками, можна гарантувати, що доступ до ресурсів контролюється за допомогою безпечних токенів. Цей процес також включає управління токенами та коригування дозволів для задоволення потреб безпеки, що змінюються. Процедура розпочинається з налаштування параметрів OAuth 2.0 у Windows Server 2025 для дозволу додаткам запитувати обмежений доступ до облікових записів користувачів, з визначенням необхідних методів авторизації, таких як коди авторизації або клієнтські облікові дані. Наступним кроком є інтеграція з додатками, що передбачає оновлення додатків для використання OAuth 2.0 для автентифікації та авторизації, забезпечуючи належну обробку токенів для підтримки безпеки. Кінцевим етапом є управління токенами, що включає моніторинг та управління виданими токенами, впровадження механізмів для відкликання та коригування дозволів у відповідь на еволюцію потреб безпеки.

Аудит подій безпеки

Аудит подій безпеки у середовищі Windows Server 2025 розглядається як елемент проактивної системи виявлення загроз. В умовах еволюції кібератак, де дедалі частіше використовуються легітимні інструменти адміністрування, архітектура аудиту в сучасній

серверній операційній системі спроектована з урахуванням принципів Zero Trust та припущень про компрометацію, що вимагає детальної фіксації активності всередині системи. Основою підсистеми реєстрації подій виступає механізм розширеної конфігурації політики аудиту (Advanced Audit Policy Configuration), який, на відміну від базових політик попередніх поколінь, забезпечує високу гранулярність налаштувань. Це дозволяє адміністраторам формувати точні правила реєстрації, мінімізуючи «інформаційний шум» у журналах та знижуючи навантаження на підсистему введення-виведення сервера. Налаштування цих параметрів здійснюється переважно через об’єкти групової політики (GPO), що забезпечує централізоване управління аудитом у масштабах усього підприємства.

Основним інструментом для безпосереднього перегляду та первинного аналізу зареєстрованих даних на локальному рівні виступає консоль Event Viewer («Переглядач подій»). Ця інтегрована оснастка MMC (Microsoft Management Console) надає структурований доступ до журналів Windows, серед яких ключовим для захисту інформації є журнал безпеки (Security Log). Event Viewer у Windows Server 2025 дозволяє не лише переглядати хронологію подій, але й виконувати складні операції фільтрації та пошуку. Для ефективної роботи з великими масивами даних застосовується механізм створення спеціальних подань, який дозволяє адміністратору сформувати вибірку подій за конкретними критеріями, такими як ідентифікатори подій (Event ID), джерела, рівні важливості або ключові слова. Крім того, Event Viewer підтримує використання XML-запитів для створення гнучких фільтрів, що дає змогу виявляти складні патерни атак, які неможливо відстежити за допомогою стандартного графічного інтерфейсу [3].

В рамках налаштування політик аудиту критична увага приділяється категоріям, що відповідають за автентифікацію та доступ до ресурсів. Зокрема, аудит входу в обліковий запис (Account Logon) дозволяє відстежувати спроби автентифікації на контролерах домену або локальних хостах, що є необхідним для виявлення атак на протокол Kerberos, таких як Golden Ticket. Паралельно з цим, аудит доступу до об’єктів забезпечує фіксацію взаємодії користувачів з критичними файловими ресурсами та ключами реєстру. У Windows Server 2025 вдосконалено алгоритми моніторингу файлової системи, що дозволяє виявляти активність шкідливого програмного забезпечення, наприклад програм-вимагачів, на ранніх етапах атаки за характерними патернами масової модифікації файлів. Також важливим є аудит зміни політик, який реєструє будь-які модифікації в налаштуваннях безпеки або довірчих відносинах домену, що часто свідчить про спроби зловмисника закріпитися в скомпрометованій системі.

Для протидії складним цільовим атакам (APT) у Windows Server 2025 реалізовано поглиблені механізми аудиту виконання коду, які вимагають активації специфічних налаштувань. Ключовим елементом тут є аудит створення процесів, зокрема реєстрація події

з ідентифікатором 4688. Критично важливим удосконаленням є опція включення командного рядка у події створення процесу, що дозволяє фіксувати не лише факт запуску виконуваного файлу, але й передані йому аргументи. Це надає можливість виявляти шкідливе використання легітимних системних утиліт. Додатково, враховуючи широке використання PowerShell зловмисниками, система інтегрує механізми аудиту скриптів, такі як Script Block Logging. Це забезпечує збереження повного тексту виконаного коду в журналі подій, оскільки реєстрація відбувається після декодування коду, але перед його виконанням [35].

Ефективність аудиту суттєво підвищується завдяки централізації збору подій, оскільки аналіз розрізнених журналів на окремих серверах через Event Viewer є часозатратним і не дає повної картини інциденту. У середовищі Windows Server 2025 активно використовується технологія Windows Event Forwarding (WEF), яка дозволяє налаштувати автоматичну передачу подій з вихідних серверів на центральний колектор. Для гібридних середовищ передбачена інтеграція з хмарними службами через агент Azure Monitor, що дозволяє експортувати події безпеки до хмарних аналітичних систем. Такий підхід забезпечує збереження цілісності журналів навіть у разі компрометації локального сервера, оскільки копії подій зберігаються у захищеному сховищі, а також відкриває можливості для застосування алгоритмів машинного навчання для кореляції подій та автоматизованого реагування на інциденти.

Інструментарій Event Viewer («Переглядач подій») у Windows Server 2025 виступає як консоль управління даними, що базується на розширюваній розмітці XML. Архітектурно журнал подій безпеки (Security Log) є унікальним серед усіх системних журналів, оскільки право запису до нього має виключно підсистема LSASS (Local Security Authority Subsystem Service). Це забезпечує цілісність даних та унеможливлює внесення фальсифікованих записів звичайними користувацькими програмами. Кожна подія в журналі представляє собою структурований об’єкт, який містить як статичні метадані (заголовок), так і динамічні змінні (тіло події), що змінюються залежно від контексту операції. Для студентів та системних адміністраторів критично важливо розуміти, що графічний інтерфейс відображає лише відрендерене подання події, тоді як її справжня сутність зберігається у форматі XML, доступ до якого відкривається через вкладку «Details» (Подробиці) [3].

Ключовим елементом аналізу безпеки є розуміння структури ідентифікаторів подій (Event IDs) та їхніх атрибутів. У Windows Server 2025 найбільш критичними для моніторингу є події категорій «Logon/Logoff» та «Process Tracking». Наприклад, подія з кодом 4624 (Успішний вхід в систему) містить критично важливий атрибут «Logon Type» (Тип входу). Значення цього атрибуту дозволяє розрізнити фізичний вхід користувача за консоллю сервера (Type 2), мережевий вхід через спільні ресурси (Type 3), запуск завдання планувальником (Type 4) або вхід через Remote Desktop Services (Type 10). Аналіз саме цього поля дозволяє

виявити аномалії, наприклад, спробу інтерактивного входу (Type 2) сервісного облікового запису, який повинен працювати виключно у фоновому режимі (Type 5). Паралельно з цим аналізується подія 4625 (Неуспішна спроба входу), де поле «Failure Reason» (Причина відмови) та «Sub Status» вказують, чи був пароль неправильним, чи обліковий запис заблокованим, або ж спроба входу відбулася у заборонений час [3].

Окремий пласт аналітики стосується моніторингу створення процесів, що є основним методом виявлення запуску шкідливого коду. Подія 4688 фіксує створення нового процесу і, за умови правильного налаштування політики аудиту, містить поле «Process Command Line» (Командний рядок процесу). Це дозволяє побачити повний шлях до виконуваного файлу та всі аргументи, передані йому при запуску. Додатково фіксується ідентифікатор батьківського процесу (Creator Process ID), що дозволяє побудувати дерево процесів і зрозуміти, яка саме програма ініціювала підозрілу активність (наприклад, якщо winword.exe запускає powershell.exe, це є класичною ознакою атаки через макроси). Також у Windows Server 2025 важливу роль відіграють події доступу до об’єктів (ідентифікатор 4663), які фіксують спроби читання, запису або видалення конкретних файлів та ключів реєстру, якщо для них налаштовано відповідні системні списки контролю доступу (SACL) [35].

Для ефективної роботи з великими масивами даних у Event Viewer реалізовано механізм фільтрації на основі XPath-запитів. Стандартні фільтри графічного інтерфейсу мають обмежені можливості, тоді як використання вкладки «XML» у діалоговому вікні «Filter Current Log» дозволяє створювати складні логічні конструкції. Наприклад, можна сформувати запит, який відображатиме лише події входу (4624) для конкретного користувача, виключаючи при цьому системні облікові записи (наприклад, ті, що закінчуються на «$»), або фільтрувати події за часовим діапазоном та IP-адресою джерела одночасно. Створені складні фільтри можуть бути збережені як «Custom Views» (Налаштовувані подання), що дозволяє адміністратору миттєво отримувати доступ до специфічних зрізів даних безпеки (наприклад, «Всі неуспішні входи з зовнішніх IP-адрес за останні 24 години») без необхідності щоразу створювати запит заново.

Важливим аспектом аудиту є захист самого журналу подій від несанкціонованого втручання. Зловмисники, отримавши адміністративний доступ, часто намагаються очистити журнал безпеки, щоб приховати сліди своєї діяльності.

Система Windows Server 2025 реєструє факт очищення журналу як подію з ідентифікатором 1102 («Журнал аудиту було очищено»). Ця подія містить інформацію про обліковий запис, який ініціював очищення, і є безумовним індикатором компрометації системи, що вимагає негайного реагування. Для запобігання втраті даних у корпоративному середовищі налаштовуються параметри ротації журналів, які визначають поведінку системи при переповненні файлу журналу – перезапис найстаріших подій або архівування повного

журналу з автоматичним створенням нового файлу. Це гарантує, що критичні докази інцидентів не будуть втрачені через обмеження дискового простору.

Практики мінімізації вразливостей

Стратегія забезпечення кіберстійкості Windows Server 2025 базується на концепції «зменшення площини атаки», яка передбачає систематичну мінімізацію кількості компонентів, служб та протоколів, доступних для потенційної експлуатації зловмисниками. Вразливість операційної системи розглядається не лише як наявність помилок у коді, але і як надлишкова функціональність, що не використовується для виконання цільових задач, проте створює додаткові вектори для проникнення. У новій версії серверної платформи реалізовано комплекс архітектурних рішень та адміністративних практик, спрямованих на превентивне усунення умов для реалізації загроз, замість реактивного реагування на інциденти.

Критично важливим нововведенням у сфері управління вразливостями є технологія Hotpatching («Гаряче виправлення»), яка набула широкого застосування у версії Windows Server 2025 та поступово інтегрується в локальні сценарії. Традиційний процес встановлення оновлень безпеки часто відкладався адміністраторами через необхідність перезавантаження сервера та переривання бізнес-процесів, що залишало системи вразливими протягом тривалого часу. Технологія Hotpatching дозволяє застосовувати виправлення безпеки безпосередньо в оперативній пам’яті працюючого процесу ядра або простору користувача без необхідності перезавантаження системи. Це досягається шляхом перенаправлення викликів функцій від старого (вразливого) коду до нового (виправленого) без зупинки роботи служб. Такий підхід гарантує, що сервер постійно захищений від відомих експлойтів, мінімізуючи «вікно вразливості» між випуском патча та його застосуванням [3].

Для нейтралізації вразливостей, пов’язаних із запуском неавторизованого або модифікованого коду, у Windows Server 2025 застосовується вдосконалений механізм Windows Defender Application Control (WDAC). На відміну від традиційних антивірусних рішень, що працюють за принципом «чорних списків» (блокування відомих загроз), WDAC реалізує модель «білих списків», дозволяючи виконання лише тих додатків, які явним чином авторизовані політикою безпеки або підписані довіреним сертифікатом. Ця практика унеможливлює експлуатацію вразливостей нульового дня через запуск шкідливого навантаження, оскільки будь-який невідомий код автоматично блокується ядром системи. У поєднанні з функцією Hypervisor-Enforced Code Integrity (HVCI), яка використовує можливості віртуалізації для ізоляції служби перевірки цілісності коду в захищеній області пам’яті, це створює надійний бар’єр проти атак, спрямованих на ін’єкцію шкідливого коду в системні процеси [3].

Окремий напрямок мінімізації вразливостей стосується захисту мережевих

комунікацій, зокрема протоколу SMB (Server Message Block), який історично був ціллю для багатьох атак (наприклад, WannaCry). У Windows Server 2025 за замовчуванням впроваджено жорсткіші налаштування безпеки, включаючи примусове шифрування SMB-трафіку та відключення застарілих версій протоколу. Важливим еволюційним кроком є впровадження SMB з QUIC, що дозволяє безпечно отримувати доступ до файлових серверів через ненадійні мережі (Інтернет) без використання VPN. Протокол QUIC забезпечує шифрування на транспортному рівні (аналогічно TLS 1.3) та стійкість до перехоплення або підміни пакетів. Це дозволяє організаціям закрити традиційні порти TCP 445 на зовнішніх периметрах, усуваючи одну з найбільш поширених точок входу для кібератак, при цьому зберігаючи зручність доступу до даних для віддалених користувачів.

Огляд нових удосконалень системи безпеки у Windows Server 2025

Windows Server 2025 впроваджує надійний набір удосконалень безпеки, спрямованих на вирішення проблем, пов'язаних зі зростаючою складністю та частотою кіберзагроз, з якими стикаються сучасні IT-інфраструктури. Ці нові функції спроектовано для забезпечення багаторівневого захисту шляхом покращення механізмів контролю доступу, використання передового виявлення загроз на базі машинного навчання та штучного інтелекту, а також впровадження високоефективних систем автоматизованого реагування. Зазначені інструменти взаємодіють для проактивної ідентифікації, запобігання та мінімізації наслідків потенційних порушень безпеки до того, як вони зможуть завдати значної шкоди. Крім того, нова структура безпеки безшовно інтегрується з існуючими політиками безпеки, що полегшує IT-адміністраторам управління та забезпечення виконання кращих практик безпеки у своїх середовищах. Зміцнюючи захист як від внутрішніх, так і від зовнішніх загроз, Windows Server 2025 гарантує, що підприємства можуть підтримувати цілісність, конфіденційність та доступність критичних систем і даних, створюючи в кінцевому підсумку більш безпечне та стійке корпоративне середовище.

Покращені засоби контролю доступу у Windows Server 2025 впроваджують трансформаційний підхід до захисту IT-середовищ. Надаючи адміністраторам високогранулярний контроль над дозволами користувачів, ці передові функції уможливлюють точне управління тим, хто може отримувати доступ до конкретних ресурсів і які дії вони можуть виконувати. Використовуючи такі технології, як управління доступом на основі ролей (RBAC) та багатофакторна автентифікація (MFA), Windows Server 2025 створює більш безпечну та контрольовану структуру для захисту чутливих даних та критичних систем.

Управління доступом на основі ролей (RBAC) у Windows Server 2025 дозволяє створювати точно налаштовані політики доступу, які тісно узгоджуються з ролями та

обов’язками користувачів в організації (рис. 9.7). Цей підхід не лише спрощує часто складне завдання управління дозволами, але й гарантує, що користувачам надається доступ лише до тих ресурсів, які необхідні для виконання їхньої роботи, дотримуючись принципу найменших привілеїв. Така деталізація є критичною для мінімізації площини атаки, оскільки вона обмежує кількість осіб, які можуть взаємодіяти з цінними системами або конфіденційною інформацією. Помітний приклад ефективності RBAC можна спостерігати в організації охорони здоров’я, яка впровадила ці засоби контролю для захисту даних пацієнтів. Призначаючи ролі на основі посадових функцій, організація гарантувала, що лише уповноважений персонал міг отримувати доступ до чутливих медичних записів. Коли фішингова атака була спрямована на кількох співробітників, система RBAC обмежила доступ, запобігаючи доступу неавторизованих користувачів до критичної інформації, навіть коли вони намагалися використати викрадені облікові дані. Цей інцидент підкреслив важливість впровадження RBAC для пом’якшення потенційних порушень [3].

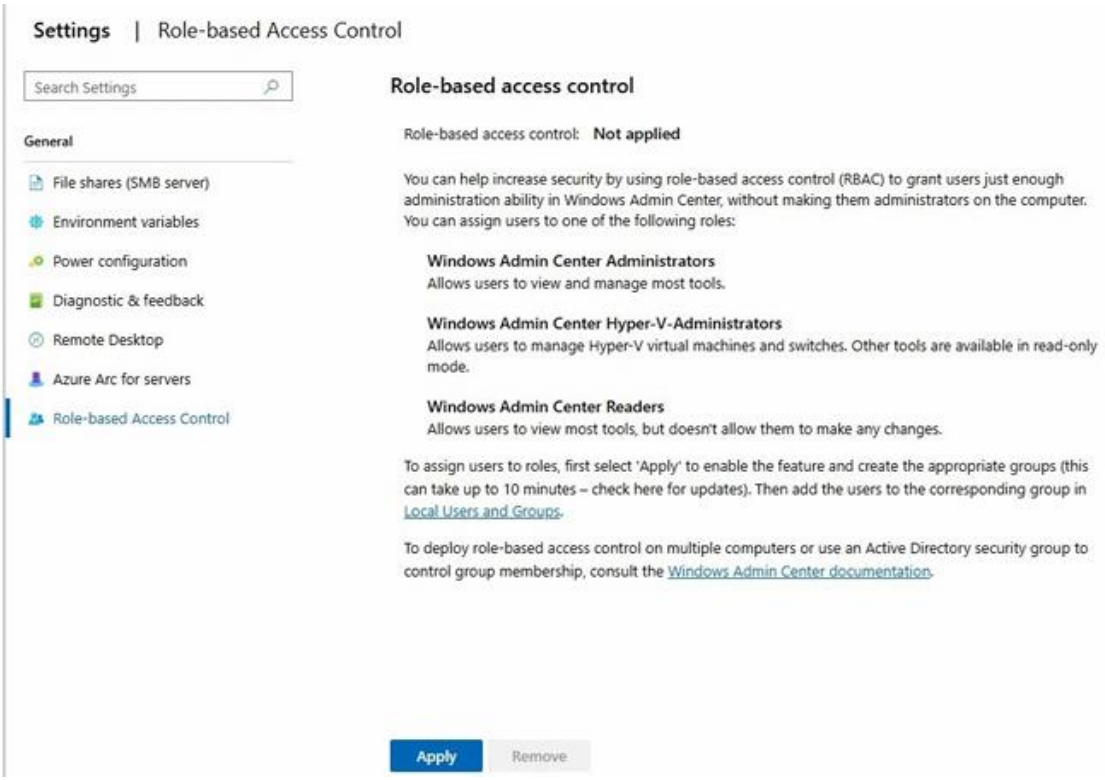

Рисунок 9.7 – Застосування RBAC у Windows Server 2025 x64 – Azure edition [3]

Багатофакторна автентифікація (MFA) додатково посилює ландшафт безпеки, вимагаючи декількох рівнів перевірки перед наданням доступу. Вимагаючи комбінацію того, що користувач знає (наприклад, пароль), того, що він має (наприклад, мобільний пристрій), або того, ким він є (біометрія), MFA додає надійний захист від несанкціонованого доступу. Це радикально знижує ймовірність атак на основі облікових даних, гарантуючи, що навіть якщо пароль скомпрометовано, необхідно подолати додаткові перешкоди безпеки.

Наприклад, фінансова установа, яка прийняла MFA, повідомила про значне зменшення спроб шахрайства. Після впровадження MFA було зірвано атаку, де неавторизований користувач намагався отримати доступ до рахунків клієнтів, використовуючи викрадені логіни. Доданий рівень безпеки, що вимагав одноразового коду, надісланого на мобільний пристрій користувача, запобіг доступу та захистив конфіденційну фінансову інформацію, ілюструючи, як MFA може слугувати критичною лінією оборони [3].

На додаток до цих засобів контролю доступу, Windows Server 2025 впроваджує передові інструменти аудиту та моніторингу, які надають адміністраторам глибшу видимість поведінки користувачів. Ці можливості дозволяють відстежувати спроби доступу в реальному часі та надають розуміння потенційних порушень безпеки або незвичних патернів активності. Маючи здатність моніторити спроби доступу в усьому середовищі, адміністратори можуть швидко виявляти підозрілу активність та реагувати на неї, зменшуючи вікно можливостей для зловмисника щодо експлуатації вразливостей. Більше того, інтеграція автоматизованого виявлення загроз у ці засоби контролю гарантує, що будь-яка нерегулярна або потенційно небезпечна поведінка негайно позначається, що дозволяє швидко реагувати. Цей безперервний нагляд покращує загальний стан безпеки, уможливлюючи проактивне пом’якшення ризиків до того, як вони зможуть завдати значної шкоди. Адміністратори можуть налаштовувати сповіщення про спроби несанкціонованого доступу, ідентифікувати повторювані аномалії та навіть динамічно коригувати політики для реагування на нові загрози. Комплексний характер цих удосконалень контролю доступу у Windows Server 2025 не лише підвищує безпеку IT-інфраструктури, але й оптимізує повсякденне адміністрування дозволів та управління користувачами, надаючи організаціям можливість захищатися від дедалі складніших кібератак при збереженні операційної ефективності.

Конфігурація RBAC дозволяє адміністраторам визначати ролі з конкретними дозволами та призначати ці ролі користувачам на основі їхніх посадових функцій, що спрощує управління правами доступу. Для ефективного налаштування RBAC процес розпочинається з визначення ключових ролей в організації, таких як HR-менеджер або IT-адміністратор, та документування їхніх обов’язків.

Далі, використовуючи консоль управління Windows Server, створюються та налаштовуються визначення ролей, наприклад, встановлюються дозволи для HR-менеджера на доступ до даних про заробітну плату, тоді як IT-адміністратору обмежується доступ до конфігурацій системи. На завершальному етапі ці ролі розподіляються між користувачами на основі їхніх посадових функцій, що забезпечує доступ лише до необхідних ресурсів. Для закріплення розуміння виконується практична вправа, яка передбачає визначення ролей для фіктивного відділу, призначення конкретних дозволів та тестування доступу для перевірки

того, що неавторизовані користувачі не можуть отримати доступ до обмежених зон. При налаштуванні рекомендується починати з попередньо визначених ролей, щоб уникнути помилок, а детальні інструкції доступні в документації Microsoft.

Налаштування багатофакторної автентифікації (MFA) додає критичний рівень захисту, який значно знижує ризик несанкціонованого доступу. Процес конфігурації включає перехід до налаштувань безпеки в Windows Admin Center (WAC), вибір опції багатофакторної автентифікації та налаштування методів перевірки, таких як SMS, електронна пошта або біометрія. Після увімкнення необхідно протестувати конфігурацію, виконавши вхід користувача та завершивши процес перевірки. Важливо зазначити, що Windows Admin Center не керує налаштуваннями MFA безпосередньо, тому сервер повинен бути підключений до Microsoft Entra ID для доступу до цих функцій. Практична вправа з налаштування та тестування MFA дозволяє перевірити коректність роботи механізму, симулюючи входи в систему та підтверджуючи, що система вимагає та валідує кілька факторів автентифікації перед наданням доступу.

Windows Server 2025 також впроваджує механізми автоматизованого реагування, спроектовані для нейтралізації загроз, як тільки вони виявлені. Ці попередньо налаштовані дії можуть автоматично ізолювати уражені системи, припиняти несанкціонований доступ або розгортати контрзаходи, зменшуючи час між виявленням та реагуванням та мінімізуючи втручання людини.

Для подальшого посилення захисту, виявлення загроз у Windows Server 2025 безшовно інтегрується з існуючими інструментами та структурами безпеки, дозволяючи IT-командам будувати більш цілісну систему безпеки. Поєднуючи аналітику на основі AI, моніторинг у реальному часі та автоматизоване пом’якшення наслідків, платформа надає адаптивне та стійке рішення безпеки. Цей комплексний набір функцій передового виявлення та реагування не лише зміцнює загальну архітектуру безпеки, але й надає IT-командам можливість займати проактивну позицію у захисті критичної інфраструктури [3].

Налаштування виявлення загроз передбачає встановлення систем для моніторингу мережевої активності, що починається з активації функції через Панель безпеки (Security Dashboard) у WAC та вказівки типів загроз для моніторингу. Далі визначаються параметри моніторингу, які встановлюють критерії незвичної активності, наприклад, спроби входу з незнайомих адрес, а сама система інтегрується із зовнішніми стрічками розвідки загроз.

Microsoft Defender Antivirus є ключовою функцією безпеки у Windows Server 2025, розробленою для забезпечення всебічного захисту від широкого спектру кіберзагроз через надання захисту в реальному часі, передового виявлення загроз та можливостей автоматизованого реагування.

Ключові особливості включають захист у реальному часі, який безперервно

моніторить сервер для виявлення шкідливих дій; передове виявлення загроз з використанням машинного навчання та хмарної розвідки; автоматизоване реагування, яке поміщає в карантин або видаляє загрози без ручного втручання; всебічну звітність для відстеження патернів загроз; та повну інтеграцію з Windows Admin Center для уніфікованого управління.

Для ефективного впровадження Microsoft Defender Antivirus необхідно активувати його через Windows Admin Center або PowerShell, регулярно оновлювати визначення безпеки та налаштовувати виключення для довірених додатків задля уникнення хибних спрацьовувань. Безперервний моніторинг та використання інструментів звітності дозволяють швидко реагувати на виявлені загрози, значно підвищуючи безпеку та стабільність IT-інфраструктури [3].

Windows Server 2025 вирішує проблему оперативного реагування за допомогою передових систем автоматизованого реагування, спроектованих для проактивного пом'якшення ризиків у реальному часі. Використовуючи машинне навчання та штучний інтелект, ці системи постійно еволюціонують, виявляють аномалії та автоматично ініціюють попередньо налаштовані дії, такі як ізоляція скомпрометованих систем або завершення підозрілих процесів, що нейтралізує загрози до завдання значної шкоди.

Автоматизація цих процесів зменшує робоче навантаження на адміністраторів, усуває людський фактор та забезпечує точність і послідовність у вирішенні інцидентів. Гнучкість систем дозволяє організаціям адаптувати реакції відповідно до специфічних політик безпеки, надаючи адміністраторам точний контроль над тригерами та діями. Впровадження автоматизованих реакцій включає налаштування дій у WAC, визначення тригерів (умов активації) та проведення тестування у контрольованому середовищі для перевірки надійності. Крім того, процес кастомізації вимагає регулярного перегляду та коригування протоколів реагування на основі нових даних про загрози, а також моніторингу впливу автоматизації на продуктивність системи для підтримання балансу між безпекою та операційною ефективністю.

Захист каналів зв'язку за допомогою різних VPN-протоколів

У сучасному цифровому середовищі, де витоки даних та кіберзагрози стають дедалі складнішими, захист каналів зв'язку набув першочергового значення.

TLS у Windows Server 2025, як проілюстровано на рисунку 9.8, впроваджує кілька передових функцій, адаптованих для вирішення еволюціонуючих потреб кібербезпеки та цілісності даних. Ключовим удосконаленням є повна інтеграція TLS 1.3, що забезпечує швидшу продуктивність та сильнішу безпеку шляхом оптимізації процесу встановлення з'єднання та видалення застарілих криптографічних алгоритмів. Це значно знижує затримку при встановленні з'єднання, покращує загальну ефективність та мінімізує площину атаки на

систему, забезпечуючи надійний захист від сучасних загроз.

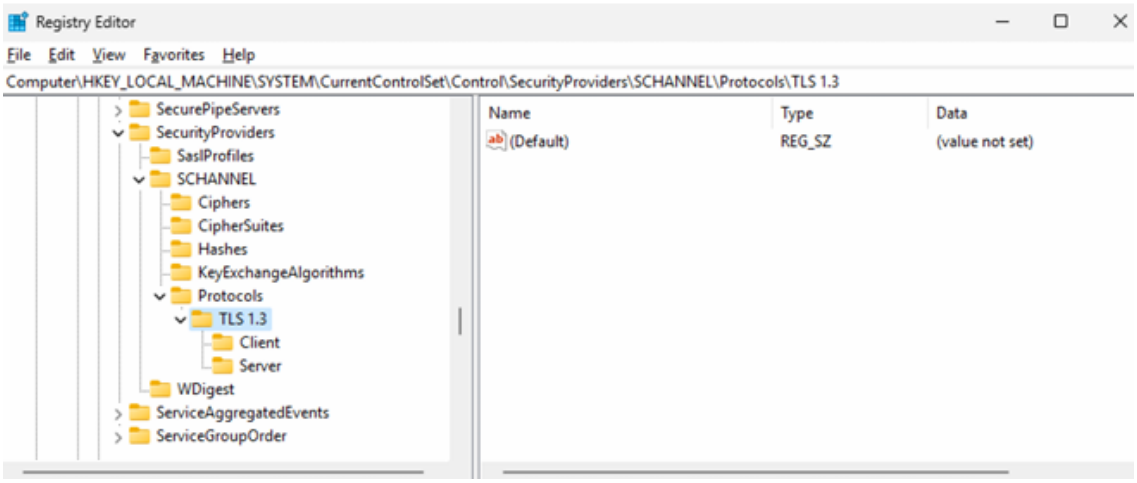

Рисунок 9.8 – Увімкнення TLS 1.3 у Windows Server 2025 [3]

Адміністратори отримують переваги від зручного інтерфейсу оновленого Windows Admin Center (WAC), який спрощує конфігурацію та управління TLS для різних ролей серверів, служб та додатків. Завдяки цьому інтерфейсу управління політиками TLS стає більш доступним, а моніторинг серверних середовищ здійснюється ефективніше.

Крім того, Windows Server 2025 покращує управління сертифікатами шляхом автоматизації видачі, оновлення та відкликання сертифікатів через інтеграцію з Active Directory Certificate Services (AD CS). Ця автоматизація зменшує адміністративне навантаження, забезпечує безперервну безпеку та усуває ризики, пов’язані з простроченими або неправильно керованими сертифікатами [3].

Сервер також використовує новітні криптографічні набори, пропонуючи організаціям гнучкість у впровадженні передових стандартів шифрування. Це гарантує відповідність суворим галузевим регламентам, таким як GDPR, HIPAA та PCI DSS, надаючи підприємствам впевненість при обробці чутливих даних.

Подальше посилення безпеки досягається завдяки включенню комплексних інструментів аудиту, які дозволяють детальне ведення журналів та оповіщення в реальному часі, надаючи IT-адміністраторам можливість швидко ідентифікувати та усувати потенційні вразливості або підозрілу активність. Розгортання TLS у Windows Server 2025 дозволяє організаціям захистити дані під час передачі та зміцнити стійкість IT-інфраструктури, що є важливим для протистояння поточним та новим кіберзагрозам.

Встановивши основи TLS та його ключову роль у захисті комунікацій, важливо дослідити інші суттєві безпечні протоколи, такі як HTTPS, IPSec та SSH, розуміння яких забезпечує більш повне уявлення про захист каналів зв’язку сервера. Впровадження надійних протоколів безпеки є основою захисту сучасної IT-інфраструктури, і Windows Server 2025

надає безпрецедентну підтримку в цьому аспекті. Окрім удосконалень, принесених TLS, сервер також пропонує широкі можливості роботи з іншими протоколами. HTTPS (HyperText Transfer Protocol Secure) гарантує, що веб-комунікації зашифровані, захищаючи чутливі дані від атак типу «людина посередині» та прослуховування. У Windows Server 2025 адміністратори можуть без зусиль налаштувати HTTPS для захисту веб-додатків та служб через WAC, використовуючи такі функції, як автоматична прив'язка сертифікатів HTTPS та інтеграція з AD CS для спрощеного управління сертифікатами [3].

Internet Protocol Security (IPSec) є ще одним критичним протоколом, що надається Windows Server 2025. IPSec працює на мережевому рівні, захищаючи пакети даних, якими обмінюються пристрої через IP-мережу. Цей протокол є суттєвим для створення віртуальних приватних мереж (VPN) та захисту внутрішнього мережевого трафіку. Передові криптографічні алгоритми, включені в IPSec для Windows Server 2025, покращують цілісність даних та автентифікацію, гарантуючи, що дані не будуть піддані втручанню під час передачі. Адміністратори можуть розгортати політики IPSec за допомогою групової політики, забезпечуючи централізований спосіб впровадження безпеки у всій мережі [3].

Secure Shell (SSH) також відіграє життєво важливу роль у захисті серверних комунікацій. SSH широко використовується для безпечного віддаленого адміністрування, дозволяючи адміністраторам керувати серверами, передавати файли та виконувати команди через зашифрований канал. Windows Server 2025 підтримує SSH нативно, уможливлюючи безшовне та безпечне віддалене управління (рис. 9.9). Інтеграція SSH у Windows Server 2025 забезпечує сумісність з різними інструментами автоматизації та скриптами, підвищуючи операційну ефективність при збереженні безпеки.

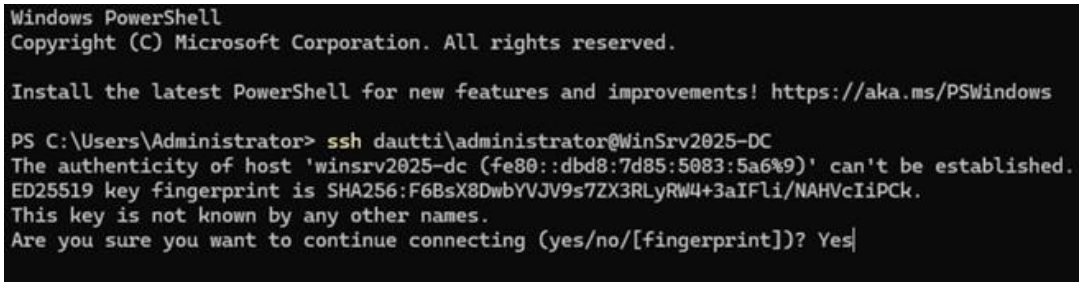

Рисунок 9.9 – Увімкнення SSH у Windows Server 2025 [3]

Експертиза є вирішальною в оптимізації розгортання та управління цими безпечними протоколами. Використовуючи HTTPS, IPSec та SSH, організації можуть створити багаторівневу структуру безпеки, яка адресує різні аспекти захисту даних. Забезпечення правильного впровадження та безперервного моніторингу цих протоколів може значно зменшити вразливості та сприяти створенню безпечного операційного середовища, підтримуючи цілісність та конфіденційність комунікацій та передачі даних. Роль фахівця у

цьому процесі є незамінною, оскільки глибоке розуміння цих систем допомагає підтримувати цілісність та конфіденційність комунікацій.

Моніторинг захищених каналів зв'язку є життєво важливим для забезпечення стійкої та безпечної IT-інфраструктури, і Windows Server 2025 оснащений передовими інструментами для підтримки цього важливого завдання. Платформа пропонує ряд функцій, розроблених для оптимізації моніторингу та управління протоколами безпечної комунікації, дозволяючи адміністраторам виявляти та пом'якшувати ризики до їх ескалації в загрози.

Безперервний моніторинг є ключовим для ідентифікації вразливостей або підозрілої активності, що уможливлює швидке втручання та посилення безпеки передачі даних. Визначною особливістю Windows Server 2025 є його покращені можливості аудиту, які забезпечують детальне ведення журналів та механізми сповіщення. Ці інструменти дозволяють адміністраторам ретельно відстежувати стан безпеки своїх мереж, полегшуючи ідентифікацію джерела будь-яких аномалій та швидке реагування. Передова аналітика додатково зміцнює цей захист, оскільки вона здатна розпізнавати патерни, що вказують на нові кіберзагрози, допомагаючи командам безпеки застосовувати проактивні стратегії.

WAC спрощує процес моніторингу, пропонуючи централізовану платформу, де адміністратори можуть налаштовувати та контролювати безпечні протоколи, такі як TLS, HTTPS, IPSec та SSH. Цей уніфікований інтерфейс підвищує операційну ефективність та гарантує, що заходи безпеки послідовно застосовуються в усій організації. Завдяки інформаційним панелям у реальному часі, які надають актуальну інформацію про стан та безпеку каналів зв'язку, адміністратори можуть приймати обґрунтовані рішення та випереджати потенційні проблеми. Автоматизація також відіграє критичну роль у підтриманні захищених каналів. Windows Server 2025 підтримує автоматизовані інструменти, такі як інструменти для управління сертифікатами через AD CS, що обробляють видачу та оновлення сертифікатів безпеки. Ця автоматизація зменшує ручне втручання та мінімізує ризик людської помилки, гарантуючи, що зашифровані комунікації залишаються безпечними та відповідають найкращим практикам [3].

Впровадження найкращих практик безпеки у Windows Server 2025

Управління виправленнями у Windows Server 2025 відіграє життєво важливу роль у забезпеченні безпечного та стійкого IT-середовища шляхом систематичного застосування оновлень та патчів, що усувають вразливості безпеки, покращують продуктивність та забезпечують відповідність галузевим стандартам. Windows Server 2025 впроваджує кілька вдосконалень, покликаних зробити процес управління виправленнями більш ефективним, надійним та оптимізованим. Одним із ключових удосконалень є інтеграція з Windows Update for Business, що дозволяє адміністраторам керувати оновленнями на кількох серверах із

централізованої панелі управління. Ця функція надає гранулярний контроль над політиками оновлення, такими як періоди відстрочки та вікна обслуговування, що уможливлює безшовне розгортання виправлень з мінімальним порушенням бізнес-операцій. Додатково, розширені можливості звітності платформи надають адміністраторам детальну інформацію про статус розгортання патчів, включаючи застосовані, очікувані або проблемні оновлення. Ці інструменти звітності є важливими для підтримання відповідності нормативним стандартам та проведення аналізу після розгортання.

Windows Server 2025 також пропонує автоматизовані інструменти управління виправленнями, що зменшує потребу в ручному втручанні. Автоматизація гарантує своєчасне розгортання критичних патчів, мінімізує людські помилки та дозволяє IT-командам зосередитися на більш стратегічних ініціативах. Платформа включає опції відкату, що забезпечує можливість повернення до попередніх конфігурацій, якщо оновлення викликає непередбачені проблеми, додаючи рівень безпеки під час процесу оновлення (рис. 9.10).

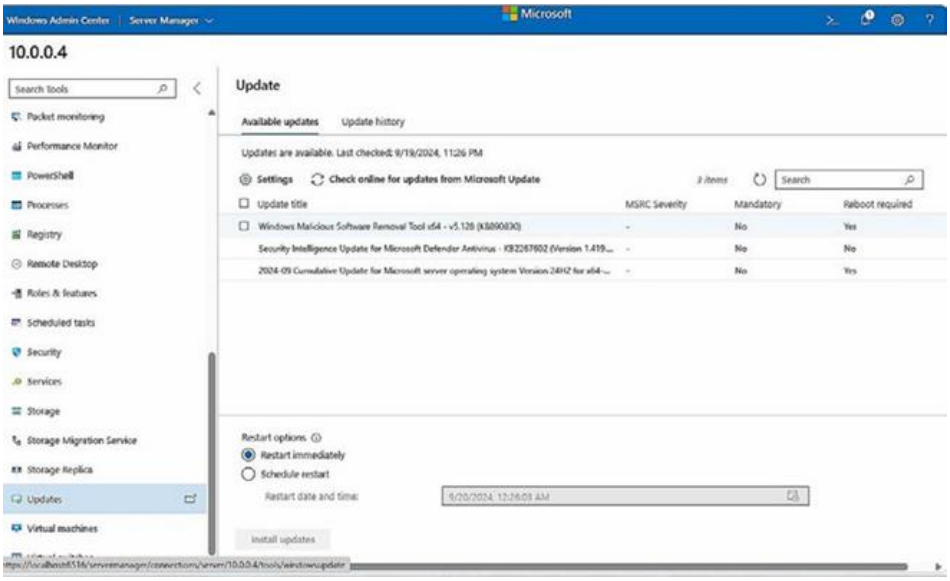

Рисунок 9.10 – Управління та застосування оновлень у WAC [3]

Експертиза фахівців є важливою для оптимізації цих процедур управління виправленнями. Глибоке розуміння системних вразливостей та протоколів оновлення дозволяє забезпечити практичність та ефективність розгортання патчів, одночасно вирішуючи будь-які проблеми, що виникають. Активний моніторинг процесу оновлення допомагає підтримувати цілісність та безпеку IT-інфраструктури. Розширені можливості управління виправленнями у Windows Server 2025 безпосередньо вирішують виклики, пов’язані з сучасними загрозами кібербезпеки. Впроваджуючи надійну стратегію управління патчами, організації можуть ефективно захищати свої системи, забезпечувати безперервність операцій та підтримувати відповідність галузевим стандартам. Ці інструменти та функції є критичними для проактивного захисту від вразливостей та підтримання довіри й надійності,

що є важливими в сучасній цифровій інфраструктурі.

Маючи повне розуміння управління виправленнями та його важливості для підтримання безпеки системи, наступним важливим аспектом є журналювання аудиту. Вивчення того, як функціонують журнали аудиту в Windows Server 2025, додатково підвищить здатність моніторити потенційні інциденти безпеки та реагувати на них.

Журналювання аудиту є фундаментальним елементом Windows Server 2025, необхідним для підтримання безпечного та відповідного нормам IT-середовища. Ця функція дозволяє адміністраторам відстежувати та записувати широкий спектр активності сервера, включаючи входи користувачів, спроби доступу, зміни в системі та використання додатків. Фіксуючи ці події в деталях, журнали аудиту створюють ретельний запис, що підтримує виявлення аномалій, розслідування інцидентів безпеки та дотримання регуляторних стандартів.

Windows Server 2025 покращує журналювання аудиту, як зображено на рисунку 9.11, розширеними можливостями, надаючи адміністраторам онтроль над тим, які дії реєструються. Можна налаштувати детальні політики, щоб гарантувати узгодження процесу аудиту зі специфічними вимогами безпеки організації. Така кастомізація є особливо цінною в середовищах з різною чутливістю даних та потребами у відповідності в різних підрозділах та системах.

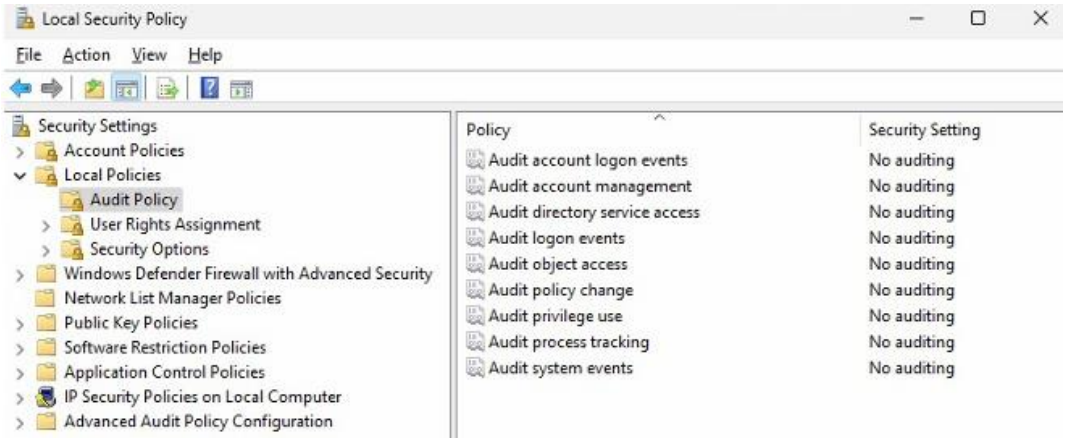

Рисунок 9.11 – Політика аудиту у Windows Server 2025 [3]

Експертиза в налаштуванні та управлінні журналами аудиту гарантує, що вони надають дієву розвідувальну інформацію, уникаючи при цьому перевантаження системи. Досягнення балансу між всебічним збором даних та ефективністю системи є ключовим, і розуміння операцій системи та протоколів безпеки є суттєвим у цьому аспекті. Більше того, журнали аудиту відіграють життєво важливу роль у виконанні галузевих стандартів та правових вимог. Підтримуючи точні та повні записи активності системи, організації можуть продемонструвати свою прихильність підзвітності та прозорості, що є критичним для

регуляторної відповідності та сертифікацій.

Загалом, опанування журналювання аудиту у Windows Server 2025 є важливим для захисту IT-інфраструктури організації. Після заглиблення в деталі журналювання аудиту, яке відіграє критичну роль у відстеженні та аналізі активності системи, наступним кроком є зосередження на регулярних оцінках безпеки. Ці оцінки допоможуть оцінити ефективність заходів безпеки та гарантувати, що система залишається стійкою до нових загроз.

Регулярні оцінки безпеки є життєво необхідними для захисту IT-інфраструктури організації. У Windows Server 2025 ці оцінки спроектовані для виявлення вразливостей, оцінювання існуючих заходів безпеки та забезпечення дотримання галузевих стандартів і правил. Проводячи ці оцінювання періодично, IT-фахівці можуть отримати ретельне розуміння стану безпеки своєї системи, що дозволяє їм проактивно усувати слабкі місця до того, як зловмисники зможуть їх експлуатувати.

Процес оцінювання у Windows Server 2025 зазвичай використовує комбінацію автоматизованих та ручних методів. Автоматизовані сканери вразливостей ефективно виявляють відомі прогалини в безпеці, тоді як ручне тестування на проникнення забезпечує більш детальну перевірку захисту сервера від складних загроз. Ці інтегровані інструменти дозволяють IT-фахівцям виконувати всебічні та ефективні оцінки, гарантуючи ретельний перегляд усіх аспектів безпеки [3].

Окрім ідентифікації вразливостей, оцінки безпеки є вирішальними для валідації ефективності існуючих політик та засобів контролю безпеки. Регулярні перегляди та тестування підтверджують, що ці заходи функціонують як задумано і здатні протистояти новітнім загрозам.

Інформація, отримана в результаті оцінок безпеки, спрямовує стратегічні рішення щодо розподілу ресурсів, управління ризиками та пріоритезації ініціатив з безпеки. Постійно оновлюючи стратегії безпеки у відповідь на результати оцінювання, IT-фахівці можуть підтримувати проактивну оборонну позицію, яка адаптується до нових кіберзагроз. Додатково, ці оцінки надають необхідну документацію для демонстрації відповідності під час аудитів, підкріплюючи зобов’язання організації підтримувати високі стандарти безпеки.

Microsoft Defender for Endpoint (MDE) пропонує передові можливості безпеки для Windows Server 2025, забезпечуючи надійний захист від складних кіберзагроз. Для повного використання можливостей безпеки MDE необхідна інтеграція з Azure, оскільки це з’єднання забезпечує централізоване управління та потужну аналітику загроз. По-перше, для ефективного використання MDE необхідний клієнт Azure, що уможливлює централізоване управління та доступ до розширеної аналітики через портал Azure. По-друге, інтеграція з Microsoft Entra ID є критичною для управління ідентичностями користувачів та контролем доступу, що уможливлює такі передові функції безпеки, як умовний та захист ідентичності.

Щодо ліцензування, MDE доступний у двох основних планах – Plan 1 та Plan 2 – з різними можливостями. Plan 1 (Standard) включає основні функції, такі як захист нового покоління, зменшення площини атаки та EDR. Plan 2 (Advanced) додає розширені функції, такі як автоматизоване розслідування, усунення загроз, управління вразливостями та можливості розширеного пошуку загроз. Організаціям слід оцінити свої потреби в безпеці, щоб обрати між Plan 1 або Plan 2, причому Plan 2 рекомендується для тих, хто потребує більш всебічних заходів безпеки та розширених функцій [3].

Додаткові системні вимоги також відіграють важливу роль у впровадженні MDE. Інтеграція з Azure Log Analytics настійно рекомендується для передової аналітики загроз та детальної звітності, оскільки ця служба збирає та аналізує дані для надання критичної інформації про безпеку [3].

Також використовується Microsoft Defender Security Center – централізована платформа, що дозволяє адміністраторам моніторити та управляти безпекою кінцевих точок, надаючи сповіщення в реальному часі та детальні звіти про загрози. Необхідно також переконатися, що Windows Server 2025 повністю оновлений останніми патчами для підтримання безпеки та сумісності з MDE [3].

Для увімкнення MDE на Windows Server 2025 необхідно виконати наступні ключові кроки: налаштувати клієнт Azure і зв’язати сервер з AAD; обрати відповідний план ліцензування (Plan 1 або Plan 2) на основі вимог безпеки; увімкнути MDE на сервері через портал Azure; налаштувати Azure Log Analytics для збору та аналізу даних, пов’язаних із безпекою; і, нарешті, використовувати Microsoft Defender Security Center для моніторингу загроз, управління налаштуваннями безпеки та генерації всебічних звітів.

Включаючи MDE у Windows Server 2025, організації можуть досягти надійної структури безпеки, здатної захищати від сучасних складних загроз, спрощуючи при цьому управління за допомогою інтегрованих інструментів та детальної аналітики.

Встановлення базових ліній безпеки є практикою для підтримання безпечного та відповідного нормам IT-середовища. Базова лінія безпеки – це набір мінімальних конфігурацій безпеки, які узгоджуються з політиками організації та найкращими галузевими практиками. Встановлення цих базових ліній гарантує, що всі системи відповідають фундаментальним вимогам безпеки, зменшуючи вразливості та спрощуючи процес підтримання узгодженості в мережі.

Моніторинг відхилень стосується відстеження змін від визначених налаштувань базової лінії, чи то навмисних, чи випадкових. Це є життєво важливим для виявлення несанкціонованих модифікацій або неправильних конфігурацій, які можуть створити ризики безпеки. Регулярна перевірка на наявність відхилень гарантує, що системи залишаються узгодженими зі стандартами безпеки організації.

Тема 10
Веб-сервер IIS

Архітектура IIS

Веб-служба розглядається як стандартизований фреймворк, що дозволяє різним програмним додаткам, які часто функціонують на відмінних платформах, ефективно комунікувати та взаємодіяти один з одним. Ця інтероперабельність досягається завдяки використанню форматів та протоколів на основі розширюваної мови розмітки (XML), таких як простий протокол доступу до об'єктів (Simple Object Access Protocol – SOAP), мова опису веб-служб (Web Services Description Language – WSDL) та універсальний опис, виявлення та інтеграція (Universal Description, Discovery, and Integration – UDDI). Ці технології полегшують обмін даними та виклик функціональних можливостей через мережу, дозволяючи додаткам безперешкодно працювати разом, незалежно від їхніх базових систем.

Веб-служби прийнято класифікувати на два основні типи.

Перший тип – це веб-служби RESTful, побудовані на архітектурі передачі репрезентативного стану (Representational State Transfer – REST), яка використовує методи протоколу передачі гіпертексту (HTTP), такі як GET, POST, PUT та DELETE, разом з уніфікованими ідентифікаторами ресурсів (URIs) для доступу до ресурсів та маніпулювання ними. Цей підхід відомий своєю простотою та масштабованістю, що робить його добре пристосованим для веб-взаємодій [3].

Другий тип – це веб-служби на основі SOAP, які покладаються на протокол SOAP, що використовує структуровані XML-повідомлення та конверти для комунікації з кінцевою точкою служби. SOAP є більш жорстким та стандартизованим, пропонуючи вбудовану обробку помилок та функції безпеки, що робить його ідеальним для додатків корпоративного рівня, де надійність та безпека є першочерговими [3].

Internet Information Services (IIS) – це надійна та універсальна платформа веб-сервера від Microsoft, спроектована для доставки масштабованих, керованих та надійних веб-додатків. IIS полегшує комунікацію між браузером та веб-сервером за допомогою різноманітних протоколів, включаючи HTTP, захищений HTTP (HTTPS), протокол передачі файлів (FTP), захищений FTP (FTPS), SMTP та протокол передачі мережевих новин (NNTP). Додатково Microsoft впроваджено технологію серверних сценаріїв Active Server Pages (ASP), яка уможливлює створення динамічного веб-контенту [3].

З випуском версії IIS 10 корпорація Microsoft значно покращила безпеку та продуктивність платформи. Ця версія підтримує довший час виконання сценаріїв та впроваджує підтримку HTTP/2. Крім того, у січні 2020 року Microsoft було запущено новий браузер на базі Chromium під назвою Microsoft Edge, що додатково доповнює екосистему IIS. IIS 10 також приніс нові функції у Windows Server 2025, такі як покращене узгодження

наборів шифрів на стороні сервера для HTTP/3, адміністрування IIS за допомогою командлетів PowerShell, підтримка заголовків хоста з підстановочними знаками (wildcard host headers), здатність запускати IIS на Nano Server та всередині контейнерів, а також інтерфейс користувача для управління HTTPS Strict Transport Security (HSTS). Ці вдосконалення колективно підвищили продуктивність та безпеку IIS.

World Wide Web (WWW) визначається як глобальна інформаційна система, що функціонує через інтернет. Вона дозволяє користувачам отримувати доступ до веб-сторінок та взаємодіяти з ними через протокол HTTP. Веб-сторінки, які зазвичай пишуться мовою розмітки гіпертексту (HTML), можуть включати текст, зображення, відео та інші мультимедійні елементи, що робить веб багатим та динамічним майданчиком для обміну інформацією.

Концепція WWW була вперше запропонована Тімом Бернерсом-Лі у 1989 році під час роботи в CERN, і вона швидко еволюціонувала у розгалужену мережу, яка використовується сьогодні. До основних технологій, що лежать в основі веб-середовища, належать HTML для структурування контенту, HTTP для передачі даних між серверами та клієнтами, а також уніфіковані покажчики ресурсів (URLs) для адресації ресурсів у мережі.

Спочатку веб-середовище було статичним, але з того часу воно розвинулося для підтримки інтерактивних додатків, комунікації в реальному часі та складних веб-служб. Як показано на рисунку 10.1, який ілюструє зразок веб-сторінки та її базовий HTML-код, веб виріс з базової платформи для обміну документами у фундаментальну частину сучасної IT-інфраструктури, що підтримує все: від електронної комерції до соціальних мереж.

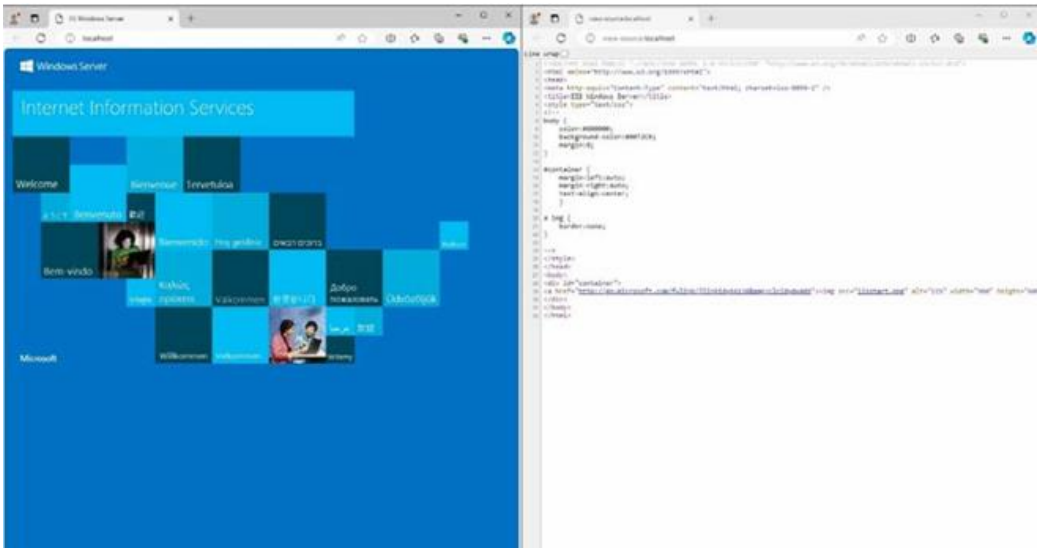

Рисунок 10.1 – Веб-сторінка та її вихідний код [3]

Встановлення ролі веб-сервера

Для налаштування веб-сервера на Windows Server 2025 необхідно додати IIS як роль

сервера. Цей процес розпочинається з входу в систему Windows Server 2025 з обліковим записом адміністратора. З меню «Пуск» відкривається «Server Manager» (Диспетчер серверів). У «Server Manager» у верхньому правому куті обирається опція «Manage» (Управління), після чого вибирається пункт «Add Roles and Features» (Додати ролі та компоненти), що запускає відповідний майстер встановлення. На сторінці «Before You Begin» (Перед початком) натискається «Next» (Далі). Потім обирається тип встановлення «Role-based or feature-based installation» (Встановлення на основі ролей або компонентів) і натискається «Next». На сторінці вибору сервера вказується локальний сервер і натискається «Next». На сторінці «Server Roles» (Ролі сервера) встановлюється прапорець навпроти «Web Server (IIS)», як показано на рисунку 10.2. Після цього з'явиться діалогове вікно, в якому слід натиснути «Add Features» (Додати компоненти), а потім – «Next».

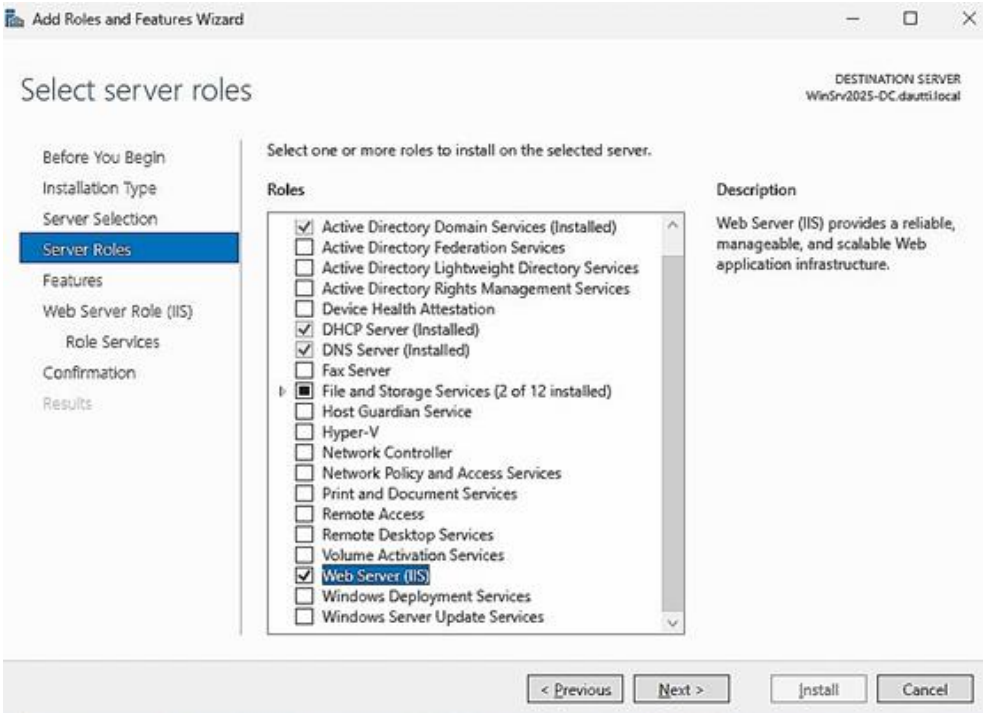

Рисунок 10.2 – Додавання веб-сервера (IIS) у Windows Server 2025 [3]

На сторінці «Features» (Компоненти) існує можливість додати додаткові компоненти, проте для більшості конфігурацій достатньо параметрів за замовчуванням. Після натискання «Next» здійснюється перегляд огляду ролі «Web Server (IIS)» і знову натискається «Next». На сторінці «Role Services» (Служби ролей) за необхідності можна додати додаткові функції IIS, такі як FTP-сервер або опції безпеки. Після завершення вибору натискається «Next». На сторінці підтвердження («Confirmation») перевіряються вибрані параметри. Тут можна вибрати опцію автоматичного перезапуску сервера у разі необхідності. Процес розпочинається натисканням кнопки «Install» (Встановити). Хід встановлення відображається на екрані, а після його завершення для виходу з майстра натискається «Close»

(Закрити) [36].

Після встановлення IIS Manager слугує адміністративною консоллю для управління веб-сервером. Доступ до нього здійснюється через «Server Manager», «Windows Administrative Tools» (Засоби адміністрування Windows) або шляхом виконання команди inetmgr у діалоговому вікні «Run» (Виконати). IIS Manager дозволяє адміністраторам ефективно керувати своїми веб-додатками, як зображено на рисунку 10.3.

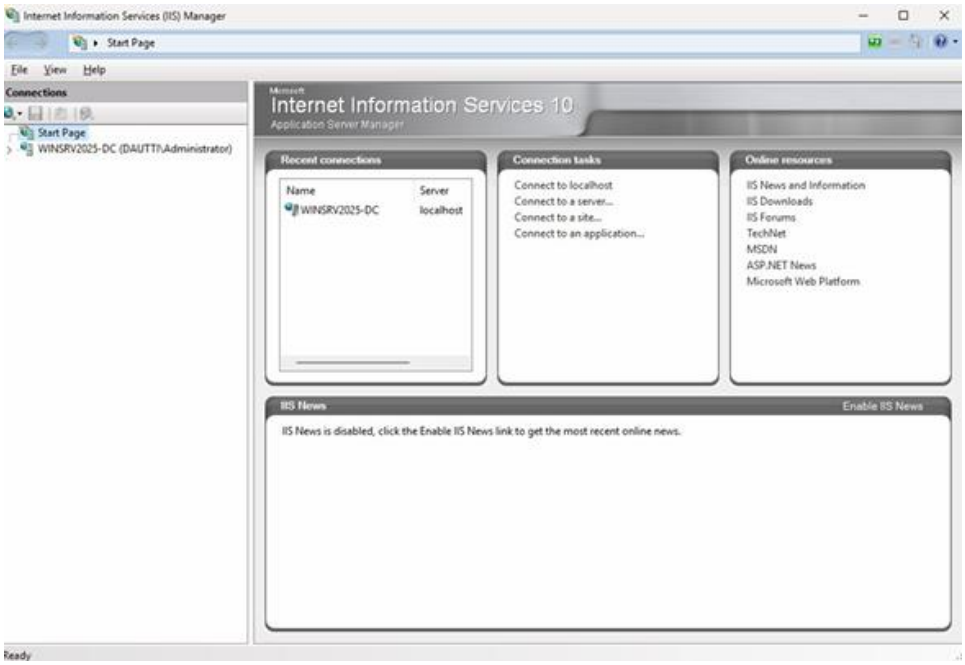

Рисунок 10.3 – IIS Manager у Windows Server 2025 [3]

FTP слугує фундаментальним методом передачі файлів через Інтернет, пропонуючи безпечний та ефективний механізм обміну даними між комп’ютерами. Спочатку розроблений на початку 1970-х років, FTP залишається життєво важливим інструментом у мережевих середовищах завдяки своїй простоті та надійності. Він широко застосовується для ряду завдань, включаючи передачу корпоративних даних у внутрішніх мережах, управління контентом веб-сайтів та забезпечення завантаження і вивантаження файлів на веб-сервери та з них [4].

FTP функціонує за моделлю клієнт-сервер, використовуючи два різні порти для управління операціями. Порт 21 призначений для встановлення керуючого з’єднання, що дозволяє обмінюватися командами та відповідями між клієнтом і сервером. Після встановлення цього з’єднання порт 20 використовується для фактичної передачі даних, обробляючи пересилання файлів між системами. Ця система з двома портами, що є свідченням ефективності протоколу, забезпечує розділення трафіку команд і даних, підвищуючи продуктивність протоколу.

Налаштування FTP-сервера на Windows Server 2025 передбачає кілька ключових

кроків. Спочатку необхідно встановити роль «Web Server (IIS)» на сервері, що закладає основу для розміщення різних веб- та FTP-служб. Після цього додається служба ролі «FTP Server» в межах ролі веб-сервера, як зображено на рисунку 10.4. Ця конфігурація дозволяє серверу обробляти FTP-з'єднання, надаючи адміністраторам надійний інструмент для управління передачею файлів у контрольований, безпечний та масштабований спосіб [3].

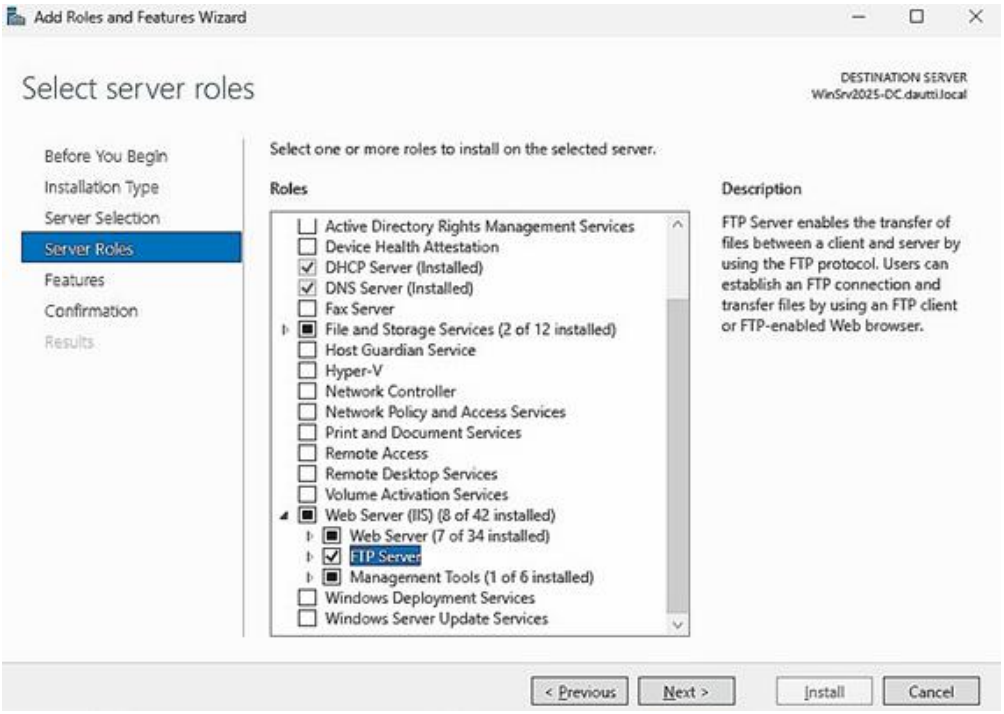

Рисунок 10.4 – Додавання FTP-сервера як служби ролі у Windows Server 2025 [3]

Якщо виникає необхідність додати або змінити служби ролей після початкового встановлення, це можна зробити через «Server Manager». Запустивши майстер «Add Roles and Features Wizard», можна встановити або налаштувати додаткові функції та служби IIS. Цей процес дозволяє подальше налаштування середовища IIS, додаючи такі компоненти, як модулі переписування URL-адрес, функції безпеки або додаткові інструменти управління за потребою [36].

Налаштування веб-сайтів і віртуальних каталогів

Платформа IIS спроектована для підтримки тисяч веб-сайтів на одному веб-сервері. Кількість веб-сайтів, які система здатна ефективно супроводжувати, безпосередньо залежить від апаратної конфігурації, зокрема від кількості процесорів, обсягу оперативної пам'яті, пропускної здатності мережі тощо. Для кожного веб-сайту, призначеного для роботи в мережі Інтернет, необхідна наявність загальнодоступної IP-адреси та зареєстрованого доменного імені. У випадках, коли в наявності є лише одна загальнодоступна IP-адреса, а виникає потреба у підтримці кількох веб-сайтів, для обслуговування інтернет-користувачів

створюються віртуальні каталоги або застосовуються заголовки хоста.

У консолі диспетчера IIS, у папці «Web Sites» (Веб-сайти), за замовчуванням міститься елемент «Default Web Site» (Стандартний веб-сайт), що являє собою стандартний зразок веб-сайту. Хоча його можна використовувати для публікації контенту, рекомендованою практикою є створення та налаштування власного, окремого веб-сайту [37].

Процедура створення нового веб-сайту передбачає виконання низки кроків. У вікні «Internet Information Services (IIS) Manager» (Диспетчер IIS) необхідно натиснути правою кнопкою миші на вузлі «Sites» (Сайти) у панелі «Connections» (Підключення) та вибрати в контекстному меню пункт «Add Website» (Додати веб-сайт). Після відкриття сторінки «Add Website» вводиться ім’я веб-сайту, наприклад, «ExpenseReport». За необхідності, у розділі «Application Pool» (Пул додатків) натискається кнопка «Select» (Вибрати) для зміни параметрів пулу додатків нового сайту, оскільки за замовчуванням пропонується варіант «DefaultAppPool». Далі у розділі «Content Directory» (Каталог контенту) вказується фізичний шлях папки «Web Sites» або здійснюється пошук цієї папки шляхом натискання на кнопку з трикрапкою [37].

Варто зауважити, що при вказівці фізичного шляху каталогу з контентом допускається використання віддаленого мережевого ресурсу. У такому випадку IIS повинен мати до нього доступ, що перевіряється натисканням кнопки «Connect As» (Підключитися від імені). Далі вказуються параметри підключення до мережевого ресурсу шляхом вибору конкретного облікового запису користувача з необхідними повноваженнями або вибирається варіант «Pass-Through Authentication» (Наскрізна автентифікація).

У розділі «Binding» (Прив’язка) сторінки «Add Website» визначається протокол для нового сайту (HTTP або HTTPS), IP-адреса (або поле залишається порожнім) та порт, який сайт повинен прослуховувати. На цій же сторінці можна вказати додатковий необов’язковий параметр – заголовок хоста, наприклад, expensereport.companyabc.com. Після встановлення прапорця «Start Website Immediately» (Запустити веб-сайт негайно) та перевірки всіх введених параметрів процес створення нового веб-сайту завершується натисканням кнопки «OK» [3].

Віртуальні каталоги дозволяють розширити домашній каталог веб-сайту за допомогою псевдоніма, що вказує на інший каталог за межами домашнього. Цей псевдонім, навіть якщо він посилається на ресурс, розташований на зовсім іншому сервері, відображатиметься для користувачів як звичайний підкаталог веб-сайту. У віртуальному каталозі можуть зберігатися документи та інша інформація як для поточного, так і для зовсім іншого веб-сайту. Наприклад, якщо виникає необхідність обслуговування на веб-сайті www.companyabc.com тимчасового веб-сайту іншої організації (наприклад, CompanyXYZ), компанія CompanyABC може розмістити цей веб-сайт у віртуальному каталозі. У такому разі веб-сайт організації

CompanyXYZ буде доступним за адресою www.companyabc.com/companyxyz/. Для створення віртуального каталогу необхідні права адміністратора сервера, сайту або додатка.

Процес створення віртуального каталогу за допомогою диспетчера IIS розпочинається із запуску «Server Manager» (Диспетчер серверів) та вибору пункту меню «Tools» – «Internet Information Services (IIS) Manager». У панелі «Connections» розгортається вузол IIS, а потім вузол «Sites». Далі вибирається потрібний веб-сайт для розміщення нового віртуального каталогу, на якому слід натиснути правою кнопкою миші та вибрати в контекстному меню пункт «Add Virtual Directory» (Додати віртуальний каталог). Після цього вводиться псевдонім для віртуального каталогу (наприклад, «Images») та вказується фізичний шлях папки з вмістом віртуального каталогу або здійснюється її пошук за допомогою кнопки з трикрапкою. Слід зазначити, що якщо як папку з контентом потрібно вказати віддалений мережевий ресурс, необхідно натиснути кнопку «Connect As» і увійти в систему з повноваженнями, достатніми для доступу до цього ресурсу, або вибрати варіант наскрізної автентифікації. Після перегляду вибраних параметрів, створення віртуального каталогу завершується натисканням кнопки «OK» (рис. 10.5) [4].

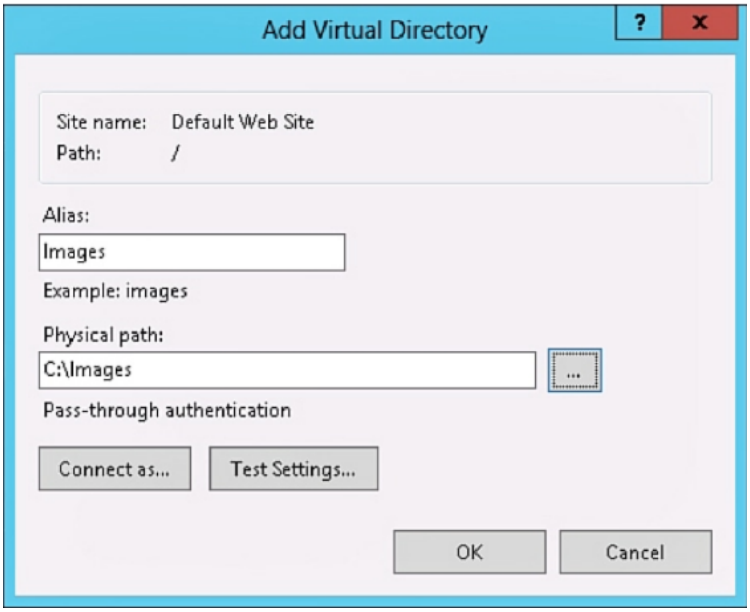

Рисунок 10.5 – Діалогове вікно Add Virtual Directory (Додати віртуальний каталог) [4]

Раніше зміна стандартних налаштувань та властивостей веб-сайту здійснювалася через контекстне меню «Properties» (Властивості). Наразі такий підхід є неможливим, оскільки вікна властивостей та вкладки зазнали серйозної реконструкції в IIS 7, IIS 7.5 та IIS 8. Їх замінили значки компонентів у центральній панелі та завдання у панелі дій. У центральній панелі відомостей наявна вкладка «Features View» (Представлення компонентів), де розташовані значки, пов’язані з налаштуванням властивостей веб-сайту. Вони дозволяють управляти аспектами розробки додатка, компонентами HTTP, працездатністю, діагностикою,

продуктивністю та безпекою. Конкретні компоненти на центральній панелі залежать від встановлених служб та об’єкта, вибраного в панелі підключень, і за замовчуванням розбиті на категорії: компоненти, пов’язані з ASP.NET, компоненти, пов’язані з IIS, та компоненти, пов’язані з управлінням.

Компоненти, пов’язані з ASP.NET, включають сторінку «.NET Authorization Rules» (Правила авторизації .NET), яка дозволяє управляти доступом до веб-сайту та додатка за допомогою правил «Allow» (Дозволити) і «Deny» (Заборонити), вказуючи користувачів, ролі та групи [4].

Сторінка «.NET Compilation» (Компіляція .NET) дозволяє налаштовувати параметри конфігурації ASP.NET і складається з розділів «Batch», «Behavior», «General» та «Assemblies».

Сторінка «.NET Error Pages» (Сторінки помилок .NET) призначена для налаштування HTTP-сторінок відповідей на випадки виникнення помилок. «.NET Globalization» (Глобалізація .NET) дозволяє налаштовувати інтернаціональні параметри відповідно до локальної мови та культури, що є важливим засобом для перекладу та форматування контенту.

Сторінка «.NET Profile» (Профіль .NET) надає доступ до властивостей профілю, а «.NET Roles» (Ролі .NET) дозволяє створювати зумовлені ролі для управління авторизацією груп (захист на основі ролей), що вимагає налаштування провайдерів AspNetWindowsTokenRoleProvider або AspNetSqlRoleProvider.

Сторінка «.NET Trust Levels» (Рівні довіри .NET) дозволяє вказувати рівень довіри для керованих об’єктів у файлі Web.config, а сторінка «.NET Users» (Користувачі .NET) дозволяє управляти ідентифікаційними даними користувачів.

Також до цієї групи належить сторінка «Application Settings» (Параметри додатка), яка рекомендується для управління змінними, що зберігаються у вигляді пар ключ/значення у файлі конфігурації.

Сторінка «Connection Strings» (Рядки підключення) дозволяє створювати та керувати рядками підключення до баз даних, наприклад SQL Server. Сторінка «Machine Key» (Ключ комп'ютера) дозволяє управляти шифруванням та ключами хешування для додатків, що важливо для захисту автентифікації та даних стану.

Сторінка «Pages and Controls» (Сторінки та елементи управління) дозволяє налаштовувати компіляцію сторінок ASP.NET. Сторінка «Providers» (Постачальники) дозволяє адмініструвати список постачальників для ролей, користувачів та профілів .NET.

Сторінка «Session State» (Стан сеансу), використовується для управління поведінкою інформації між сеансами браузера, дозволяючи зберігати стани в браузері або базі даних та налаштовувати обробку cookie-наборів (рис. 10.6). Останній компонент – «SMTP E-Mail»

(Електронна пошта SMTP), сторінка якого містить властивості для управління пересиланням повідомлень з веб-сервера (рис. 10.7).

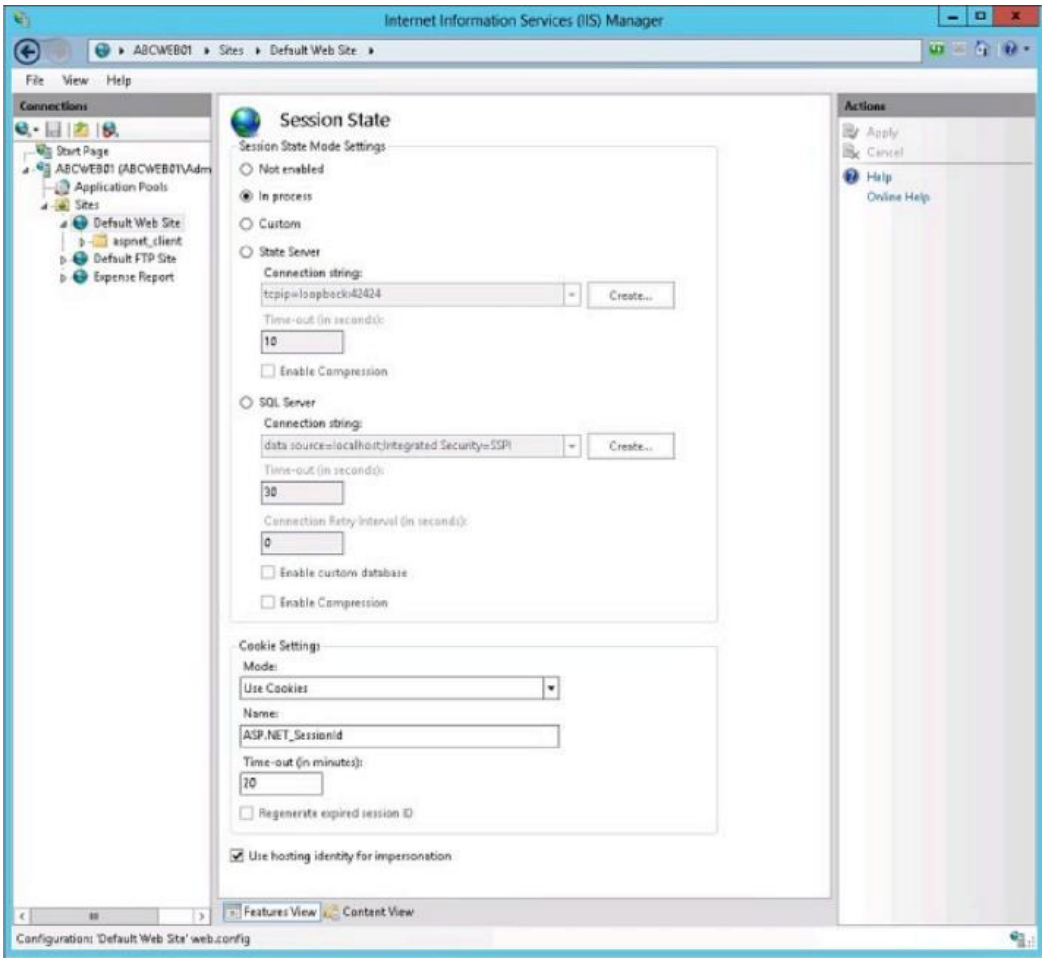

Рисунок 10.6 – Сторінка компонента Session State (Стан сеансу) [4]

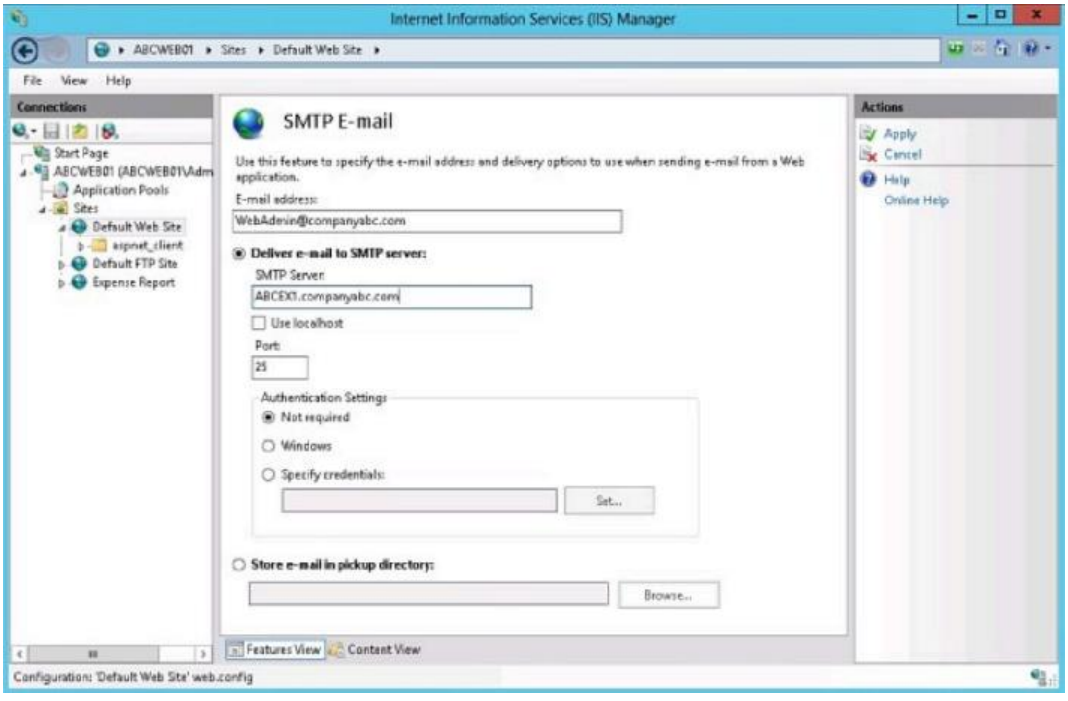

Рисунок 10.7 – Сторінка компонента SMTP E-Mail (Електронна пошта SMTP) [4]

Компоненти, пов’язані з IIS, починаються зі сторінки «ASP», яка призначена для налаштування класичних параметрів ASP, таких як поведінка, компіляція та налагодження. Сторінка «Authentication» (Автентифікація) дозволяє задавати методи безпеки та автентифікації (анонімна, базова, Windows тощо), причому кожен елемент необхідно активувати окремо [4].

Сторінка «Authentication Rules» (Правила автентифікації) дозволяє примусово встановлювати контроль за доступом до веб-контенту. Сторінка «CGI» (Інтерфейс CGI) дозволяє налаштовувати властивості CGI-додатків.

Сторінка «Compression» (Стиснення) надає варіанти стиснення статичного та динамічного контенту для зниження часу передачі даних. Сторінка «Default Document» (Стандартний документ) дозволяє вибрати веб-сторінку, що з’являється за замовчуванням.

Сторінка «Directory Browsing» (Перегляд каталогу) використовується для конфігурування функції перегляду вмісту каталогу. Сторінка «Errors» (Помилки) дозволяє адміністратору створювати спеціальні повідомлення про помилки. Сторінка «Failed Request Tracing Rules» (Правила трасування невдалих запитів) дозволяє налаштовувати правила трасування, що вимагає включення реєстрації невдалих запитів. Також доступні сторінки «FastCGI Settings» для налаштування додатків FastCGI, «Handler Mappings» (Зіставлення обробників) для вказівки ресурсів обробки відповідей, «HTTP Redirect» (Переадресація HTTP) для перенаправлення запитів, та «HTTP Response Headers» (Заголовки відповідей HTTP).

До додаткових компонентів IIS належать «IP Address and Domain Restrictions» (Обмеження на IP-адреси та домени), що дозволяє створювати правила доступу для мереж та IP-адрес, включаючи динамічні обмеження. Сторінка «ISAPI Filters» (Фільтри ISAPI) дозволяє додавати та управляти фільтрами, що реагують на події під час обробки запитів. «Logging» (Ведення журналів) визначає спосіб обробки запитів до журналів. «MIME Types» (Типи MIME) дозволяє налаштовувати список типів MIME. «Modules» (Модулі) дозволяє управляти керованими або власними модулями. «Output Caching» (Кешування виводу) визначає правила кешування контенту. «Request Filtering» (Фільтрація запитів) дозволяє налаштовувати правила фільтрації розширень, URL-адрес та дієслів HTTP. «SSL Settings» (Параметри SSL) допомагає задіяти SSL та налаштувати підтримку клієнтських сертифікатів. Сторінка «Server Certificates» (Сертифікати сервера) надає інтерфейс для управління сертифікатами SSL. Сторінка «WebDav Authoring Rules» (Правила застосування WebDav) містить інформацію про процеси на сервері IIS [4].

Компоненти, пов’язані з управлінням, включають сторінку «Central Certificates» (Центр управління сертифікатами), яка дозволяє вказати розташування центрального сховища сертифікатів. «Configuration Editor» (Редактор конфігурації) дозволяє управляти

конфігураційними файлами. «Feature Delegation» (Делегування компонентів) використовується для делегування конфігурації різних компонентів IIS. «IIS Manager Permissions» (Дозволи диспетчера IIS) дозволяє управляти доступом користувачів до компонентів. «IIS Manager Users» (Користувачі диспетчера IIS) використовується для підготовки користувачів, яким можна призначати ролі. «Management Service» (Служба управління) використовується для конфігурування доступу дистанційного управління сервером. Нарешті, «Shared Configuration» (Спільне використання конфігурації) використовується для управління конфігураційними файлами для ферм серверів IIS [4].

SSL-сертифікати та безпека

Безперечно, остання версія IIS характеризується значно вищим рівнем безпеки порівняно з попередниками. Кілька важливих удосконалень, таких як скорочення площі вразливості, мінімізація стандартної установки та покращення ізоляції додатків, забезпечують надійну та захищену веб-платформу. Крім того, за замовчуванням в IIS дозволено представлення лише статичної інформації. Для використання додатків або іншого динамічного контенту необхідно включити відповідні компоненти вручну.

Однак саме щодо продуктів Microsoft здійснюється найбільша кількість спроб злому. Тому важливо максимально захистити веб-сервер. Чим більше бар'єрів встановлено, тим менше у зловмисника буде бажання намагатися отримати несанкціонований доступ. Кожен компонент на веб-сервері повинен бути захищеним. Загальна безпека сервера визначається безпекою його найслабшої ланки.

Варто зазначити, що забезпечення безпеки Windows Server 2025 розпочинається з опрацювання всіх можливих проблем з безпекою ще на етапі планування та проектування – на фізичному рівні, логічному рівні (операційна система, додатки тощо) та на рівні мережевих підключень.

При забезпеченні безпеки системи Windows Server 2025 з роллю Web Server (IIS) важливо підтримувати актуальність сервера та застосовувати всі свіжі пакети оновлень і виправлення безпеки. Це дозволить Windows Server 2025 функціонувати зі значно вищим ступенем захисту. У системі Windows Server 2025 з роллю Web Server (IIS) слід ретельно перевірити захист додатків, особливо нестандартних. Усі додатки, розроблені сторонніми виробниками, повинні бути сертифіковані на сумісність з Windows Server. Також слід переглянути всі рекомендації постачальників щодо їх налаштування та захисту і, якщо це доцільно, реалізувати їх [3].

Автентифікація визначається як процес перевірки того, чи дійсно користувач є тим, за кого себе видає. В IIS підтримується велика кількість методів автентифікації:

Анонімна автентифікація – користувачі можуть підключатися до веб-сайту без

пред’явлення своїх повноважень.

Автентифікація сертифікатів клієнтів Active Directory (Active Directory Client Certificate Authentication) – користувачі можуть підключатися до веб-сайту за допомогою автентифікації своїх клієнтських сертифікатів Active Directory.

Запозичення прав ASP.NET (ASP.NET Impersonation) – користувачі можуть використовувати для автентифікації обліковий запис ASP.NET.

Автентифікація Windows може інтегруватися з Active Directory. Після входу користувачів у систему замість пароля передається значення його хешу.

Дайджест-автентифікація, схожа на попередній метод автентифікації і тут також передається хеш пароля, але для перевірки його достовірності необхідний контролер домену Windows Server.

Базова автентифікація – ім’я та пароль користувачів передаються мережею у вигляді відкритого тексту, через що цей метод вважається недостатньо захищеним від несанкціонованого доступу і зазвичай застосовується в поєднанні із захистом сайту або сторінки за допомогою SSL.

Автентифікація за допомогою форм (Forms Authentication): Користувачі перенаправляються на спеціальну сторінку для введення облікових даних. Після проходження автентифікації вони перенаправляються на сторінку, яку запитували спочатку.

Усі ці методи автентифікації включаються на сторінці компонента «Authentication» (Автентифікація), яка показана на рисунку 10.8. Для її відображення необхідно вибрати даний компонент у розділі IIS на потрібному сервері, сайті або у віртуальному каталозі.

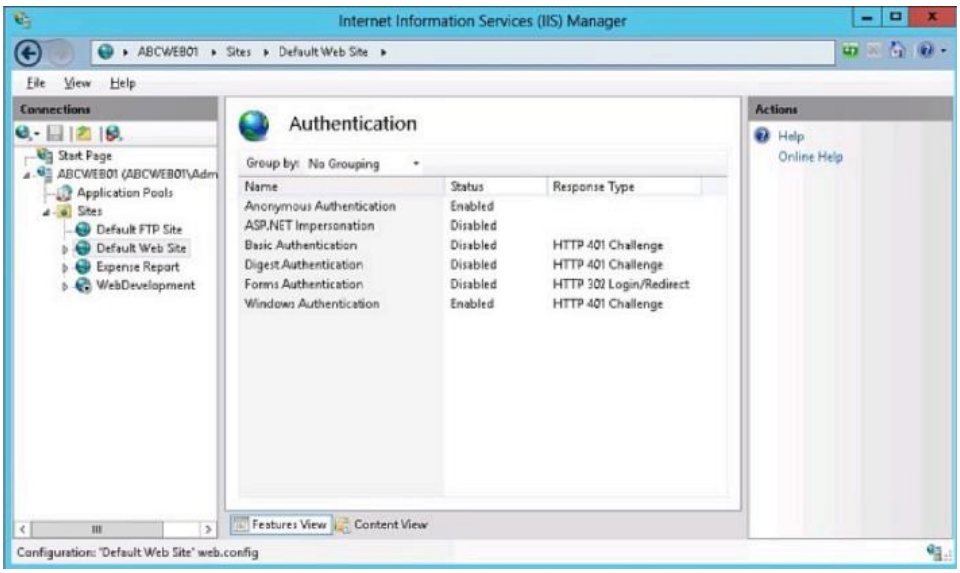

Рисунок 10.8 – Сторінка налаштування автентифікації в IIS [4]

SSL розглядається як критично важлива технологія для захисту даних, якими обмінюються веб-сервер та веб-браузер. Шляхом шифрування переданих даних SSL

забезпечує конфіденційність та цілісність будь-якої комунікації між цими двома сутностями. Коли веб-браузер підключається до веб-сайту, що використовує SSL, він використовує протокол HTTPS, який функціонує через порт 443, для ініціювання захищеного з'єднання.

Це захищене з'єднання встановлюється завдяки використанню цифрових сертифікатів, які є криптографічними документами, виданими довіреними центрами сертифікації (Certificate Authorities – CAs). Ці сертифікати підтверджують автентичність веб-сайту та полегшують встановлення безпечного, зашифрованого каналу зв'язку. Під час цього процесу браузер та сервер використовують сертифікат для узгодження спільного секретного ключа. Цей ключ потім використовується для шифрування всіх даних, що передаються між ними, запобігаючи перехопленню або розшифровці інформації неавторизованими сторонами, тим самим забезпечуючи безпечний та захищений онлайн-досвід [3].

SSL не лише забезпечує конфіденційність даних, але й верифікує легітимність веб-сайту, захищаючи користувачів від потенційних кіберзагроз, таких як фішингові атаки. Використовуючи шифрування, SSL допомагає підтримувати цілісність даних, гарантуючи, що дані залишаються надійними та незмінними під час передачі (рис. 10.9).

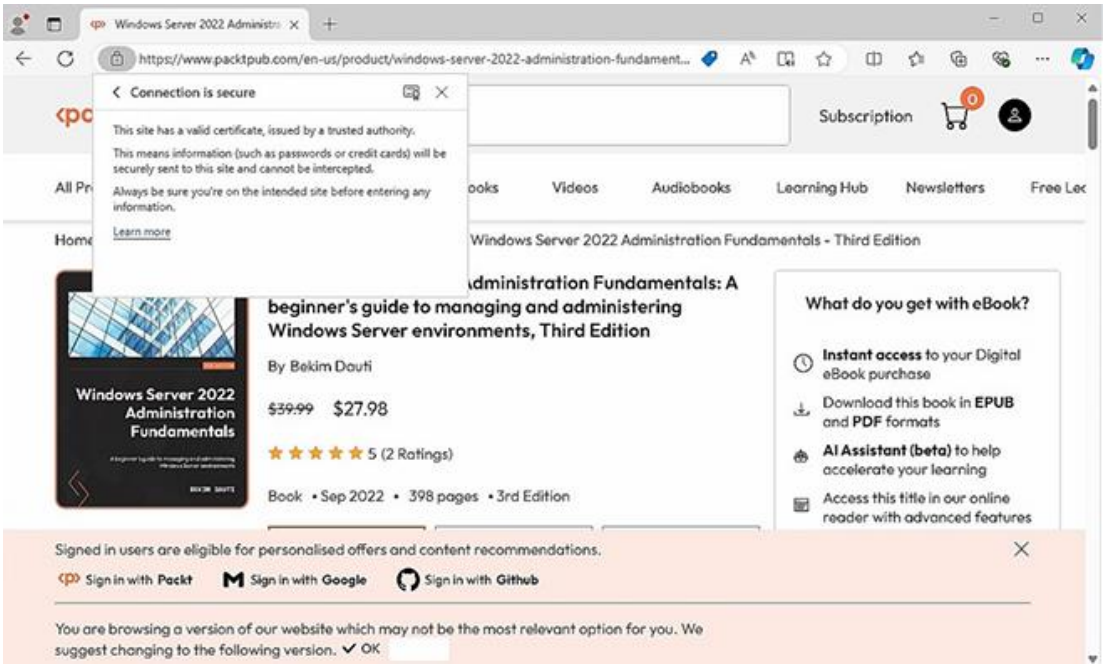

Рисунок 10.9 – Безпечна комунікація між браузером та веб-сайтом [3]

Слід зауважити, що протокол безпеки транспортного рівня (Transport Layer Security – TLS) вдосконалює SSL, усуваючи його обмеження за допомогою покращених функцій безпеки. На відміну від SSL, TLS підтримує більш надійні алгоритми шифрування та безпечніші криптографічні практики, пропонуючи кращий захист від вразливостей та атак. TLS також вдосконалює процес рукостискання та методи валідації сертифікатів, забезпечуючи більш безпечне та стійке з'єднання. Ці досягнення роблять TLS кращим

вибором для захисту даних, що передаються мережами, ефективно долаючи недоліки свого попередника [3].

Цифрові сертифікати є критично важливими для встановлення безпечної комунікації через Інтернет, зокрема між веб-сайтом та браузером. Ці сертифікати, видані довіреною сутністю, відомою як CA, підтверджують ідентичність веб-сайту та уможливлюють зашифрований обмін даними. Як проілюстровано на рисунку 10.10, CA несе відповідальність за валідацію та видачу сертифікатів, гарантуючи, що вони є надійними та точними.

Рисунок 10.10 – Сертифікат, виданий центром сертифікації (CA) [3]

Цифрові сертифікати функціонують у межах інфраструктури відкритих ключів (Public Key Infrastructure – PKI). PKI – це система, спроектована для управління цифровими ключами та сертифікатами, що забезпечує надійний метод верифікації власності відкритих ключів. Кожен сертифікат містить відкритий ключ та інформацію про власника сертифіката, таку як назва організації та адреса. Роль CA полягає у підтвердженні того, що відкритий ключ, який міститься у сертифікаті, дійсно належить сутності, яку він представляє. Цей процес валідації допомагає запобігти шахрайським діям та гарантує, що дані, якими обмінюються, залишаються безпечними [3].

Коли браузер підключається до веб-сайту, що використовує SSL/TLS, цифровий сертифікат використовується для встановлення безпечного з’єднання. Сервер веб-сайту та браузер використовують сертифікат для узгодження спільного ключа шифрування. Цей ключ потім використовується для шифрування та дешифрування даних, якими обмінюються, забезпечуючи конфіденційність чутливої інформації та її захист від несанкціонованого

доступу. Окрім шифрування, цифрові сертифікати також забезпечують цілісність даних та автентифікацію. Вони гарантують, що дані, надіслані між веб-сайтом та браузером, не були підроблені під час передачі, і що ідентичність веб-сайту є справжньою.

В IIS 8 передбачено можливість задавати адміністративні права доступу для серверів, веб-сайтів, каталогів, додатків та сторінок як на рівні Active Directory, так і на рівні локальних користувачів Windows. Окрім цього, для цілей адміністрування IIS можна створити особливі облікові записи. Зазвичай рекомендується використовувати облікові записи Active Directory, оскільки ними легше управляти та їх легше застосовувати у разі адміністрування більше одного або двох серверів IIS. Для управління обліковими записами та безпекою в IIS потрібне встановлення служби «Management Service» (Служба управління). Налаштування SSL для контенту веб-сайту або додатку здійснюється на сторінці «SSL Settings» (рисунку 10.11).

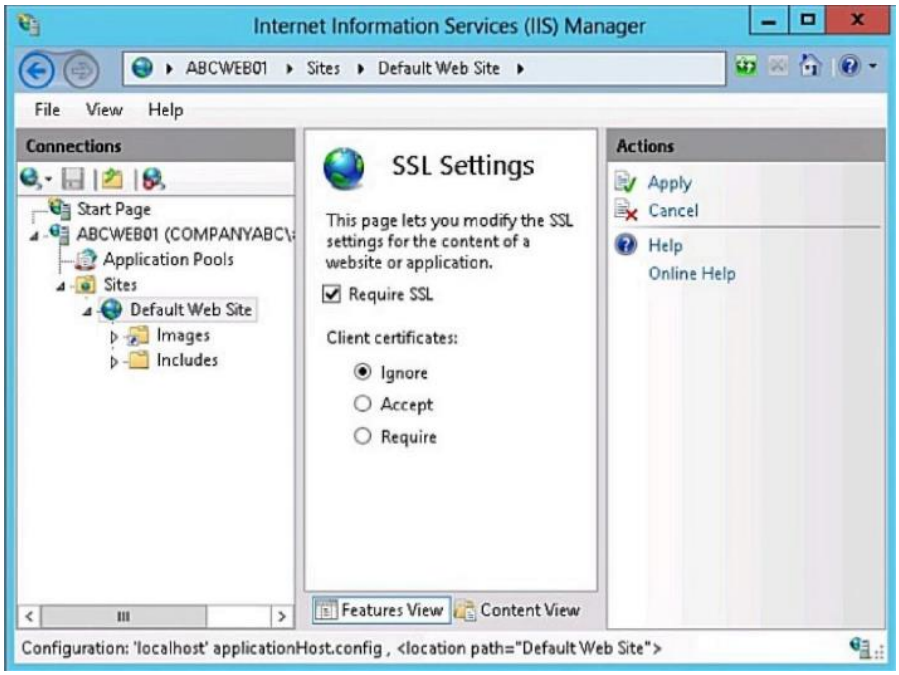

Рисунок 10.11 – Налаштування властивостей на сторінці SSL Settings (Параметри SSL) [4]

Іноді може виникнути потреба надати можливості управління, але без використання облікового запису Active Directory або Windows. Таке часто буває потрібно для авторської підтримки додатку. У подібних випадках може бути створений спеціальний обліковий запис користувача IIS. Такому користувачеві (тільки IIS, але не Windows) можна делегувати права на управління компонентами інфраструктури IIS. Щоб дозволити підтримку облікових записів користувачів IIS, виконуються наступні кроки. У вікні диспетчера IIS здійснюється перехід до панелі «Connections» і обирається потрібний сервер IIS. У центральній панелі відомостей відкривається компонент «Management Service». У розділі «Identity Credentials» (Дані для ідентифікації) вибираються повноваження Windows або «IIS Manager» (Диспетчер

IIS). У панелі «Actions» натискається кнопка «Apply» (Застосувати).

Для створення облікового запису користувача IIS виконуються наступні дії. У вікні диспетчера IIS здійснюється перехід до панелі «Connections» і обирається потрібний сервер IIS. У центральній панелі відомостей відкривається компонент «IIS Manager Users» (Користувачі диспетчера IIS). На сторінці «IIS Manager Users» натискається завдання «Add User» (Додати користувача), що знаходиться в панелі «Actions». У діалоговому вікні «Add User» вводиться ім'я та пароль для нового облікового запису користувача, а потім натискається кнопка «OK». Для подальшого управління обліковим записом користувача після його створення використовуються додаткові завдання в панелі «Actions», які дозволяють змінити пароль, а також тимчасово відключити або видалити обліковий запис [4].

Наступний крок у процесі створення користувача – призначення щойно створеному обліковому запису відповідних прав доступу, щоб користувач міг налаштовувати дозволені компоненти для певного веб-сайту або додатку. Для того щоб дозволити користувачеві підключатися до сайту або додатку, виконуються такі кроки. У диспетчері IIS здійснюється перехід до панелі «Connections», де розгортається вузол потрібного сервера IIS, а потім вузол «Sites» (Сайти). Виділяється сайт, до якого необхідно дозволити підключення даному користувачеві, і в центральній панелі відомостей здійснюється клік на значку «IIS Manager Permissions» (Права доступу диспетчера IIS). На сторінці «IIS Manager Permissions», що відкрилася, натискається посилання «Allow User» (Надати доступ користувачеві) в панелі «Actions». У діалоговому вікні «Allow User» спочатку вибирається варіант «IIS Manager», потім вводяться дані облікового запису, який був створений раніше, і натискається кнопка «OK». Якщо варіант «IIS Manager» буде недоступний у діалоговому вікні «Allow User», це означає, що служба управління не налаштована на прийом підключень від користувачів IIS. Щоб налаштувати її, необхідно скористатися сторінкою «Management Service» для дозволу віддалених підключень, як це було описано вище. Все це впливає на параметри безпеки веб-сервера.

Моніторинг і продуктивність IIS

До веб- та FTP-сайтів можуть застосовуватися засоби аудиту, що постачаються у Windows Server 2025, з метою отримання систематизованої інформації про спроби входу (як успішні, так і невдалі), отримання несанкціонованого доступу до облікових записів служб, зміни або видалення файлів та виконання заборонених команд. Ця інформація доступна для перегляду за допомогою програми «Event Viewer» (Перегляд подій). Окрім цих відомостей, разом із спостережуваними подіями важливо переглядати інформацію в журналах IIS для визначення того, чи були спроби зовнішніх користувачів отримати несанкціонований доступ, і якщо такі спроби мали місце, то яким чином і коли вони відбувалися.

Журнали IIS слід розглядати як обов’язкову, а не просто бажану функціональну можливість IIS, оскільки вони допомагають забезпечувати безпеку IIS та значно полегшують супровід і усунення неполадок. Наприклад, у разі компрометації системи існує можливість ретельно проаналізувати інформацію, зафіксовану в журналах IIS, а потім на підставі цієї інформації переглянути процедури обслуговування та виявити проблеми в системі. Не менш важливим є і те, що в сучасних умовах багато організацій зобов’язані вести журнали для дотримання законодавчих вимог.

За ведення текстових журналів IIS у форматах «W3C Extended Log File Format» (Розширений формат журналов W3C), «Microsoft IIS Log File Format» (Формат журналів Microsoft IIS) та «NCSA Common Log File Format» (Загальний формат журналів NCSA) відповідає процес Http.sys, який функціонує в режимі ядра. У цьому полягає значна відмінність від попередніх версій, де процес ведення журналів працював у режимі користувача. Єдиним форматом, більш схожим на попередні версії, є ODBC, адже він також заснований на робочому процесі, що функціонує в режимі користувача [3].

Ще однією перевагою функції журналювання є можливість її реалізації на рівні сервера, сайту, веб-додатка, файлу або каталогу. Нижче перераховано кроки, необхідні для налаштування ведення журналів IIS для конкретного веб-сайту.

Спершу запускається диспетчер IIS. У панелі «Connections» (Підключення) вибирається веб-сайт, для якого потрібно налаштувати ведення журналів. Після цього необхідно двічі клацнути на елементі «Logging» (Ведення журналів) у панелі «Actions» (Дії). На сторінці «Logging» вибирається потрібний формат ведення журналів. Далі вказується каталог для розміщення файлу журналу: шлях вводиться у текстовому полі «Directory» (Каталог) або обирається потрібний каталог після натискання кнопки «Browse» (Огляд).

У розділі «Log File Rollover» (Перезапис журналу) обирається метод створення нового журналу. Можливі варіанти: «Hourly» (Щогодини), «Daily» (Щодня), «Weekly» (Щотижня) або «Monthly» (Щомісяця). Також можна ввести максимальний розмір файлу (у байтах) або вибрати умову припинення створення нових файлів журналу. В останньому параметрі вказується, чи слід застосовувати при іменуванні та створенні файлів журналів локальний час. Після введення всіх параметрів ведення журналу натискається кнопка «Apply» (Застосувати) у панелі «Actions», щоб застосувати зміни.

Варто зауважити, що на сторінці «Logging» (Ведення журналу) можна увімкнути або вимкнути ведення журналу для конкретного сайту. Для цього в панелі «Actions» (Дії) вибирається варіант «Enable» (Увімкнути) або «Disable» (Вимкнути). Для ведення журналів в IIS повинен бути встановлений компонент «HTTP Logging Module» (Модуль ведення журналів HTTP).

Тема 11
Основи Linux-адміністрування. Мережеві служби Linux. Веб-сервісна інфраструктура у Linux

Структура ОС Linux

Структура операційної системи Linux являє собою складну, багаторівневу ієрархічну структуру, яка спроектована для забезпечення ефективного керування апаратними ресурсами обчислювальної машини та надання абстрагованого інтерфейсу для прикладного програмного забезпечення. Фундаментальною основою побудови системи є чітке розмежування простору виконання на привілейований режим, відомий як простір ядра та режим користувача. Така сегрегація реалізується на апаратному рівні через механізм кілець захисту процесора, де ядро функціонує у «кільці 0», маючи повний доступ до пам'яті та периферії, тоді як прикладні програми та системні служби працюють у «кільці 3» з обмеженими правами. Взаємодія між цими двома просторами здійснюється виключно через суворо регламентований інтерфейс системних викликів, що гарантує стабільність роботи сервера. Збій у прикладному додатку не призводить до критичної зупинки всієї операційної системи.

Центральним компонентом системи виступає ядро Linux, яке класифікується як монолітне з можливістю динамічного завантаження модулів. Монолітність архітектури передбачає, що всі критично важливі підсистеми – планувальник процесів, менеджер пам'яті, драйвери пристроїв, мережевий стек та віртуальна файлова система – виконуються в єдиному адресному просторі, що забезпечує високу продуктивність завдяки мінімізації накладних витрат на перемикання контексту. Водночас модульний принцип дозволяє розширювати функціональність ядра без необхідності перезавантаження сервера, шляхом підключення зовнішніх об'єктних файлів. Ця особливість є критично важливою для серверних інфраструктур, де вимагається забезпечення безперервної роботи при зміні апаратної конфігурації або оновленні драйверів [38].

Важливою концептуальною особливістю Linux, успадкованою від систем UNIX, є парадигма «все є файл». Цей принцип уніфікації означає, що доступ до більшості системних ресурсів, включаючи дискові накопичувачі, мережеві сокети, канали міжпроцесної взаємодії та навіть інформацію про стан оперативної пам'яті, здійснюється через стандартні операції читання та запису файлових дескрипторів. Для реалізації цього підходу в ядрі спроектовано прошарок віртуальної файлової системи (VFS), який надає єдиний універсальний інтерфейс для роботи з різнорідними фізичними файловими системами (наприклад, ext4, XFS, Btrfs) та мережевими протоколами. Організація файлового простору підпорядковується стандарту ієрархії файлової системи (Filesystem Hierarchy Standard – FHS), що визначає призначення стандартних каталогів та забезпечує сумісність між різними дистрибутивами та програмним забезпеченням [38].

Управління життєвим циклом системи покладається на підсистему ініціалізації, яка запускається безпосередньо після завантаження ядра і отримує ідентифікатор процесу PID 1. У сучасних дистрибутивах Linux, в тому числі і серверних версіях ОС, цю роль виконує системний менеджер systemd, який замінив застарілу модель SysVinit. Systemd спроектовано для забезпечення паралельного запуску служб, відстеження залежностей між компонентами, керування логуванням через journald та автоматичного перезапуску критичних демонів у разі їх аварійної зупинки. Розуміння механізмів роботи процесу ініціалізації є необхідним для адміністратора, оскільки саме на цьому рівні конфігурується автозавантаження веб-серверів, баз даних та інших мережевих служб, що формують серверну інфраструктуру.

Інтерфейс взаємодії адміністратора з системою реалізується, в основному, через командну оболонку, яка виступає інтерпретатором команд та середовищем для виконання скриптів автоматизації. Оболонка функціонує у просторі користувача і не є частиною ядра, що дозволяє використовувати різні варіанти інтерпретаторів (Bash, Zsh, Sh) залежно від потреб. У серверному середовищі Linux графічний інтерфейс зазвичай відсутній з метою економії ресурсів та підвищення безпеки, тому основна робота з налаштування мережевих служб та моніторингу продуктивності виконується через термінальний доступ. Багатокористувацька природа ОС Linux забезпечується системою прав доступу на основі ідентифікаторів користувачів (UID) та груп (GID), а також атрибутів файлів, що дозволяє чітко розмежувати права на читання, запис та виконання для різних суб’єктів системи, забезпечуючи конфіденційність та цілісність даних у багатокористувацькому середовищі.

Специфіка серверної структури Linux полягає в орієнтації на забезпечення максимальної продуктивності та надійності при обробці конкурентних мережевих запитів, що досягається шляхом використання спеціалізованих профілів планувальника завдань та відмовою від графічної підсистеми хоча є можливість і встановлення графічного компонента для зручності адміністрування.

Робота сервера в режимі «headless» (без монітора та периферії введення) дозволяє вивільнити критичні системні ресурси – процесорний час та оперативну пам’ять – для обслуговування веб-серверів, систем керування базами даних або балансувальників навантаження, замість відмальовування інтерфейсу користувача. Налаштування параметрів ядра через механізм sysctl у серверних дистрибутивах зазвичай виконується з пріоритетом на пропускну здатність мережевого стека та ефективність дискового введення-виводу, на відміну від десктопних систем, де пріоритетом є мінімізація затримок для комфорту користувача. Управління такою інфраструктурою здійснюється дистанційно через захищені криптографічні протоколи, зокрема SSH, що вимагає впровадження суворих політик безпеки та використання засобів автоматизації конфігурування, оскільки фізичний доступ до обладнання в дата-центрах часто є неможливим [38].

Принципи роботи з командним рядком

Взаємодія адміністратора з серверною операційною системою Ubuntu Server здійснюється переважно через командний рядок (Command Line Interface – CLI), який виступає основним інструментом керування системними ресурсами, конфігурацією служб та діагностикою мережевої інфраструктури. На відміну від графічних інтерфейсів, які приховують складність внутрішніх процесів за візуальними абстракціями, командний рядок забезпечує безпосередній доступ до системних викликів та утиліт, дозволяючи виконувати операції з максимальною точністю та ефективністю.

У середовищі Ubuntu Server за замовчуванням використовується командна оболонка Bash (Bourne Again Shell), яка функціонує як інтерпретатор командної мови. Вона зчитує текстові команди, введені користувачем, здійснює їх синтаксичний аналіз та ініціює виконання відповідних програм або системних процедур. Розуміння принципів роботи оболонки є критичним для автоматизації адміністративних завдань, оскільки Bash підтримує змінні, умовні оператори, цикли та функції, перетворюючи командний рядок на повноцінне середовище програмування сценаріїв.

Синтаксична структура команд у середовищі Linux підпорядковується суворому формату, що зазвичай складається з назви утиліти (команди), опцій (ключів або прапорців), які модифікують поведінку програми, та аргументів, що визначають об’єкт дії (файл, каталог, процес або мережевий хост). Процес виконання команди розпочинається з пошуку відповідного виконуваного файлу в файловій системі. Оболонка використовує змінну оточення PATH, яка містить впорядкований перелік директорій, де здійснюється пошук бінарних файлів. Якщо команда не є вбудованою функцією оболонки (наприклад, cd або echo) і не знайдена в шляхах, визначених у змінній PATH, система повертає повідомлення про помилку. Важливою особливістю роботи з аргументами є чутливість файлової системи Linux до регістру символів, що вимагає точності при введенні назв файлів та каталогів, а також використання механізму автодоповнення (tab completion) для підвищення продуктивності та уникнення синтаксичних помилок [38].

Фундаментальною концепцією роботи в командному рядку Unix-подібних систем є модель стандартних потоків введення-виведення, яка забезпечує універсальний механізм обміну даними між процесами. Кожна запущена програма автоматично асоціюється з трьома дескрипторами потоків: стандартним введенням (stdin, дескриптор 0), стандартним виведенням (stdout, дескриптор 1) та стандартним потоком помилок (stderr, дескриптор 2).

За замовчуванням введення здійснюється з клавіатури, а виведення спрямовується на термінал користувача. Проте, архітектура оболонки дозволяє змінювати напрямок цих потоків за допомогою операторів перенаправлення. Це дозволяє зберігати результати роботи програм у файли, ігнорувати повідомлення про помилки або зчитувати вхідні дані з

попередньо підготовлених джерел, що є необхідним для ведення логування та автоматичного виконання завдань без участі оператора.

Особливу потужність командному рядку надає механізм конвеєризації, який реалізується за допомогою символу вертикальної риски (|). Конвеєр дозволяє об'єднувати прості, спеціалізовані утиліти в складні ланцюжки обробки даних, передаючи стандартне виведення однієї команди безпосередньо на стандартне введення іншої. Цей принцип, відомий як філософія Unix («роби одну річ, але роби її добре»), дозволяє адміністратору виконувати складні маніпуляції з текстовими даними, фільтрацію логів, сортування процесів та обробку мережевого трафіку в реальному часі без необхідності написання спеціалізованого програмного забезпечення. Наприклад, комбінація утиліт для перегляду вмісту файлів, пошуку за шаблоном (grep), сортування (sort) та підрахунку унікальних входжень (uniq) є стандартним патерном для аналізу журналів доступу веб-сервера.

Адміністрування Ubuntu Server вимагає чіткого розуміння моделі привілеїв та керування сеансами користувачів. Оскільки пряме використання облікового запису суперкористувача (root) вважається небезпечною практикою, що підвищує ризик випадкового пошкодження системи, в Ubuntu застосовується механізм sudo (SuperUser DO). Цей інструмент дозволяє делегувати адміністративні повноваження звичайним користувачам, вимагаючи підтвердження особистості через введення пароля та логуючи кожну виконану команду з підвищеними правами. Робота в командному рядку також передбачає керування фоновими та активними процесами. Адміністратор має можливість переводити тривалі операції у фоновий режим, призупиняти або завершувати їх за допомогою сигналів, що надсилаються процесам через утиліти керування завданнями або команду kill, забезпечуючи таким чином гнучкий контроль за навантаженням на сервер.

Оскільки доступ до сервера найчастіше здійснюється віддалено, принципи роботи з командним рядком нерозривно пов'язані з використанням протоколу SSH. Цей протокол забезпечує захищений, шифрований канал зв'язку для передачі команд та отримання результатів їх виконання через незахищені мережі. При роботі через SSH командна оболонка функціонує на віддаленому сервері, але відображення результатів відбувається на локальному терміналі клієнта. Це накладає певні особливості на роботу з інтерактивними програмами та вимагає використання термінальних мультиплексорів (наприклад, tmux або screen), які дозволяють зберігати сеанс роботи активним навіть у разі розриву мережевого з'єднання, що є критично важливим при виконанні тривалих оновлень системи або компіляції програмного забезпечення на віддаленому сервері.

Налаштування мережевих параметрів

Конфігурування мережевих інтерфейсів є одним з основних етапів розгортання

серверної інфраструктури, оскільки коректна адресація забезпечує доступність сервісів для клієнтів та взаємодію з іншими вузлами мережі. В операційній системі Linux, зокрема в дистрибутиві Ubuntu Server, керування мережею базується на взаємодії ядра з простором користувача через спеціалізовані демони, такі як NetworkManager або systemd-networkd. Для серверних систем критично важливим є використання статичної IP-адресації замість динамічної (DHCP), оскільки це гарантує постійність точки входу для веб-серверів, баз даних та служб віддаленого доступу. Процес налаштування вимагає розуміння параметрів протоколу IPv4, зокрема IP-адреси хоста, маски підмережі, яка визначає межі широкомовної ділянки мережі, та шлюзу за замовчуванням, що забезпечує маршрутизацію трафіку до зовнішніх мереж.

Алгоритм процесу налаштування статичної адресації можна формалізувати як послідовність логічно пов’язаних етапів. На початковому кроці здійснюється ідентифікація активного мережевого інтерфейсу та отримання прав доступу до зміни його конфігурації. Другий етап передбачає переведення методу отримання адреси з автоматичного режиму в ручний, що виключає вплив DHCP-сервера на параметри хоста. Третій етап полягає у безпосередньому введенні мережевих реквізитів (адреса, маска, шлюз, DNS-сервери) у відповідні конфігураційні файли або графічні форми. Четвертий етап вимагає перезапуску мережевої служби або інтерфейсу для ініціалізації нових параметрів ядром системи. Завершальним етапом є верифікація з’єднання шляхом надсилання ехо-запитів до шлюзу та зовнішніх вузлів [38].

При використанні серверних дистрибутивів ОС із встановленим графічним оточенням, налаштування часто виконується через графічний інтерфейс користувача, що дозволяє візуалізувати параметри NetworkManager. Процедура розпочинається із запуску екземпляра Linux Server, розгорнутого в результаті виконання попередніх етапів проектування інфраструктури. Після завантаження операційної системи здійснюється автентифікація в системі під обліковим записом користувача, що має відповідні права. Налаштування ініціюється відкриттям утиліти системних параметрів («Settings»), де необхідно обрати розділ керування мережею («Network»). У переліку доступних апаратних інтерфейсів обирається провідне з’єднання («Wired»), після чого здійснюється перехід до режиму редагування параметрів шляхом натискання на піктограму конфігурації (шестерні), як це продемонстровано на рисунку 11.1.

Внаслідок виконання вищезазначених дій ініціюється вікно налаштувань конкретного підключення, що містить деталізовані параметри мережевого адаптера. Для зміни схеми адресації необхідно здійснити перехід у вкладку «IPv4» у вікні, що відкрилося, яка відповідає за конфігурацію протоколу Інтернет четвертої версії (рис. 11.2).

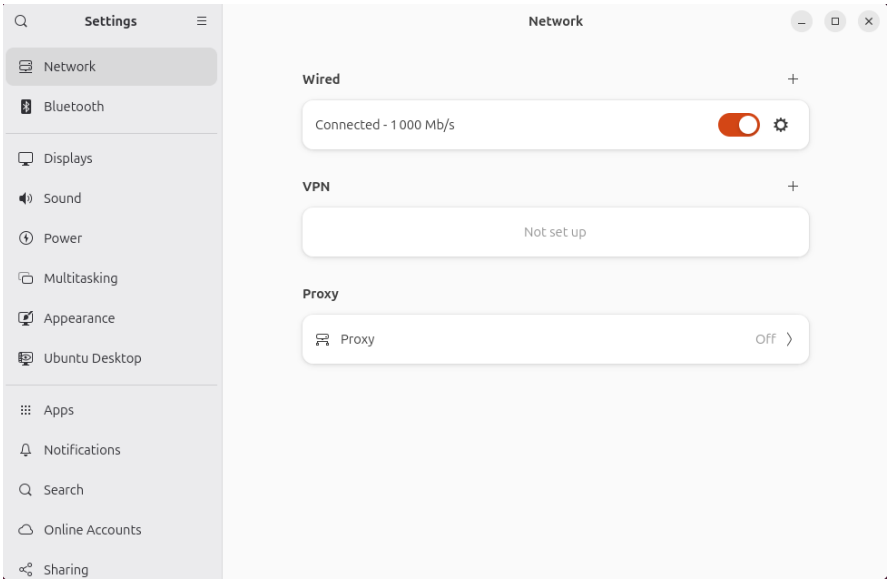

Рисунок 11.1 – Налаштування мережі [38]

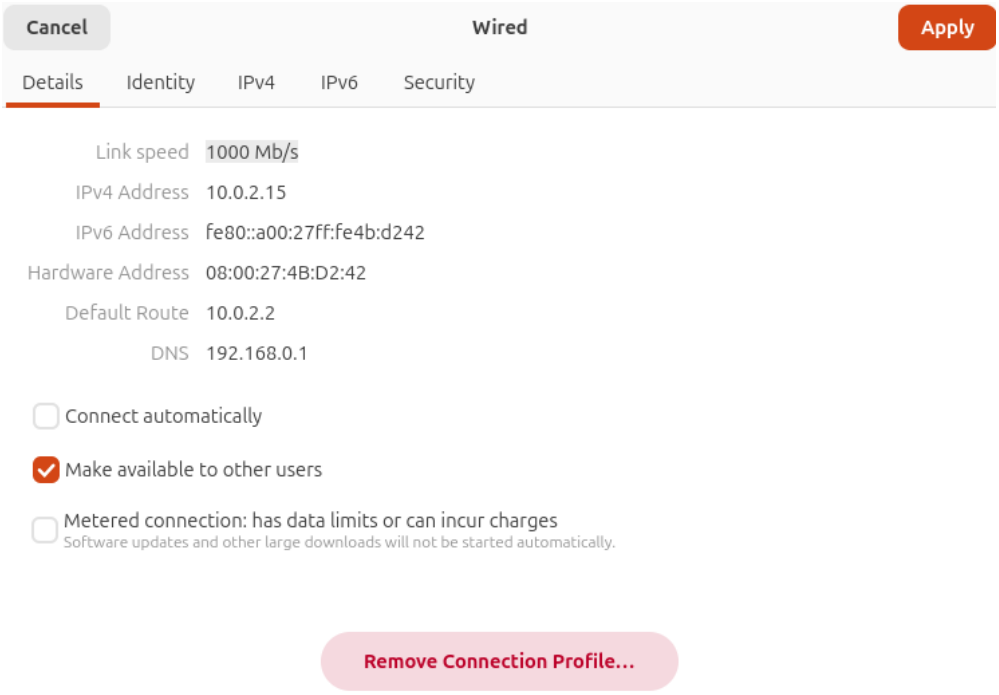

Рисунок 11.2 – Налаштування провідного з’єднання мережі [38]

У межах вкладки «IPv4» здійснюється ключова зміна логіки роботи інтерфейсу: у полі вибору методу присвоєння адреси («Method») встановлюється значення «Manual» (Ручний), що деактивує клієнт DHCP. Далі у секції «Addresses» виконується введення детермінованих мережевих параметрів, визначених топологією мережі. Зокрема, у відповідні поля вносяться наступні значення: IP-адреса хоста – наприклад, 192.168.56.10; маска підмережі – наприклад, 255.255.255.0, що відповідає префіксу /24; та шлюз за замовчуванням – наприклад, 192.168.56.1. Фіксація внесених змін здійснюється натисканням кнопки «Apply» (Застосувати). Для того щоб нові параметри набули чинності на рівні ядра, необхідно

виконати реініціалізацію інтерфейсу шляхом його вимкнення та повторного ввімкнення засобами графічного інтерфейсу (рис. 11.3)

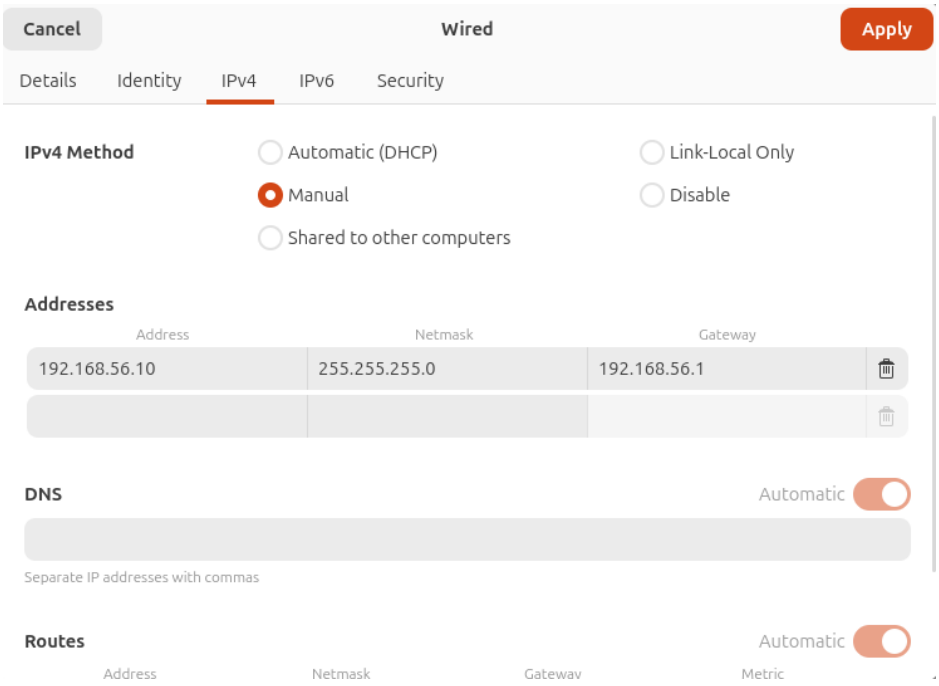

Рисунок 11.3 – Налаштування статичної IP-адресації для сервера [38]

Завершальним етапом конфігурування є верифікація застосованих параметрів та перевірка доступності вузлів мережі. Для діагностики використовується емулятор термінала, в якому виконуються команди перевірки мережевого стека. Команда ip addr show дозволяє пересвідчитися, що інтерфейсу дійсно присвоєно статичну адресу 192.168.56.10.

Наступним кроком виконується перевірка зв'язності з локальним шлюзом за допомогою команди ping -c 4 192.168.56.1, яка надсилає чотири ICMP-пакети. Аналогічна перевірка здійснюється для зовнішнього вузла (наприклад, DNS-сервера Google) командою ping -c 4 8.8.8.8. Успішне отримання відповідей на ехо-запити свідчить про коректність налаштування статичної IP-адресації та працездатність маршрутизації.

Управління користувачами

Основою безпеки та організації роботи в операційній системі Linux, і зокрема в дистрибутиві Ubuntu Server, є концепція багатокористувацького середовища. Архітектура системи спроектована таким чином, що кожен процес, який виконується в просторі користувача, повинен бути асоційований з певним суб'єктом – обліковим записом користувача. Цей підхід дозволяє ядру операційної системи реалізовувати механізми розмежування доступу, ізоляції процесів та аудиту дій.

З точки зору ядра, користувач ідентифікується не за текстовим іменем (логіном), а за унікальним числовим ідентифікатором – UID (User Identifier). Аналогічним чином, для

групування користувачів та надання їм спільних прав доступу використовується ідентифікатор групи – GID (Group Identifier). Процес трансляції зрозумілих людині текстових імен у числові ідентифікатори та навпаки здійснюється системними бібліотеками шляхом звернення до спеціалізованих баз даних облікових записів [38].

Центральним сховищем інформації про користувачів у системі є файл /etc/passwd. Цей файл являє собою текстову базу даних, де кожен рядок описує окремий обліковий запис і складається з семи полів, розділених двокрапкою. Перше поле містить логін користувача, який використовується при автентифікації. Друге поле історично призначалося для зберігання хешу пароля, проте в сучасних системах, з міркувань безпеки, там розміщується символ «x», що вказує на перенесення криптографічних даних у захищений файл /etc/shadow. Третє та четверте поля містять, відповідно, UID користувача та GID його основної групи. П’яте поле, відоме як GECOS, використовується для зберігання додаткової інформації, такої як повне ім’я користувача, номер кабінету чи телефон. Шосте поле визначає абсолютний шлях до домашнього каталогу користувача, де зберігаються його особисті файли та налаштування. Сьоме поле вказує на командну оболонку, яка буде запущена автоматично після успішного входу в систему. Якщо в цьому полі вказати /sbin/nologin або /bin/false, вхід для даного користувача буде заблоковано, що часто використовується для сервісних облікових записів.

Важливим аспектом адміністрування є розуміння ієрархії користувачів. Користувач з UID 0 (root) має необмежені права доступу до всіх ресурсів системи, ігноруючи будь-які перевірки прав доступу. Діапазон UID від 1 до 999 (у більшості сучасних дистрибутивів, включаючи Ubuntu) зарезервовано для системних користувачів – спеціальних облікових записів, від імені яких запускаються системні служби (наприклад, www-data для веб-сервера, mysql для бази даних). Це забезпечує принцип найменших привілеїв: якщо зловмисник скомпрометує веб-сервер, він отримає права лише користувача www-data, а не адміністратора системи. Облікові записи реальних користувачів-людей зазвичай починаються з UID 1000. Коректне управління цими ідентифікаторами є необхідним при налаштуванні спільних файлових сховищ (NFS) або перенесенні архівів між різними серверами для уникнення колізій прав доступу [38].

Безпека автентифікації забезпечується механізмом тіньових паролів, реалізованим у файлі /etc/shadow. Цей файл доступний для читання виключно користувачу root, що унеможливлює проведення атак типу «brute-force» звичайними користувачами системи. У файлі зберігається не сам пароль, а його хеш-сума, отримана за допомогою криптостійких алгоритмів (в Ubuntu Server за замовчуванням використовується SHA-512, що позначається префіксом 6). Окрім хешу, файл містить параметри політики старіння паролів: дату останньої зміни, мінімальний та максимальний термін дії пароля, період попередження про

необхідність зміни та час неактивності, після якого обліковий запис блокується. Адміністратор має можливість керувати цими параметрами за допомогою команди chage, примушуючи користувачів регулярно оновлювати паролі для підвищення загального рівня безпеки інфраструктури.

Процес створення нового користувача в Ubuntu Server може виконуватися за допомогою низькорівневої утиліти useradd або високорівневого скрипта adduser. Використання useradd надає адміністратору повний контроль над процесом, дозволяючи вручну вказати UID, GID, домашній каталог та інші параметри, але вимагає чіткого розуміння ключів запуску.

Натомість adduser, який є інтерактивною надбудовою над useradd у системах Debian/Ubuntu, автоматизує більшість рутинних операцій: він створює домашній каталог, копіює в нього конфігураційні файли за замовчуванням, пропонує ввести пароль та інформацію GECOS (рис. 11.4). При створенні домашнього каталогу система використовує шаблон, що знаходиться в директорії /etc/skel. Усі файли (зазвичай це приховані налаштування оболонки, такі як .bashrc та .profile), які розміщені в /etc/skel, автоматично копіюються до домашньої папки нового користувача, забезпечуючи стандартизоване початкове оточення.

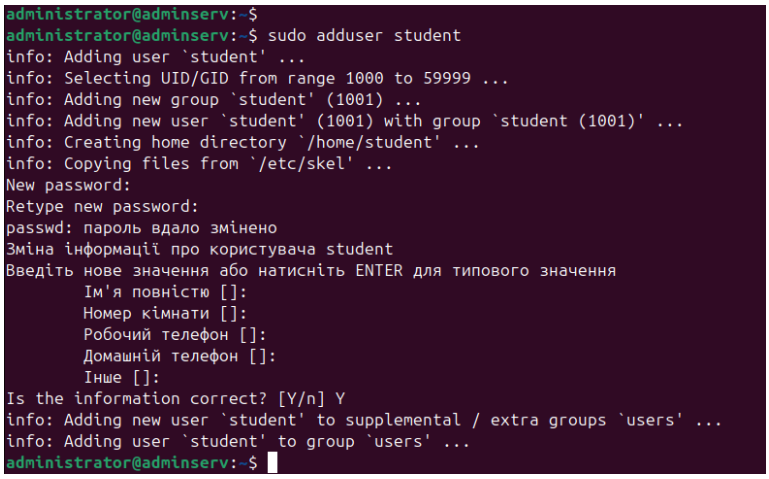

Рисунок 11.4 – Створення нового користувача з використанням adduser [38]

Керування групами є невід’ємною складовою моделі доступу. Кожен користувач повинен мати одну основну групу (primary group), GID якої записується в /etc/passwd. При створенні файлів новим користувачем, ці файли автоматично отримують групу-власника, що відповідає основній групі користувача. Окрім основної, користувач може бути членом довільної кількості додаткових груп (supplementary groups), інформація про які зберігається у файлі /etc/group. Це дозволяє гнучко налаштовувати доступ до проектних директорій або системних функцій. Наприклад, в Ubuntu членство в групі sudo надає адміністративні права,

а група docker дозволяє керувати контейнерами без використання sudo. Модифікація членства в групах здійснюється командою usermod з ключами -aG (append group), де критично важливо використовувати ключ додавання -a, щоб не перезаписати існуючий список груп користувача (рис. 11.5).

```
administrator@adminserv:~$ sudo groupadd Students_KI
administrator@adminserv:~$
administrator@adminserv:~$ sudo usermod -aG Students_KI student
administrator@adminserv:~$
administrator@adminserv:~$ groups student
student : student users Students_KI
administrator@adminserv:~$
```

Рисунок 11.5 – Робота з групами в Ubuntu Server [38]

В Ubuntu Server за замовчуванням обліковий запис root заблокований (не має встановленого пароля), що унеможливлює прямий вхід в систему під цим ім'ям. Замість цього використовується механізм делегування повноважень sudo (SuperUser DO). Цей підхід значно підвищує безпеку, оскільки дозволяє адміністраторам виконувати привілейовані команди, використовуючи власний пароль, що забезпечує персоніфікований аудит дій у системних журналах. Конфігурація прав доступу sudo визначається у файлі /etc/sudoers. Редагування цього файлу повинно виконуватися виключно за допомогою спеціалізованої команди visudo, яка здійснює перевірку синтаксису перед збереженням.

Помилка в синтаксисі /etc/sudoers, допущена при прямому редагуванні текстовим редактором, може призвести до повної втрати можливості адміністрування системи. Синтаксис файлу дозволяє налаштовувати права з високою точністю, оскільки можна дозволити конкретному користувачу виконувати лише певний набір команд від імені root або іншого користувача, і навіть без запиту пароля.

Основою системи захисту файлової системи Linux є модель дискреційного розмежування доступу (Discretionary Access Control – DAC). Для кожного файлу або каталогу в файловій системі зберігаються атрибути, що визначають права доступу для трьох категорій суб'єктів: власника файлу (user), групи-власника (group) та всіх інших користувачів (others). Права визначаються трьома базовими дозволами: читання (r – read), запис (w – write) та виконання (x – execute). Інтерпретація цих прав відрізняється для файлів та каталогів. Для файлу право r дозволяє зчитати його вміст, w – змінити вміст, а x – запустити файл як програму. Для каталогу право r дозволяє отримати список файлів у ньому, w – створювати або видаляти файли в каталозі, а x – входити в каталог (робити його поточним) та отримувати доступ до метаданих файлів у ньому [38].

Управління правами доступу здійснюється за допомогою команди chmod (change mode), яка підтримує два режими нотації: символьний та вісімковий (октальний) (рис. 11.6).

У вісімковій системі правам присвоюються числові ваги: читання – 4, запис – 2, виконання – 1. Сума цих значень формує цифру прав для кожної категорії користувачів. Наприклад, комбінація 754 (rwxr-xr--) означає повні права для власника, права лише на читання і виконання для групи та виключно на читання для інших. Зміна власника файлу виконується командою chown (change owner), а групи – chgrp (change group) (рис. 11.7). Важливим поняттям є umask (user mask) – маска режиму створення файлів користувача, яка визначає права доступу за замовчуванням для новостворених об'єктів. Значення маски віднімається від базових повних прав, що дозволяє адміністратору глобально обмежувати права на нові файли для забезпечення конфіденційності.

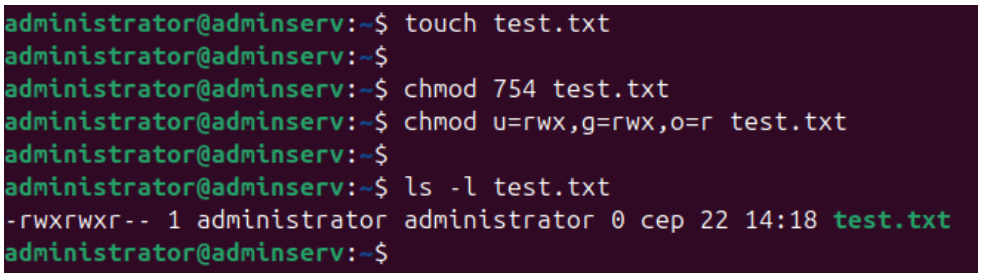

Рисунок 11.6 – Управління правами доступу в Ubuntu Server двома режимами нотації [38]

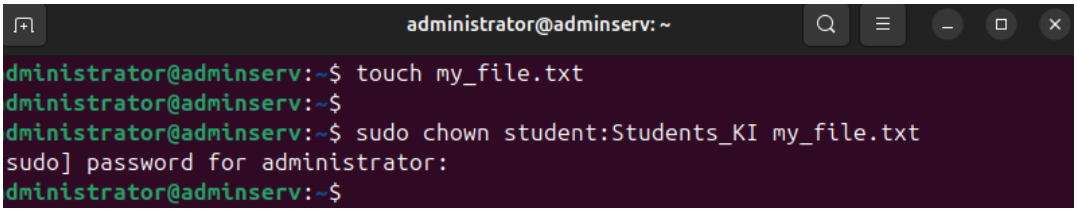

Рисунок 11.7 – Зміна власника файлу в Ubuntu Server [38]

Крім стандартних прав rwx, Linux підтримує спеціальні біти доступу: SUID (Set User ID), SGID (Set Group ID) та Sticky Bit. Встановлення біта SUID на виконуваний файл дозволяє звичайному користувачеві запускати програму з правами власника файлу (зазвичай root). Це механізм, який використовують такі утиліти, як passwd або ping, що потребують привілейованого доступу до системних ресурсів. Біт SGID на каталозі забезпечує спадкування групи-власника, тобто нові файли, створені в такому каталозі, отримують групу каталогу, а не основну групу користувача, що є ключовим для організації спільних робочих просторів. Sticky Bit встановлюється на каталоги загального доступу (наприклад, /tmp) і забороняє користувачам видаляти файли, власниками яких вони не є, навіть якщо вони мають право запису в каталог. У випадках, коли стандартної моделі прав недостатньо, застосовуються списки контролю доступу (Access Control Lists – ACL), що дозволяють надавати права на конкретний файл довільній кількості окремих користувачів або груп за допомогою команд setfacl та getfacl.

Принципи безпеки у Linux і відмінність безпеки між Linux і Windows

Забезпечення інформаційної безпеки в операційній системі Linux, зокрема в дистрибутиві Ubuntu Server, базується на комплексній, багаторівневій архітектурі захисту, яка охоплює рівень ядра, простору користувача, файлової системи та мережевих інтерфейсів.

Основним принципом побудови безпечної серверної інфраструктури є концепція «глибокого захисту», яка передбачає створення декількох ешелонів захисту, де компрометація одного рівня не призводить до автоматичного отримання зловмисником повного контролю над системою. У середовищі Linux базовою аксіомою є принцип найменших привілеїв, згідно з яким будь-який процес або користувач повинен мати лише той мінімальний набір прав, який необхідний для виконання поставленого завдання. Цей підхід реалізується як через дискреційні механізми доступу (DAC), розглянуті в попередньому розділі цієї лекції, так і через мандатний контроль доступу (MAC).

Одним із ключових механізмів підвищення безпеки в сучасних дистрибутивах Linux, включаючи Ubuntu, є використання систем примусового контролю доступу (Mandatory Access Control – MAC), таких як AppArmor (Application Armor) або SELinux (Security-Enhanced Linux) [38].

На відміну від стандартної моделі DAC, де власник файлу самостійно визначає права доступу, модель MAC накладає централізовані політики безпеки, які не можуть бути змінені користувачами або навіть скомпрометованими програмами, що запущені з правами суперкористувача. В Ubuntu Server за замовчуванням використовується AppArmor, який працює на основі профілів безпеки, прив’язаних до конкретних виконуваних файлів. Ці профілі чітко регламентують, до яких файлів програма може звертатися, які мережеві порти відкривати та які системні виклики здійснювати. У випадку, якщо вразливість у веб-сервері (наприклад, Nginx) дозволить зловмиснику виконати довільний код, політика AppArmor заблокує спробу доступу до системних файлів, таких як /etc/shadow, навіть якщо процес веб-сервера теоретично мав би відповідні права власності, тим самим локалізуючи інцидент.

Мережева безпека серверного варіанту ОС Linux реалізується безпосередньо в ядрі операційної системи за допомогою підсистеми Netfilter, яка надає інфраструктуру для перехоплення та маніпуляції мережевими пакетами. Адміністрування правил фільтрації трафіку здійснюється через утиліти iptables або більш сучасний nftables.

Для спрощення конфігурації міжмережевого екрану в Ubuntu Server застосовується надбудова UFW (Uncomplicated Firewall), яка дозволяє адміністратору оперувати високорівневими поняттями, такими як дозвіл або заборона трафіку на конкретних портах чи для певних сервісів. Стратегія налаштування брандмауера повинна базуватися на принципі «заборонити все, що не дозволено явно» (default deny). Це означає, що початкова політика для вхідного трафіку встановлюється у значення DROP або REJECT, після чого додаються

виключення лише для критично необхідних портів (наприклад, 22 для SSH, 80/443 для HTTP/HTTPS). Крім того, на рівні ядра налаштовуються параметри захисту від атак типу «відмова в обслуговуванні» (DoS), такі як SYN-cookies, відключення перенаправлення пакетів (IP forwarding) для серверів, що не є маршрутизаторами, та ігнорування ICMP-запитів.

Захист віддаленого доступу до сервера є теж важливим аспектом безпеки сервера, оскільки протокол SSH є основним вектором для спроб несанкціонованого проникнення. Стандартна конфігурація SSH вимагає значного посилення. Першочерговим заходом є повна заборона входу для користувача root через SSH, що змушує адміністратора входити під звичайним обліковим записом і підвищувати привілеї через sudo, залишаючи слід в аудиті. Далі рекомендується відмовитися від автентифікації за паролем на користь використання пар криптографічних ключів (RSA, ED25519), що унеможливлює успішне проведення атак методом підбору пароля (brute-force). Додатковим рівнем захисту є зміна стандартного порту прослуховування 22 на нестандартний для зменшення кількості автоматизованих сканувань, а також використання інструментів типу Fail2Ban, які аналізують логи (журнали) автентифікації в реальному часі та динамічно додають правила в брандмауер для блокування IP-адрес, з яких фіксуються багаторазові невдалі спроби входу [38].

У контексті безпеки веб-сервісної інфраструктури (Apache, Nginx) та файлових служб (Samba, NFS) застосовуються специфічні механізми ізоляції. Одним із найефективніших методів є запуск служб у середовищі chroot (change root), яке змінює видимий кореневий каталог для процесу, ізолюючи його від основної файлової системи. Це гарантує, що навіть у разі зламу веб-сервісу зловмисник не зможе вийти за межі визначеного дерева каталогів. Також важливою є регулярна перевірка конфігурації SSL/TLS – відключення застарілих версій протоколів (SSLv3, TLS 1.0, 1.1) та слабких шифрів, налаштування HSTS (HTTP Strict Transport Security) для запобігання атакам зі зниженням рівня захисту.

Система аудиту та журналювання подій у Linux виконує роль «чорної скриньки», дозволяючи реконструювати послідовність подій у разі інциденту з безпекою. Центральним елементом журналювання є rsyslog або journald (у системах із systemd), які збирають повідомлення від ядра та служб. Для забезпечення цілісності журналів на серверах із високими вимогами до безпеки налаштовується відправка логів на віддалений виділений сервер у реальному часі. Це гарантує, що зловмисник, отримавши доступ до сервера, не зможе знищити сліди своєї діяльності, оскільки копії журналів вже будуть збережені на іншому вузлі. Додатково використовується підсистема Linux Audit Framework (auditd), яка дозволяє налаштувати детальне відстеження системних викликів, доступу до конкретних файлів або зміни атрибутів, надаючи значно детальнішу інформацію, ніж стандартні логи.

Проведення порівняльного аналізу безпеки серверних операційних систем Linux та

Windows вимагає розгляду архітектурних відмінностей, моделей управління доступом та екосистем програмного забезпечення. Першою суттєвою відмінністю є модель розробки, адже Linux базується на відкритому вихідному коді, тоді як Windows є пропрієтарною системою із закритим кодом.

Архітектурна відмінність також полягає в способі зберігання конфігурації. У Linux усі налаштування зберігаються у текстових файлах, що спрощує їх перевірку, версіонування (через Git) та автоматизований аудит за допомогою скриптів. У Windows конфігурація зосереджена у Реєстрі – ієрархічній базі даних, яка є бінарною, менш прозорою та складнішою для аналізу змін без спеціалізованих інструментів. Крім того, Linux є модульною системою, де адміністратор може і повинен видалити всі непотрібні компоненти, зменшуючи поверхню атаки. Ядро Windows є більш монолітним у своїй комерційній поставці, і хоча існують варіанти Windows Server Core або Nano Server, стандартні інсталяції часто містять значну кількість успадкованих компонентів та графічний інтерфейс.

Суттєві відмінності спостерігаються в системах контролю доступу. Windows використовує складну систему списків контролю доступу (ACL) для NTFS та об'єктів Active Directory, яка забезпечує надзвичайно високу гранулярність прав (наприклад, окремі права на створення папок, запис атрибутів, зміну дозволів), але є складною в адмініструванні та діагностиці конфліктів. Linux використовує простішу модель rwx (читання/запис/виконання), доповнену списками ACL POSIX та атрибутами. Модель Windows є більш гнучкою та кращою в сфері систем контролюю доступу, проте модель Linux у поєднанні з SELinux/AppArmor надає дещо кращі можливості для ізоляції процесів. У Windows механізм UAC (User Account Control) виконує функцію, аналогічну sudo в Linux [3].

Окремо слід виділити питання шкідливого програмного забезпечення. Статистично, переважна більшість вірусів, троянів та програм-вимагачів створюється для середовища Windows. Це зумовлено як домінуванням Windows на десктопному ринку, так і можливістю виконання бінарних файлів (.exe), завантажених з довільних джерел в Інтернеті. У Linux інсталяція програмного забезпечення здійснюється переважно з довірених репозиторіїв пакетів (APT, YUM), які підписуються цифровими ключами розробників дистрибутиву. Це створює «ланцюг довіри», який значно ускладнює розповсюдження шкідливого ПЗ. Для запуску вірусу в Linux користувач часто повинен свідомо надати файлу права на виконання та ввести пароль адміністратора, що робить випадкове зараження малоймовірним. Проте, Linux-сервери є пріоритетною ціллю для складних таргетованих атак, спрямованих на веб-сервіси та бази даних, а не на саму ОС і в цьому поступаються Windows Server.

В аспекті оновлень та патч-менеджменту підхід Linux дозволяє оновлювати всі встановлені компоненти системи (ядро, бібліотеки, прикладне ПЗ) однією командою через пакетний менеджер. Windows Server має централізовану службу Windows Update для

швидкого виконання оновлень.

Також Windows пропонує більш потужні інструменти централізованого управління політиками безпеки через об'єкти групових політик (GPO) в середовищі Active Directory, що є беззаперечним стандартом для корпоративних мереж, тоді як в Linux аналогічний рівень централізації досягається використанням інструментів конфігураційного управління (Ansible, Puppet, Chef) або LDAP-рішень (FreeIPA), які вимагають вищої кваліфікації для впровадження, є більш складними у всіх аспектах та не перевершують можливості Windows Server [3].

Встановлення та налаштування DHCP і DNS у Linux

Протокол динамічної конфігурації хостів (DHCP) є надважливим елементом мережевої інфраструктури, що забезпечує автоматизований розподіл IP-адрес та супутніх параметрів (маски підмережі, шлюзу за замовчуванням, DNS-серверів) клієнтським пристроям. В ОС Linux найбільш поширеним та стабільним рішенням для реалізації DHCP-сервера є пакет ISC DHCP Server, розроблений Internet Systems Consortium. Його використання дозволяє мінімізувати ймовірність виникнення конфліктів IP-адрес та значно спрощує адміністрування мережі, особливо в середовищах з великою кількістю мобільних клієнтів. Робота протоколу базується на клієнт-серверній архітектурі та використовує транспортний протокол UDP, де обмін повідомленнями відбувається за моделлю DORA (Discover, Offer, Request, Acknowledge). Сервер прослуховує порт 67, а клієнти відправляють запити з порту 68.

Процес розгортання служби DHCP на базі Ubuntu Server розпочинається з оновлення індексу пакетів для гарантування завантаження актуальних версій програмного забезпечення. Встановлення здійснюється за допомогою пакетного менеджера apt шляхом інсталяції пакета isc-dhcp-server. Характерною особливістю першого запуску служби після інсталяції є можлива поява повідомлення про помилку запуску. Це є штатною ситуацією, зумовленою тим, що конфігураційний файл за замовчуванням не містить визначень підмереж, які відповідали б наявним мережевим інтерфейсам сервера. Для коректної роботи служби необхідно виконати налаштування прив'язки до мережевого інтерфейсу. Це здійснюється шляхом редагування файлу /etc/default/isc-dhcp-server, де у параметрі INTERFACESv4 вказується ім'я фізичного інтерфейсу (наприклад, eth0 або ens33), через який сервер буде обслуговувати запити клієнтів. Таке обмеження є важливим заходом безпеки, що запобігає випадковій видачі адрес у зовнішні мережі [38].

Основним конфігураційним файлом сервера є /etc/dhcp/dhcpd.conf. Перед початком налаштування рекомендується створити резервну копію оригінального файлу для можливості відкату змін. Структура файлу складається з глобальних параметрів та секцій оголошення

підмереж. На початку файлу визначаються загальні налаштування для всіх клієнтів: доменне ім’я та адреси DNS-серверів.

Важливим параметром є директива authoritative, розкоментування якої вказує, що даний DHCP-сервер є головним у мережі. Якщо цей параметр не активовано, сервер ігноруватиме запити клієнтів на поновлення адрес, виданих іншими серверами, що може призвести до затримок у підключенні. Також задаються параметри часу оренди: default-lease-time (час у секундах, на який видається адреса, якщо клієнт не запитав інше) та max-lease-time (максимально допустимий час оренди).

Ключовим етапом конфігурування DHCP на базі Ubuntu Server є оголошення підмережі. Синтаксис вимагає опису мережі, яка відповідає IP-адресі інтерфейсу сервера. У блоці subnet вказується адреса мережі та маска підмережі. Внутрішні параметри блоку включають діапазон адрес для динамічного розподілу, який визначає пул доступних IP-адрес (наприклад, від 192.168.1.100 до 192.168.1.200). Окрім діапазону, обов’язково вказується шлюз за замовчуванням, який клієнти використовуватимуть для виходу в інші мережі. Важливо пам’ятати, що адреса самого DHCP-сервера повинна бути статичною і знаходитися поза межами діапазону динамічної видачі range, щоб уникнути конфлікту адрес.

Окрім динамічного розподілу, ISC DHCP Server дозволяє налаштовувати резервування адрес, що гарантує отримання конкретним пристроєм незмінної IP-адреси. Це є необхідним для мережевих принтерів, файлових серверів або точок доступу. Резервування реалізується через блок host, у якому вказується довільне ім’я хоста, MAC-адреса мережевої карти пристрою (параметр hardware ethernet) та фіксована IP-адреса, що присвоюється цьому клієнту. Така конфігурація дозволяє централізовано керувати адресацією критичної інфраструктури без необхідності ручного налаштування мережевих параметрів на кожному окремому пристрої.

Після завершення редагування конфігураційних файлів виконується перезапуск служби isc-dhcp-server за допомогою системи ініціалізації systemd. Для діагностики роботи сервера використовується команда перевірки статусу служби, а також аналіз системних журналів. Інформація про видані адреси зберігається у файлі бази даних оренди /var/lib/dhcp/dhcpd.leases. Цей файл містить записи про всі активні та минулі оренди, включаючи час видачі, час закінчення дії, MAC-адресу клієнта та його ім’я хоста. Періодичний моніторинг цього файлу дозволяє адміністратору оцінювати утилізацію адресного простору та виявляти несанкціоновані підключення до локальної мережі. Налаштування DHCP-сервера є фундаментом для подальшого розгортання мережевих служб, зокрема системи доменних імен.

Система доменних імен (DNS) є ієрархічною розподіленою базою даних, що забезпечує перетворення доменних імен, зрозумілих людині, у IP-адреси, необхідні для

маршрутизації пакетів. У середовищі ОС Linux адміністрування DNS традиційно передбачає використання програмного забезпечення BIND (Berkeley Internet Name Domain).

Архітектура DNS розрізняє кілька типів серверів залежно від їхньої ролі в обробці запитів та зберіганні даних зон. Основним типом є первинний або майстер-сервер (Primary/Master DNS Server). Цей сервер зберігає оригінальні файли зон, має повноваження на внесення змін до записів і вважається авторитетним джерелом інформації для відповідного домену. Саме на ньому адміністратор створює та редагує записи ресурсів [39].

Для забезпечення відмовостійкості та розподілу навантаження використовуються вторинні або підлеглі сервери (Secondary/Slave DNS Server). Вторинний сервер не містить власних файлів зон, що редагуються вручну; натомість він отримує копію даних зони з первинного сервера через механізм трансферу зони. Вторинний сервер також є авторитетним для зони, але функціонує в режимі «тільки для читання» відносно бази даних доменних імен.

Процес розгортання DNS-сервера на базі Ubuntu Server розпочинається з підготовки системи. Першочерговим кроком є оновлення списків пакетів репозиторіїв командою apt update та оновлення встановленого програмного забезпечення командою apt upgrade. Це гарантує наявність останніх виправлень безпеки, що є критично важливим для служби, яка обробляє зовнішні запити. Наступним етапом виконується встановлення пакета bind9, який містить сам програмний модуль служби DNS, та bind9utils, що надає набір утиліт для діагностики та керування (наприклад, dig, rndc). Конфігураційні файли BIND в Ubuntu за замовчуванням розміщуються в каталозі /etc/bind (рис. 11.8).

```
root@ns1:~# ls -la /etc/bind/
drwxr-sr-x   2 root bind 4096 Sep 22 16:57 .
drwxr-xr-x 111 root root 4096 Sep 21 18:42 ..
-rw-r--r--   1 root root 2403 Jul 16 18:16 bind.keys
-rw-r--r--   1 root root  255 Jan 25  2024 db.0
-rw-r--r--   1 root root  271 Jan 25  2024 db.127
-rw-r--r--   1 root root  237 Jan 25  2024 db.255
-rw-r--r--   1 root root  353 Jan 25  2024 db.empty
-rw-r--r--   1 root root  270 Jan 25  2024 db.local
-rw-r--r--   1 root bind  458 Jan 25  2024 named.conf
-rw-r--r--   1 root bind  498 Jan 25  2024 named.conf.default-zones
-rw-r--r--   1 root bind  165 Jan 25  2024 named.conf.local
-rw-r--r--   1 root bind  846 Jan 25  2024 named.conf.options
-rw-r-----   1 bind bind  100 Sep 21 18:42 rndc.key
-rw-r--r--   1 root root 1317 Jan 25  2024 zones.rfc1918
```

Рисунок 11.8 – Файли конфігурації DNS-сервера [39]

Архітектура конфігурації BIND модульна. Головний файл named.conf зазвичай не редагується напряму, а містить посилання на інші файли, що дозволяє логічно розділити налаштування. Файл named.conf.options містить глобальні параметри роботи сервера, налаштування безпеки та шляхів. Файл named.conf.local використовується для оголошення

зон (прямої та зворотної), які обслуговує даний сервер. Файл named.conf.default-zones описує стандартні зони, такі як localhost та root hints, і зазвичай залишається без змін.

Налаштування глобальних параметрів DNS здійснюється у файлі /etc/bind/named.conf.options. Для підвищення безпеки створюється список контролю доступу (ACL) з назвою local-network, який визначає довірені підмережі (наприклад, 192.168.1.0/24), яким дозволено надсилати рекурсивні запити до сервера. У блоці options задаються ключові директиви: directory вказує робочу папку кешу; dnssec-validation auto активує перевірку підписів DNSSEC; allow-query обмежує коло клієнтів, що можуть опитувати сервер, використовуючи створений ACL; recursion yes дозволяє серверу виконувати запити до зовнішніх доменів від імені клієнтів; forwarders визначає IP-адреси вищестоящих DNS-серверів (наприклад, 8.8.8.8), куди перенаправляються запити, які сервер не може вирішити самостійно. Також налаштовуються параметри прослуховування мережевих інтерфейсів через директиви listen-on (для IPv4) та listen-on-v6 (для IPv6). Після внесення змін служба перезапускається командою systemctl restart bind9 [39].

Наступним кроком є оголошення зон у файлі /etc/bind/named.conf.local. Для прикладу, створюється пряма зона для домену lab.com та зворотна зона для мережі 192.168.1.0/24. У блоці конфігурації кожної зони вказується тип type master, що визначає роль сервера як первинного, та параметр file, який вказує шлях до файлу з записами ресурсів (наприклад, /etc/bind/zones/forward.lab.com.db). Директива allow-update { none; }; забороняє динамічне оновлення зон, що підвищує безпеку статичної конфігурації. Рекомендується створити окремий каталог /etc/bind/zones для зберігання файлів зон та надати відповідні права доступу користувачу bind.

Наповнення файлу прямої зони починається з директиви $TTL та запису SOA (Start of Authority), який описує основні параметри зони: серійний номер, який необхідно збільшувати при кожній зміні, інтервали оновлення, повторної спроби та застарівання. Далі додаються записи NS (Name Server), що вказують на сам DNS-сервер, та записи типу A (Address), які зіставляють імена хостів (ns1, laptop1, pc1) з їхніми IP-адресами. Наприклад, запис ns1 IN A 192.168.1.10 пов’язує ім’я сервера імен з його адресою (рис. 11.9).

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

Рисунок 11.9 – Файл зони для інтерфейсу зворотного зв’язку [39]

Конфігурація зворотної зони, яка відповідає за перетворення IP-адрес у доменні імена, виконується аналогічно, але замість записів типу A використовуються записи PTR. Файл зворотної зони також містить SOA та NS записи. Записи PTR мають формат, де вказується останній октет IP-адреси та відповідне йому повне доменне ім’я (FQDN). Наприклад, запис 10 IN PTR ns1.lab.com. дозволяє визначити ім’я хоста за IP-адресою 192.168.1.10 (рис. 11.10). Якщо в мережі не використовується протокол IPv6, рекомендується примусово перевести BIND у режим роботи тільки з IPv4, відредагувавши файл /etc/default/named та додавши параметр -4 до змінної OPTIONS [39].

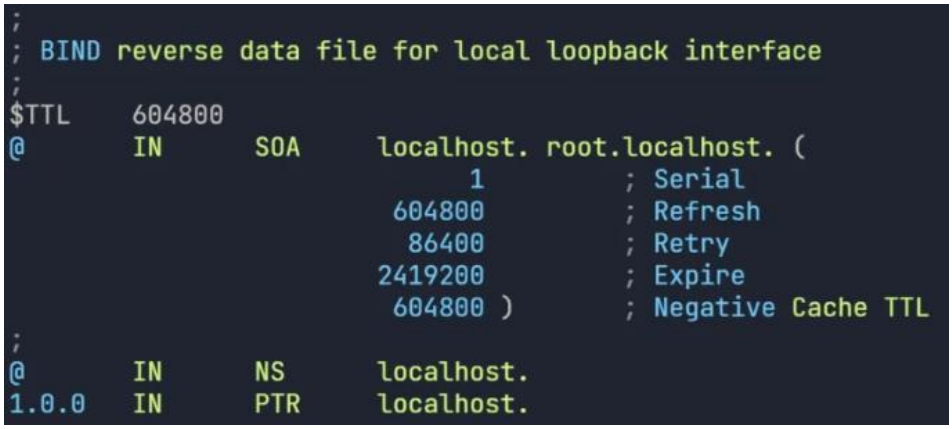

Рисунок 11.10 – Зворотна зона для інтерфейсу зворотного зв’язку [39]

Перевірка коректності налаштувань є обов’язковим етапом перед введенням сервера в експлуатацію. Для цього використовуються утиліти синтаксичного контролю: named-checkconf для перевірки головних конфігураційних файлів та named-checkzone для перевірки файлів зон. Якщо помилок не виявлено, виконується перезапуск служби. Тестування працездатності здійснюється з клієнтських машин за допомогою утиліт ping (перевірка вирішення імен), а також спеціалізованих інструментів nslookup, dig або host. Успішне вирішення прямих (ім’я в IP) та зворотних (IP в ім’я) запитів свідчить про коректну роботу первинного DNS-сервера [39].

Для забезпечення відмовостійкості інфраструктури виконується налаштування вторинного DNS-сервера. Цей процес вимагає попередніх змін на первинному сервері. У файлі зони майстер-сервера необхідно додати запис NS та A для вторинного сервера (наприклад, ns2) (рис. 11.11). Крім того, у файл named.conf.local на майстер-сервері додається директива allow-transfer, в якій вказується IP-адреса вторинного сервера (рис. 11.12). Це дозволяє передачу даних зони виключно авторизованому вторинному серверу. На стороні вторинного сервера процес встановлення програмного забезпечення ідентичний первинному. Відмінності полягають у конфігурації файлу /etc/bind/named.conf.local. При оголошенні зон на вторинному сервері використовується тип «type slave».

```
vi /etc/bind/zones/forward.lab.com.db

$TTL    604800
@       IN      SOA     ns1.lab.com. root.lab.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL


@       IN      NS      ns1.lab.com.
@       IN      NS      ns2.lab.com.

ns1     IN      A    192.168.1.10
ns2     IN      A    192.168.1.11

laptop1 IN      A    192.168.1.21
laptop2 IN      A    192.168.1.22
pc1     IN      A    192.168.1.23
pc2     IN      A    192.168.1.24
pc3     IN      A    192.168.1.25
phone   IN      A    192.168.1.26
printer IN      A    192.168.1.27


:x //save the file
```

Рисунок 11.11 – Записи вторинного DNS-сервера на головному DNS-сервері [39]

```
vi /etc/bind/named.conf.local


zone "lab.com" {
    type master;
    file "/etc/bind/zones/forward.lab.com.db";
    allow-update { none; };
    allow-transfer { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/reverse.192.168.1.db";
    allow-update { none; };
    allow-transfer { 192.168.1.11; };
};


:x //save the file
```

Рисунок 11.12 – Надання дозволу на вторинний DNS-сервер для передачі зони [39]

Обов’язково додається директива masters, яка містить IP-адресу первинного сервера (наприклад, 192.168.1.10), звідки будуть завантажуватися дані. Параметр file вказує локальний шлях, куди вторинний сервер збереже отриману копію зони. Після перезапуску служби на вторинному сервері ініціюється процес трансферу зони, і файли зон автоматично створюються в зазначеному каталозі, що можна перевірити переглядом вмісту директорії або аналізом системних журналів. Це завершує побудову системи доменних імен на базі Linux Server.

Механізми віддаленого доступу (SSH)

У сучасних мережевих інфраструктурах забезпечення безпечного віддаленого адміністрування серверних вузлів є важливою вимогою, яка реалізується за допомогою

протоколу прикладного рівня SSH (Secure Shell).

Протокол SSH був розроблений як захищена альтернатива застарілим і незахищеним інструментам, таким як Telnet, rlogin та RSH, які передавали автентифікаційні дані та командний трафік у відкритому вигляді. Архітектура SSH базується на клієнт-серверній моделі, де серверний компонент (sshd) очікує на вхідні з'єднання на певному TCP-порту (стандартно 22), а клієнтське програмне забезпечення (ssh) ініціює з'єднання. Фундаментальною особливістю протоколу є обов'язкове шифрування всього трафіку, включаючи процедуру автентифікації, що досягається використанням гібридної криптографії. Асиметричні алгоритми застосовуються для обміну ключами сесії та автентифікації сторін, тоді як симетричні алгоритми використовуються для швидкого шифрування потоку даних в рамках встановленої сесії.

Процес розгортання серверної частини SSH у середовищі Ubuntu Server є стандартизованою процедурою, що виконується через систему керування пакетами. Для встановлення SSH-сервера в терміналі застосовуються команди оновлення індексу пакетів «sudo apt update» та безпосередньої інсталяції пакунка «sudo apt install openssh-server –y», як це показано на рисунку 11.13. Виконання цих команд ініціює завантаження бінарних файлів, генерацію унікальних хост-ключів сервера, які слугують його цифровим відбитком для запобігання атакам типу «людина посередині», та автоматичну реєстрацію служби в системі ініціалізації systemd. Важливо зазначити, що хост-ключі генеруються один раз при встановленні, і їх зміна призведе до появи попереджень про порушення безпеки у клієнтів, що раніше підключалися до цього вузла.

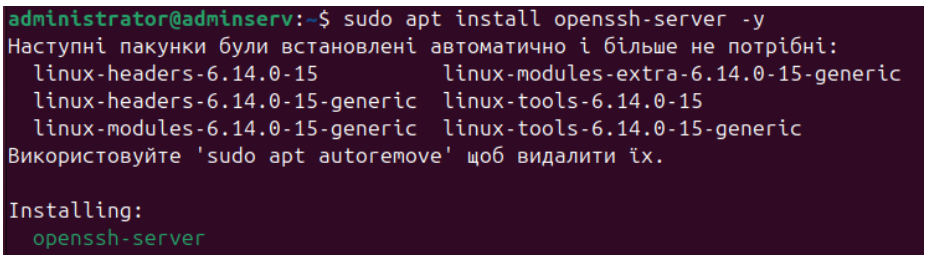

Рисунок 11.13 – Встановлення SSH-сервера [38]

Після завершення процесу інсталяції, важливим етапом є верифікація коректності запуску служби. Для цього перевіряється робота служби SSH-сервера, використовуючи команду «sudo systemctl status ssh» в терміналі, яка повинна повернути статус «active (running)». Окрім статусу процесу, необхідно впевнитися у коректності прив'язки до мережевих сокетів. Також після цього здійснюється перевірка, чи «слухає» сервер порт 22 командою «ss -tlnp | grep 22» (рис. 11.14). У виводі цієї команди прапорці «LISTEN» свідчать про готовність сервера приймати вхідні з'єднання, а відображення адреси «0.0.0.0» або «*» вказує на прослуховування всіх доступних мережевих інтерфейсів.

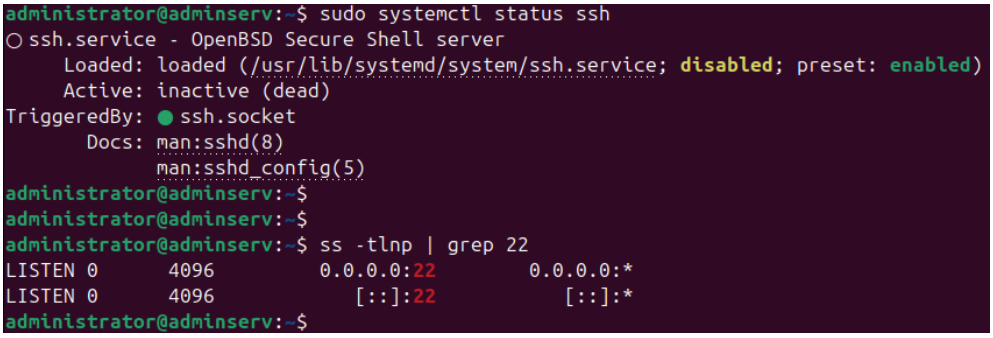

Рисунок 11.14 – Перевірка роботи SSH-сервера [38]

Конфігурування параметрів роботи служби здійснюється шляхом редагування текстових файлів налаштувань. Важливо розрізняти файл налаштувань клієнта (ssh_config) та файл налаштувань сервера (sshd_config). Для зміни налаштувань SSH-сервера слід відкрити конфігураційний файл, що міститься за адресою «/etc/ssh/sshd_config». Там, знайшовши потрібне поле, необхідно провести зміни згідно з політикою безпеки. До типових налаштувань належить зміна стандартного порту для зменшення кількості автоматизованих атак, заборона прямого входу суперкористувача (параметр PermitRootLogin no) та обмеження списку дозволених користувачів (AllowUsers). Після будь-якої зміни конфігурації виконується перезапуск SSH-сервера командою «sudo systemctl restart ssh», що змушує перечитати файл налаштувань без розриву вже встановлених активних з'єднань [38].

Забезпечення мережевої доступності сервісу вимагає коректного налаштування міжмережевого екрану сервера. Для подальшого правильного функціонування SSH-сервера проводяться налаштування відповідних параметрів брандмауера UFW (Uncomplicated Firewall), який є стандартним інструментом в Ubuntu. Для цього в терміналі вводиться команда «sudo ufw allow 22/tcp», яка створює правило дозволу вхідного трафіку на порт 22 по протоколу TCP. Після цього застосовується команда «sudo ufw enable» для активації брандмауера та завантаження правил (рис. 11.15). Коли ці дії зроблено, то SSH-сервер має коректно працювати і бути доступним із зовнішньої мережі, при цьому решта портів залишатимуться закритими згідно з політикою за замовчуванням.

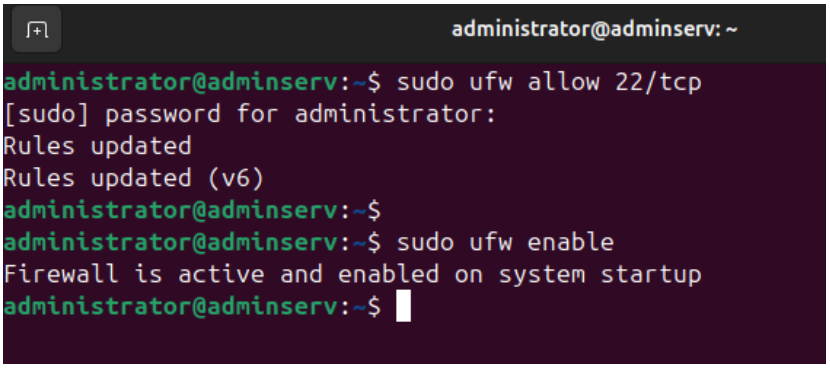

Рисунок 11.15 – Налаштування брандмауера для роботи SSH-сервера [38]

Найбільш надійним методом автентифікації в SSH вважається використання пари криптографічних ключів замість паролів. Цей метод базується на асиметричній криптографії: користувач генерує пару ключів (публічний та приватний) на локальній машині. Публічний ключ, який не є секретним, копіюється на сервер у файл ~/.ssh/authorized_keys у домашньому каталозі користувача. При спробі з'єднання сервер шифрує випадкове повідомлення за допомогою публічного ключа користувача. Клієнт може розшифрувати це повідомлення і підтвердити свою особу тільки за наявності відповідного приватного ключа. Цей підхід нівелює ризики, пов'язані зі слабкими паролями та брутфорс-атаками [38].

Окрім надання віддаленого термінального доступу, протокол SSH забезпечує захищений транспорт для інших протоколів та утиліт. Зокрема, утиліта SCP (Secure Copy) та протокол SFTP (SSH File Transfer Protocol) використовують встановлений SSH-канал для шифрованої передачі файлів між хостами, замінюючи незахищений FTP. Також SSH підтримує механізм тунелювання, який дозволяє інкапсулювати трафік інших застосунків (наприклад, запити до бази даних або веб-трафік) всередину зашифрованої сесії SSH. Це дозволяє адміністраторам отримувати доступ до внутрішніх сервісів локальної мережі сервера, які не мають прямого виходу в Інтернет, створюючи своєрідний ситуативний VPN-канал для безпечного адміністрування складної інфраструктури.

Контроль процесів і логів

У операційній системі Ubuntu Server, як і в будь-якій Unix-подібній системі, поняття процесу є фундаментальним для розуміння принципів функціонування програмного забезпечення. Процес визначається як екземпляр програми, що знаходиться в стані виконання, якому ядро операційної системи виділяє певний адресний простір у пам'яті та набір системних ресурсів. Кожен процес у системі ідентифікується унікальним цілим числом, відомим як ідентифікатор процесу (Process Identifier – PID). Ієрархія процесів будується деревоподібно: кожен новий процес породжується батьківським процесом (Parent Process) за допомогою системного виклику fork(), отримуючи при цьому ідентифікатор батька (PPID). Винятком є лише процес ініціалізації systemd (у сучасних версіях Ubuntu), який має PID 1 і запускається безпосередньо ядром під час завантаження системи. Саме systemd виступає коренем дерева процесів користувацького простору і відповідає за запуск решти системних служб та терміналів.

Керування процесами неможливе без розуміння їхніх станів, оскільки процес не завжди активно використовує центральний процесор. У планувальнику завдань Linux (Completely Fair Scheduler – CFS) розрізняють декілька основних станів. Стан «Running» (R) означає, що процес або виконується на процесорі в даний момент, або знаходиться в черзі на виконання. Стан «Sleeping» поділяється на перериваний (S – Interruptible sleep) та

непереривний (D – Uninterruptible sleep). Перериваний сон характерний для процесів, що очікують на певну подію (наприклад, введення даних користувачем), і можуть бути розбуджені сигналом. Непереривний сон зазвичай виникає при очікуванні операцій введення-виведення на апаратному рівні (дискові операції), і такий процес неможливо примусово завершити до закінчення операції. Особливої уваги адміністратора вимагають процеси у стані «Zombie» (Z) – це процеси, які завершили своє виконання, звільнили ресурси, але запис про них все ще залишається в таблиці процесів ядра, оскільки батьківський процес не зчитав код їх завершення через виклик wait() [38].

Для отримання інформації про поточний стан системи в Ubuntu Server використовується віртуальна файлова система /proc. Ця директорія не містить реальних файлів на жорсткому диску, а є інтерфейсом до структур даних ядра. Кожен запущений процес має власну піддиректорію в /proc, назва якої відповідає його PID (наприклад, /proc/1234/). У цій директорії містяться файли з повною інформацією про процес: cmdline (команда запуску), environ (змінні оточення), fd (відкриті файлові дескриптори), status (поточний стан та використання пам’яті). Інструменти моніторингу, такі як ps, top або htop, фактично зчитують та форматують інформацію саме з цієї файлової системи, надаючи адміністратору зрозуміле візуальне представлення.

Базовим інструментом для отримання миттєвого зрізу активності процесів є утиліта ps (process status). Для повноцінного аналізу в серверному середовищі найчастіше застосовується комбінація ключів aux (стандарт BSD) або -ef (стандарт System V). Виконання команди ps aux виводить таблицю, де відображаються користувач-власник процесу, PID, відсоток використання процесора та пам’яті віртуальна та резидентна пам’ять, статус, час старту та сама команда. Важливим аспектом аналізу є розуміння параметра TTY: якщо в цьому полі стоїть знак питання ?, це свідчить про те, що процес є службою, яка не прив’язана до жодного термінала. Це типова поведінка для веб-серверів (Apache, Nginx) або баз даних, які працюють у фоновому режимі.

Для спостереження за динамікою споживання ресурсів у реальному часі використовуються інтерактивні утиліти top та його вдосконалений аналог htop. Утиліта top дозволяє сортувати процеси за споживанням ЦП або ОЗП, а також надає загальну статистику системи: час роботи (uptime), кількість користувачів та середнє навантаження (Load Average). Показник Load Average, що відображається як три числа (за 1, 5 та 15 хвилин), є критичною метрикою для оцінки продуктивності сервера. Він показує середню кількість процесів, які знаходяться в стані виконання або в черзі на виконання (включаючи ті, що перебувають у стані непереривного сну). Якщо значення Load Average перевищує кількість доступних ядер процесора, це свідчить про перевантаження системи та виникнення черг, що потребує втручання адміністратора для оптимізації або масштабування ресурсів [38].

Механізм керування процесами базується на використанні сигналів – це засіб міжпроцесної взаємодії, що дозволяє ядру або одному процесу передати керуючу команду іншому. Для надсилання сигналів використовується команда kill. Попри свою назву, ця утиліта призначена не лише для знищення процесів, а й для керування ними. За замовчуванням kill надсилає сигнал SIGTERM (код 15), який просить процес коректно завершити роботу, закрити відкриті файли та звільнити пам’ять. Якщо процес завис і не реагує на SIGTERM, застосовується сигнал SIGKILL (код 9), який обробляється безпосередньо ядром і миттєво припиняє виконання процесу без можливості збереження даних. Ще одним важливим сигналом є SIGHUP (код 1), який використовується для перезавантаження конфігурації служб без повної зупинки процесу.

У багатокористувацькому середовищі Linux важливим є керування пріоритетами виконання завдань. Кожен процес має атрибут «niceness» (значення nice), який визначає його відношення до інших процесів у боротьбі за процесорний час. Діапазон значень варіюється від -20 (найвищий пріоритет) до +19 (найнижчий пріоритет). За замовчуванням процеси запускаються з пріоритетом 0. Звичайний користувач може лише знижувати пріоритет своїх процесів (збільшувати значення nice), тоді як суперкористувач (root) має право підвищувати пріоритет (зменшувати значення nice). Для запуску процесу з нестандартним пріоритетом використовується команда nice, а для зміни пріоритету вже запущеного процесу – renice. Це дозволяє адміністратору, наприклад, надати вищий пріоритет процесу бази даних і знизити пріоритет для завдань резервного копіювання, що виконуються у фоні.

Керування фоновим та активним виконанням процесів здійснюється засобами командної оболонки Bash. Якщо виконання команди займає тривалий час і блокує термінал, її можна запустити у фоновому режимі, додавши символ амперсанда & в кінці рядка. Вже запущений процес можна призупинити комбінацією клавіш Ctrl+Z, що надсилає сигнал SIGSTOP, а потім перевести у фоновий режим командою bg або повернути в активний режим командою fg. Для перегляду списку завдань поточної сесії оболонки використовується команда jobs. Однак, процеси, запущені в терміналі, є нащадками процесу оболонки, тому при закритті сесії SSH вони отримають сигнал SIGHUP і завершаться. Щоб уникнути цього, використовують утиліту nohup або термінальні мультиплексори (screen, tmux), які дозволяють процесам продовжувати роботу після від’єднання користувача.

В контексті Ubuntu Server основним інструментом керування серверними процесами (службами) є система systemd, яка оперує поняттям «юнітів». Контроль процесів здійснюється через утиліту systemctl. На відміну від прямого запуску бінарних файлів, systemd забезпечує стандартизоване оточення, автоматичний перезапуск у разі збоїв, керування залежностями та логування. Статус служби перевіряється командою systemctl status <service_name>, яка надає детальну інформацію про PID головного процесу, дерево

дочірніх процесів, споживання пам’яті та останні рядки логів. Керування станом здійснюється командами start, stop, restart та reload. Важливою функцією є systemctl enable/disable, яка керує символічними посиланнями для автоматичного запуску служби під час завантаження системи [38].

Оперативний контроль логів процесів, стосується роботи зі стандартними потоками введення-виведення (stdout та stderr) у реальному часі. У традиційній моделі Unix процеси виводять інформаційні повідомлення у стандартний потік виведення (stdout), а повідомлення про помилки – у стандартний потік помилок (stderr). Адміністратор повинен вміти перехоплювати та аналізувати ці потоки безпосередньо під час виконання. Для цього використовуються оператори перенаправлення. Наприклад, конструкція command > log.txt 2>&1 перенаправляє обидва потоки в один файл, що дозволяє зберегти повну історію виконання. Для відкидання непотрібного виводу використовується спеціальний пристрій /dev/null, який діє як «чорна діра» для даних.

Для спостереження за логами процесів у режимі реального часу, особливо тих, що записують дані у текстові файли, незамінною є утиліта tail з ключем -f (follow). Виконання команди tail -f /var/log/syslog або tail -f /var/log/nginx/access.log дозволяє адміністратору бачити нові рядки журналу в момент їх появи. Це є основним методом діагностики при налагодженні роботи сервісів, коли необхідно співставити дії користувача (наприклад, HTTP-запит) з реакцією сервера. У середовищі systemd аналогічний функціонал надає команда journalctl -f -u <service_name>, яка підключається до системного журналу і виводить повідомлення конкретної служби в міру їх надходження, дозволяючи відстежувати поведінку демонів, що не мають власних лог-файлів.

Крім того, контроль процесів включає моніторинг використання ними файлових дескрипторів та мережевих сокетів. У ОС Linux «все є файлом», тому мережеве з’єднання для процесу виглядає як відкритий файл. Утиліта lsof (List Open Files) дозволяє визначити, які файли відкриті конкретним процесом (ключ -p PID), або навпаки – які процеси використовують конкретний файл або порт (ключ -i). Це критично важливо для діагностики помилок «File in use» або виявлення несанкціонованої мережевої активності. Наприклад, команда lsof -i :80 покаже всі процеси, що взаємодіють через порт 80. Такий глибокий аналіз взаємозв’язків між процесами та ресурсами файлової системи є завершальним етапом повного контролю над станом сервера перед переходом до налаштування систем довгострокового зберігання та аналізу журналів.

Налаштування Apache/Nginx

У сучасній інженерії веб-систем та адмініструванні серверних інфраструктур одним із ключових завдань є забезпечення надійної, безпечної та продуктивної доставки контенту

кінцевому користувачеві. Реалізація цього завдання часто вимагає виходу за межі використання єдиного монолітного веб-сервера. Найбільш ефективним підходом, що зарекомендував себе в індустрії, є побудова багаторівневої архітектури, де поєднуються сильні сторони різних програмних рішень.

У цьому контексті розглядається методологія розгортання та конфігурації гібридної системи, що складається з двох найпопулярніших веб-серверів: Apache2 та Nginx. У запропонованій архітектурі Nginx виконуватиме роль зворотного проксі-сервера, що приймає вхідні запити та здійснює їх попередню обробку, тоді як Apache2 функціонуватиме як сервер додатків, безпосередньо обробляючи логіку веб-ресурсу [40].

Процес побудови веб-серверної інфраструктури розпочинається з ретельного підготовчого етапу, який визначає фундамент стабільності майбутньої системи. Оскільки веб-сервери Nginx та Apache2 є нативними для Unix-подібних систем, першочерговою вимогою є наявність налаштованого сервера під управлінням операційної системи Linux. У контексті даного навчального матеріалу базовою платформою обрано дистрибутив Ubuntu, який базується на архітектурі Debian і широко використовується в корпоративному секторі завдяки своїй стабільності та широкій підтримці спільноти. Слід зазначити, що для користувачів, які працюють у середовищі Windows, існує можливість емуляції необхідного оточення за допомогою підсистеми WSL (Windows Subsystem for Linux), що дозволяє використовувати інструментарій Linux без необхідності повної переінсталяції операційної системи або використання важковагових віртуальних машин. Критично важливими передумовами для успішної реалізації проекту є наявність стабільного підключення до мережі Інтернет для завантаження пакетів із репозиторіїв, а також наявність привілеїв суперкористувача (root) або прав на виконання команд через механізм sudo, оскільки конфігурація мережевих служб та модифікація системних файлів вимагають підвищеного рівня доступу [40].

Наступним кроком підготовчої фази є забезпечення наявності веб-додатку, який буде обслуговуватися розгорнутою інфраструктурою. Адміністратор системи постає перед вибором: розробити власний програмний продукт, що надає повний контроль над архітектурою коду та функціональними можливостями, або використати готове рішення для пришвидшення процесу розгортання та фокусування на налаштуванні серверної частини.

У навчальних цілях, для стандартизації процесу та уникнення помилок на етапі кодування, рекомендується використання попередньо підготовленого веб-додатку, доступного у відповідному репозиторії на платформі GitHub. Після завантаження вихідного коду на локальну машину або сервер, необхідно провести первинну верифікацію цілісності файлів. Це виконується шляхом відкриття головного файлу index.html у локальному веб-браузері. Відображення коректного графічного інтерфейсу свідчить про готовність додатку до розгортання, проте на цьому етапі він функціонує лише як набір локальних файлів і ще не

інтегрований у серверну інфраструктуру, що підводить до необхідності інсталяції відповідного серверного програмного забезпечення.

Першим компонентом серверної тріади, що підлягає інсталяції, є веб-сервер Apache2. Цей сервер вирізняється своєю модульністю, надійністю та підтримкою широкого спектра технологій обробки динамічного контенту. Процедура інсталяції в середовищі Ubuntu виконується через термінальний інтерфейс, який є основним інструментом системного адміністратора. Перед початком інсталяції критично важливо актуалізувати інформацію про доступні пакети в системних репозиторіях. Виконання команди sudo apt-get update ініціює з'єднання з серверами оновлень та завантаження актуальних списків пакетів, що гарантує встановлення останніх стабільних версій програмного забезпечення та наявність необхідних патчів безпеки. Після оновлення індексу виконується безпосередня інсталяція пакету Apache2 за допомогою команди sudo apt-get install apache2 (рис. 11.16). Пакетний менеджер автоматично вирішує залежності, завантажує бінарні файли та конфігураційні скрипти, розміщуючи їх у відповідних директоріях файлової системи.

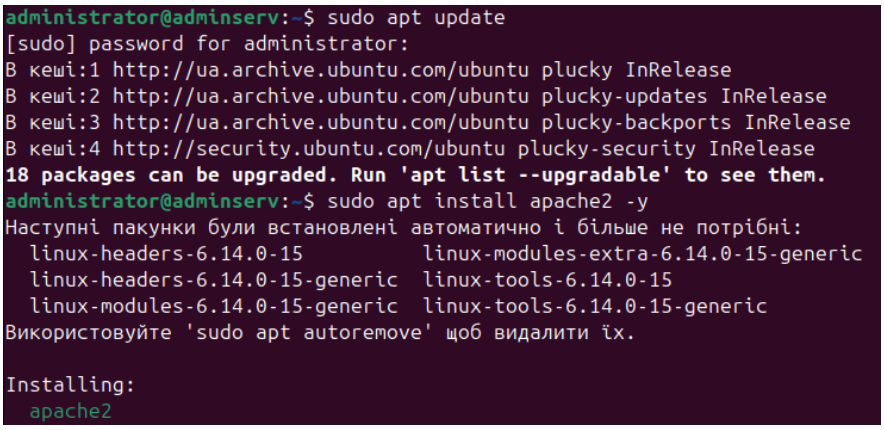

Рисунок 11.16 – Встановлення Apache2 [40]

Після завершення процесу розпакування та налаштування пакетів, службу Apache2 необхідно запустити та перевести в активний стан. Керування службами в сучасних дистрибутивах Linux здійснюється системою ініціалізації systemd. Виконання команди sudo systemctl start apache2 ініціює запуск головного процесу веб-сервера. Для перевірки успішності запуску та коректності прив'язки до мережевих інтерфейсів використовується метод тестового запиту [40].

Адміністратор повинен відкрити веб-браузер та ввести в адресний рядок IP-адресу сервера або стандартне доменне ім'я локального хоста – localhost. Якщо процес інсталяції пройшов без помилок, браузер відобразить стандартну сторінку привітання «Apache2 Default Page» (рис. 11.17). Ця сторінка є важливим діагностичним індикатором, який підтверджує, що веб-сервер коректно встановлений, запущений, прослуховує порт 80 за протоколом TCP і

має доступ до файлової системи для читання веб-документів.

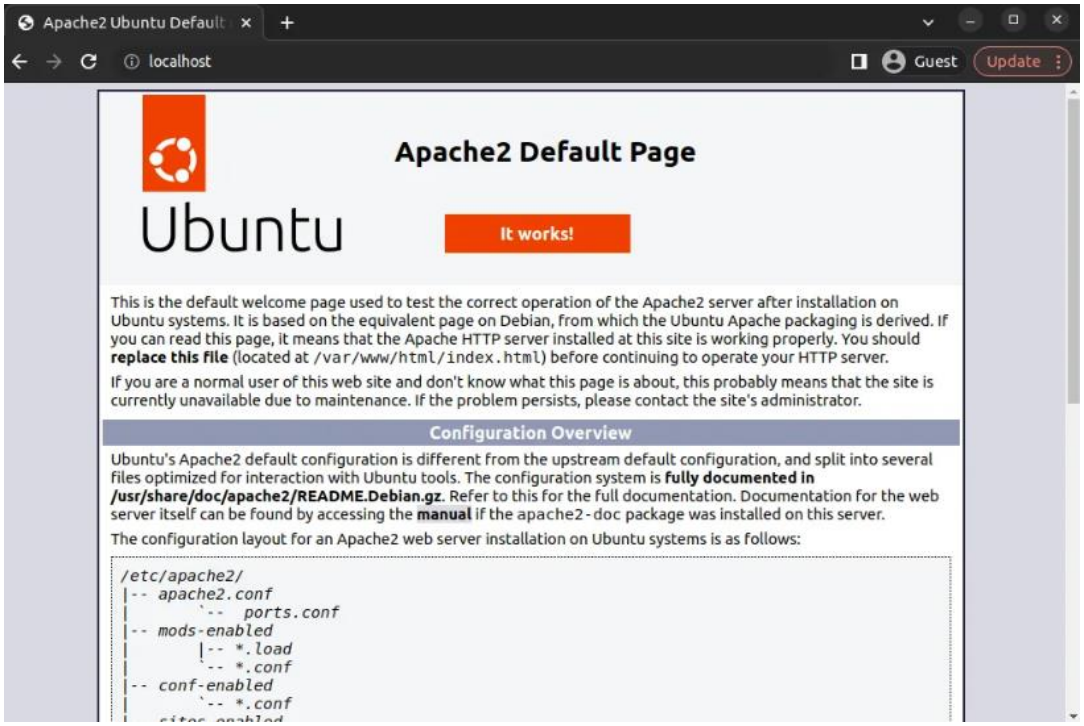

Рисунок 11.17 – Сторінка привітання «Apache2 Default Page» [40]

Інтеграція користувацького веб-додатку в середовище Apache2 вимагає заміни стандартного контенту, що постачається разом із сервером, на файли цільового проекту. Стандартна конфігурація Apache в Ubuntu визначає директорію /var/www/html як кореневу папку документів. Оскільки файл привітання зазвичай має назву index.html, його наявність конфліктуватиме з індексним файлом веб-додатку. Тому, використовуючи термінал, необхідно виконати очищення цільової директорії. Команда sudo rm -r /var/www/html/index.html виконує видалення стандартного файлу. Використання прапора -r (recursive) у даному контексті є запобіжним заходом для гарантованого видалення об’єкта, навіть якщо це директорія, хоча для окремого файлу це не є обов’язковим. Наступним кроком здійснюється перенесення файлів веб-додатку з директорії завантаження до кореневої директорії сервера. Команда sudo cp -r * /var/www/html виконує рекурсивне копіювання всього вмісту поточного каталогу в системну директорію веб-сервера [40].

Після заміни файлів необхідно провести повторне тестування для підтвердження коректності розгортання додатку. Звернення до адреси localhost у веб-браузері повинно призвести до відображення інтерфейсу користувацького веб-додатку замість стандартної сторінки Apache (рис. 11.18). Успішне відображення контенту свідчить про те, що Apache2 налаштований правильно, має необхідні права доступу до нових файлів і готовий виконувати функції бекенд-сервера. Однак, на даному етапі архітектура системи ще не є завершеною, оскільки додаток обслуговується безпосередньо сервером Apache, без проміжного шару

проксіювання, який необхідний для забезпечення масштабованості та безпеки згідно з поставленим технічним завданням. Наступні етапи передбачають розгортання Nginx та налаштування взаємодії між двома серверами.

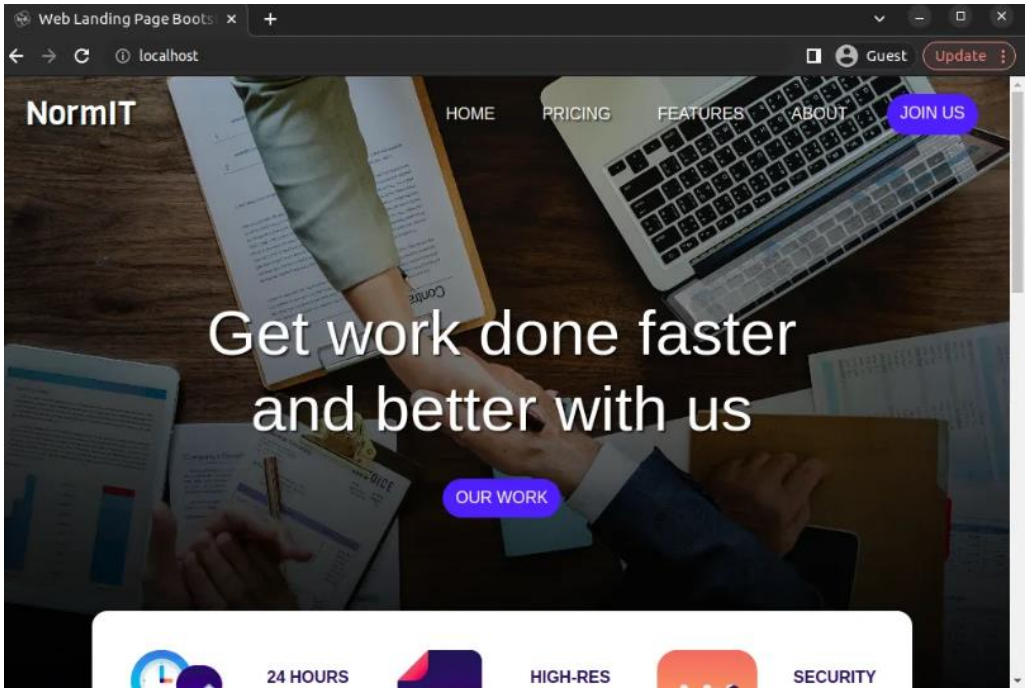

Рисунок 11.18 – Успішне відображення інтерфейсу користувацького веб-додатку [40]

Встановлення веб-сервера Nginx здійснюється за аналогічним алгоритмом, що й встановлення Apache2, використовуючи пакетний менеджер apt. Після оновлення репозиторіїв командою sudo apt-get update, виконується команда sudo apt-get install nginx (рис. 11.19). Ця дія встановлює сервер Nginx у систему.

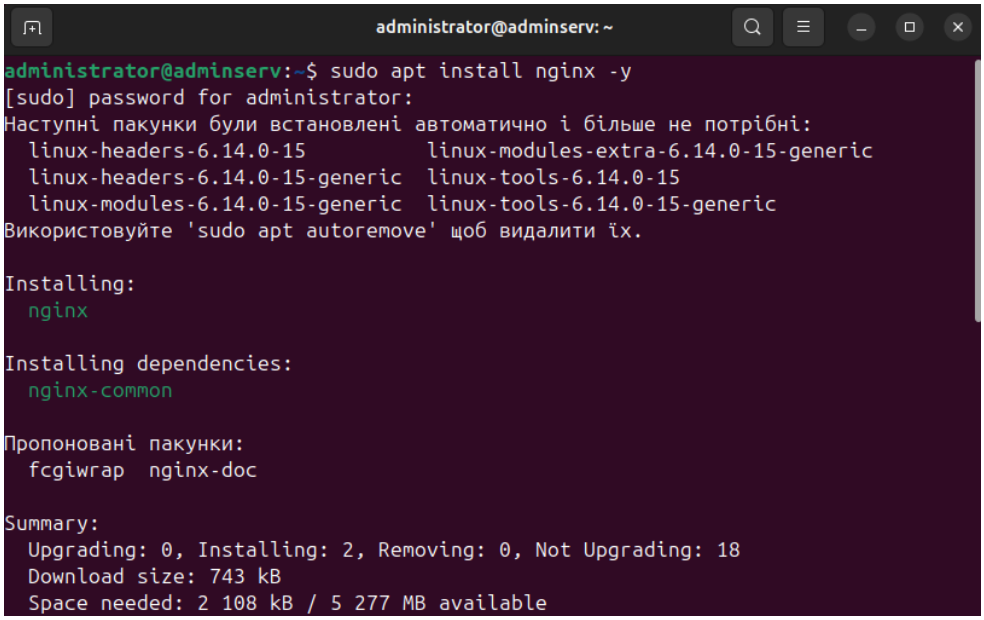

Рисунок 11.19 – Встановлення Nginx [40]

Однак, виникає архітектурна колізія, адже за замовчуванням обидва сервери – і Apache2, і Nginx – налаштовані на прослуховування стандартного HTTP-порту 80. Оскільки два процеси не можуть одночасно використовувати один і той самий мережевий порт на одному IP-інтерфейсі, необхідно змінити конфігурацію Nginx перед його запуском у робочий режим. Стратегія полягає в тому, щоб перенести Nginx на альтернативний порт (порт 3000) для початкового налаштування, а згодом налаштувати його як точку входу.

Для зміни порту прослуховування Nginx необхідно внести правки до головного файлу конфігурації віртуального хоста. Використовуючи текстовий редактор, наприклад nano, адміністратор відкриває файл за шляхом /etc/nginx/sites-available/default командою sudo nano /etc/nginx/sites-available/default. У структурі файлу необхідно знайти директиви listen, які відповідають за прив’язку до портів. Стандартні записи listen 80 default_server; (для IPv4) та listen [::]:80 default_server; (для IPv6) необхідно модифікувати, замінивши значення 80 на 3000. Таким чином, конфігурація набуде вигляду listen 3000 default_server; та listen [::]:3000 default_server;. Крім того, рекомендується скоригувати директиву index, залишивши в пріоритеті файл index.nginx-debian.html для перевірки роботи самого Nginx, або адаптувати її під потреби додатку. Збереження внесених змін виконується стандартними засобами редактора (CTRL+X, Y, Enter) [40].

Після модифікації конфігураційного файлу необхідно перевірити працездатність Nginx на новому порту. Для цього у веб-браузері вводиться адреса сервера з явним зазначенням порту: localhost:3000. Відображення стандартної сторінки привітання «Welcome to nginx!» підтверджує, що сервер успішно інстальовано, конфігурацію зчитано коректно, і конфлікт портів з Apache2 (який залишається на порту 80) вирішено (рис. 11.20).

Рисунок 11.20 – Відображення стандартної сторінки привітання «Welcome to nginx!» [40]

На цьому етапі в системі паралельно функціонують два веб-сервери, які працюють незалежно один від одного. Наступним, критично важливим кроком, є об’єднання їх у єдину логічну структуру шляхом налаштування Nginx як зворотного проксі-сервера, що дозволить йому приймати запити від клієнтів і перенаправляти їх на бекенд-сервер Apache.

Концепція зворотного проксі є центральною в сучасних веб-архітектурах. Зворотний проксі діє як посередник, що стоїть між клієнтом (браузером користувача) та внутрішнім сервером ресурсів (Apache2). На відміну від прямого проксі, який обслуговує вихідні запити клієнтів до Інтернету, зворотний проксі обслуговує вхідні запити з Інтернету до внутрішніх серверів. Використання такої схеми надає низку вагомих переваг. По-перше, це підвищення рівня безпеки, оскільки зворотний проксі приховує топологію внутрішньої мережі та характеристики бекенд-серверів від зовнішнього світу, виступаючи своєрідним щитом. По-друге, це покращення продуктивності за рахунок можливостей кешування статичного контенту, стиснення даних та ефективного управління з’єднаннями. По-третє, це можливість гнучкого перенаправлення трафіку та балансування навантаження між декількома серверами додатків [40].

Реалізація функціоналу зворотного проксі в Nginx вимагає подальшого редагування файлу конфігурації /etc/nginx/sites-available/default. Ключові зміни вносяться в блок location /, який відповідає за обробку запитів до кореневої директорії сайту. У цьому блоці необхідно додати директиву proxy_pass, яка вказує адресу призначення для перенаправлення запитів. У даному сценарії це буде http://localhost:80, тобто адреса локального сервера Apache. Однак простого перенаправлення недостатньо для коректної роботи сучасних веб-додатків. Необхідно також налаштувати передачу HTTP-заголовків, щоб зберегти контекст запиту. Директива proxy_set_header Host $host; передає оригінальне ім’я хоста, що дозволяє Apache коректно визначати віртуальний хост. Заголовки Upgrade та Connection налаштовуються для підтримки протоколу WebSocket та механізму оновлення з’єднання (HTTP Upgrade mechanism).

Повна конфігурація блоку location має виглядати наступним чином: спочатку вказується proxy_pass http://localhost:80;, потім встановлюється версія протоколу proxy_http_version 1.1;. Далі слідують директиви встановлення заголовків: proxy_set_header Upgrade $http_upgrade;, proxy_set_header Connection 'upgrade';, proxy_set_header Host $host;. Також додається директива proxy_cache_bypass $http_upgrade;, яка дозволяє оминати кеш для певних типів запитів. Після внесення цих налаштувань та збереження файлу, службу Nginx необхідно перезавантажити командою sudo systemctl restart nginx для застосування змін. Тестування проводиться шляхом звернення до localhost:3000. У разі успішного налаштування, за цією адресою повинен відображатися веб-додаток, який фізично розміщений на Apache, що підтверджує прозоре проксіювання трафіку через Nginx [40].

Кінцевим етапом налаштування є впровадження механізмів захисту, зокрема обмеження частоти запитів. Ця практика є критично важливою для забезпечення стабільності роботи сервера в умовах високого навантаження або зловмисних атак. Обмеження частоти запитів дозволяє контролювати кількість звернень, які сервер приймає від одного клієнта за одиницю часу. Це ефективний інструмент протидії атакам типу DDoS (розподілена відмова в обслуговуванні) та брутфорс-атакам (підбір паролів). Крім того, це дозволяє справедливо розподіляти системні ресурси (процесорний час, оперативну пам'ять) між користувачами, запобігаючи ситуації, коли один клієнт монополізує всі потужності сервера.

Налаштування обмеження частоти запитів в Nginx здійснюється у два етапи. Перший етап – визначення зони обмеження – виконується в основному контексті конфігурації (зазвичай на рівні http, але в спрощеному варіанті можна додати на початку файлу конфігурації сайту поза блоком server). Директива limit_req_zone $binary_remote_addr zone=one:10m rate=30r/m; створює зону з назвою «one». Параметр $binary_remote_addr означає, що ідентифікація клієнтів відбувається за їхньою IP-адресою у бінарному форматі (що економить пам'ять). Розмір зони 10m (10 мегабайт) дозволяє зберігати інформацію про стани десятків тисяч сесій. Параметр rate=30r/m встановлює ліміт швидкості обробки – 30 запитів на хвилину, що еквівалентно одному запиту кожні 2 секунди.

Другий етап – застосування обмеження до конкретного контексту. У блоці location / (або в блоці server) додається директива limit_req zone=one;. Це вказує Nginx використовувати раніше визначену зону «one» для перевірки частоти запитів до даного ресурсу. Після збереження конфігурації та перезапуску служби Nginx (sudo systemctl restart nginx), система починає відстежувати активність клієнтів. Якщо частота запитів від однієї IP-адреси перевищить встановлений поріг (у даному прикладі – частіше ніж раз на 2 секунди), Nginx тимчасово заблокує обробку нових запитів від цього клієнта і поверне HTTP-відповідь з кодом помилки 503 «Service Temporarily Unavailable» [40].

Для верифікації роботи механізму необхідно відкрити веб-додаток за адресою localhost:3000, сторінка завантажиться у звичайному режимі. Однак, якщо спробувати виконати швидке оновлення сторінки декілька разів поспіль (інтервал менше 2 секунд), користувач побачить сторінку з повідомленням про помилку 503. Це є індикатором того, що захисний механізм спрацював коректно, і сервер відхилив надлишкові запити.

Конфігурація віртуальних хостів

У контексті адміністрування веб-сервісів поняття віртуального хостингу є ключовим механізмом, що дозволяє одному фізичному або віртуальному серверу обслуговувати декілька незалежних доменних імен одночасно. Ця технологія базується на здатності веб-сервера аналізувати HTTP-заголовки, зокрема заголовок Host, для маршрутизації вхідного

запиту до відповідного кореневого каталогу файлової системи або специфічного обробника. Впровадження віртуальних хостів є необхідною умовою для оптимізації використання апаратних ресурсів, оскільки дозволяє уникнути розгортання окремого екземпляра операційної системи для кожного веб-сайту. У середовищі Ubuntu Server реалізація віртуальних хостів для Apache2 та серверних блоків для Nginx має уніфіковану структуру каталогів, проте відрізняється синтаксисом конфігураційних файлів та алгоритмами обробки запитів, що вимагає детального розгляду кожного підходу.

Організація файлової системи є першим етапом у проектуванні мультидоменного середовища. Згідно зі стандартом FHS (Filesystem Hierarchy Standard), дані веб-сайтів зазвичай розміщуються у директорії /var/www/. Для забезпечення ізоляції контенту для кожного домену створюється окрема директорія, наприклад /var/www/example.com/html. Критично важливим аспектом є налаштування прав доступу та власників файлів. Процес веб-сервера, який у Debian-подібних системах зазвичай виконується від імені користувача www-data, повинен мати права на читання файлів для їх відправки клієнту, а в деяких випадках – і на запис (для директорій завантаження медіа-файлів або кешу). Налаштування здійснюється за допомогою системних утиліт chown для зміни власника та chmod для встановлення маски прав доступу, що забезпечує базовий рівень безпеки та запобігає несанкціонованому доступу між різними віртуальними хостами.

Конфігурація віртуальних хостів у веб-сервері Apache2 базується на використанні модульної системи конфігураційних файлів. У дистрибутиві Ubuntu прийнята схема, де доступні конфігурації зберігаються в каталозі /etc/apache2/sites-available/, а активовані – у /etc/apache2/sites-enabled/. Кожен віртуальний хост описується в окремому файлі з розширенням .conf у блоці <VirtualHost *:80> (для HTTP) або <VirtualHost *:443> (для HTTPS). Ключовою директивою, яка визначає приналежність запиту, є ServerName, де вказується основне доменне ім’я, та ServerAlias, що дозволяє вказати альтернативні імена (наприклад, з префіксом www). Директива DocumentRoot вказує шлях до каталогу з файлами сайту. Важливим елементом адміністрування є розділення журналів подій: директиви ErrorLog та CustomLog дозволяють записувати помилки та статистику доступу в окремі файли для кожного домену, що значно спрощує процес відлагодження та аудиту безпеки [38].

Активація віртуального хоста в Apache2 здійснюється шляхом створення символічного посилання з каталогу sites-available в sites-enabled. У середовищі Ubuntu для цього розроблено спеціалізовану утиліту a2ensite (Apache2 Enable Site), яка автоматизує цей процес. Після виконання команди sudo a2ensite example.com.conf, система створює необхідне посилання. Однак зміни набувають чинності лише після перезавантаження конфігурації веб-сервера. Перед цим обов’язково виконується синтаксична перевірка конфігураційних файлів за допомогою команди apache2ctl configtest або apache2 -t. Якщо перевірка повертає статус

Syntax OK, ініціюється м’яке перезавантаження служби командою systemctl reload apache2, що дозволяє застосувати нові налаштування без розриву існуючих активних з’єднань користувачів.

У веб-сервері Nginx концепція віртуальних хостів реалізується через механізм, що називається «Server Blocks» (серверні блоки). Аналогічно до Apache, в Ubuntu використовується структура каталогів /etc/nginx/sites-available/ та /etc/nginx/sites-enabled/. Конфігурація описується директивою server { ... }, всередині якої параметр listen визначає порт прослуховування, а директива server_name вказує доменні імена, на які реагуватиме даний блок [38].

Особливістю Nginx є алгоритм вибору сервера. При надходженні запиту система перевіряє відповідність заголовка Host значенням server_name. Якщо точного співпадіння не знайдено, запит обробляється сервером, позначеним атрибутом default_server у директиві listen, або першим завантаженим конфігураційним файлом. Це вимагає від адміністратора уважності при проектуванні конфігурацій для уникнення ситуацій, коли запити потрапляють на неправильний обробник [40].

Для коректної роботи PHP-додатків у віртуальних хостах Nginx (оскільки Nginx не має вбудованого модуля обробки PHP, як Apache) налаштовується взаємодія з менеджером процесів PHP-FPM через протокол FastCGI. У блоці location ~ \.php$ прописуються параметри передачі запитів до сокету PHP-FPM (наприклад, fastcgi_pass unix:/var/run/php/php8.1-fpm.sock). Також важливо налаштувати порядок обробки індексних файлів через директиву index, надаючи пріоритет index.php перед index.html. Активація конфігурації в Nginx зазвичай виконується шляхом ручного створення символічного посилання командою ln -s, хоча логіка роботи залишається ідентичною до Apache. Перевірка синтаксису здійснюється командою nginx -t, яка аналізує структуру блоків, наявність крапок з комою та коректність шляхів, після чого виконується перезапуск служби.

Окремим аспектом конфігурації віртуальних хостів є забезпечення безпеки передачі даних за допомогою протоколу HTTPS. Це передбачає додавання у конфігураційний файл окремого блоку VirtualHost (Apache) або server (Nginx), що прослуховує порт 443. У цьому блоці обов’язково вказуються шляхи до SSL-сертифіката та приватного ключа за допомогою директив SSLCertificateFile / SSLCertificateKeyFile (для Apache) або ssl_certificate / ssl_certificate_key (для Nginx) [40].

Сучасною практикою є налаштування автоматичного перенаправлення всього трафіку з порту 80 на порт 443 для примусового використання шифрованого з’єднання. Це реалізується шляхом створення спрощеного віртуального хоста на порту 80, який повертає HTTP-код 301 з новою адресою, що гарантує цілісність та конфіденційність обміну даними між клієнтом та сервером.

Безпека веб-сервісів

Забезпечення інформаційної безпеки веб-сервісів у середовищі Linux є комплексним, багаторівневим процесом, що вимагає системного підходу до захисту конфіденційності, цілісності та доступності даних. В умовах постійного зростання кількості кіберзагроз, адміністратори серверів повинні реалізовувати стратегію «глибинного захисту, яка передбачає створення ешелонованих рубежів захисту: від рівня операційної системи та мережевого стеку до рівня додатків і баз даних.

Основним етапом забезпечення безпеки є проведення регулярного аудиту стану операційної системи для виявлення потенційних слабких місць у конфігурації та невідповідностей стандартам безпеки. Для автоматизації цього процесу в професійному середовищі широко застосовується спеціалізований інструментарій, зокрема утиліта Lynis. Це програмне забезпечення призначене для глибокого аналізу системи, перевірки цілісності файлів, аналізу встановленого програмного забезпечення та конфігураційних файлів на предмет відповідності кращим практикам безпеки. Процес імплементації даного інструменту в середовищі Ubuntu Server розпочинається з його інсталяції через стандартний менеджер пакетів. Для цього виконується команда з правами суперкористувача sudo apt install lynis –y, яка завантажує необхідні бінарні файли та залежності, інтегруючи утиліту в систему.

Після успішної інсталяції програмного забезпечення ініціюється процедура базового аудиту системи. Запуск перевірки здійснюється за допомогою команди sudo lynis audit system. Під час виконання цієї операції Lynis проводить сканування сотень параметрів системи. Перевіряються права доступу до критично важливих файлів, налаштування завантажувача GRUB, параметри ядра Linux, статус мережевих інтерфейсів, налаштування SSH-сервера та веб-серверів (Apache/Nginx). Алгоритм роботи програми базується на порівнянні поточного стану системи з базою знань про відомі вразливості та стандарти безпеки (наприклад, ISO 27001 або PCI-DSS). Результатом роботи утиліти є деталізований звіт, що виводиться безпосередньо в термінал та записується у лог-файли [40].

Важливим етапом роботи з результатами аудиту є аналіз отриманих даних. Адміністратор повинен ретельно вивчити секції звіту, зосереджуючись на повідомленнях категорій «Warning» (Попередження) та «Suggestion» (Пропозиція). Попередження зазвичай вказують на серйозні недоліки, такі як відсутність пароля на завантажувачі, некоректні права на файли конфігурації або наявність застарілого програмного забезпечення, що потребує негайного виправлення. Пропозиції носять рекомендаційний характер і спрямовані на подальше посилення захисту, наприклад, активацію додаткових модулів ядра або налаштування банерів безпеки. Систематичне виправлення виявлених недоліків дозволяє значно підвищити так званий «індекс безпеки» сервера, мінімізуючи поверхню атаки.

Наступним рівнем захисту веб-сервісів є протидія атакам методом повного перебору

(brute-force атаки), які спрямовані на підбір паролів до служб віддаленого доступу (SSH) або панелей адміністрування веб-додатків. Для автоматизації захисту від подібних загроз в інфраструктурі Linux використовується система запобігання вторгненням Fail2Ban. Цей сервіс функціонує шляхом постійного моніторингу лог-файлів (системних журналів) обраних служб. При виявленні підозрілої активності, яка відповідає заданим шаблонам (наприклад, багаторазові невдалі спроби входу з однієї IP-адреси), Fail2Ban динамічно змінює правила міжмережевого екрану (iptables або nftables), тимчасово або постійно блокуючи доступ для джерела атаки. Інсталяція сервісу виконується командою sudo apt install fail2ban –y [40].

Після інсталяції пакета необхідно забезпечити автоматичний запуск служби при завантаженні системи та її негайну активацію. Це досягається послідовним виконанням команд управління системними службами: sudo systemctl enable fail2ban для додавання в автозавантаження та sudo systemctl start fail2ban для запуску служби. Архітектура конфігурації Fail2Ban передбачає використання файлів .conf для стандартних налаштувань, які можуть бути перезаписані при оновленні пакету, та файлів .local для користувацьких налаштувань. Тому, згідно з кращими практиками адміністрування, редагування основного конфігураційного файлу jail.conf не рекомендується. Замість цього створюється або редагується файл локальних правил jail.local.

Налаштування правил захисту веб-сервера здійснюється шляхом редагування файлу конфігурації через текстовий редактор, наприклад, командою sudo nano /etc/fail2ban/jail.local. У цьому файлі описуються так звані «ізолятори» для конкретних сервісів. Для веб-серверів Apache або Nginx налаштовуються секції, що відстежують логи помилок та логи доступу. Визначаються параметри bantime (час блокування порушника), findtime (інтервал часу, за який підраховуються невдалі спроби) та maxretry (максимальна допустима кількість спроб перед блокуванням). Коректно налаштований файл jail.local дозволяє ефективно відсікати автоматизовані бот-мережі, що сканують сервер на наявність вразливостей, не впливаючи при цьому на легітимний трафік. Після внесення змін служба перезапускається для застосування нових правил.

Окрім внутрішнього аудиту та захисту, важливим аспектом безпеки є зовнішнє тестування периметра мережі, яке імітує дії потенційного зловмисника. Для виявлення відкритих портів, доступних сервісів та версій програмного забезпечення використовується мережевий сканер Nmap. Цей інструмент дозволяє адміністратору побачити свій сервер «очима хакера» і виявити непотрібні відкриті служби, які можуть слугувати точкою входу для атаки. Перед використанням утиліту необхідно інсталювати в систему командою sudo apt install nmap –y. Регулярне сканування дозволяє контролювати дотримання принципу мінімізації привілеїв, згідно з яким доступними ззовні мають бути лише критично необхідні порти (зазвичай 80, 443 та порт SSH).

Процедура тестування вразливостей ініціюється запуском Nmap з певними параметрами сканування. Команда sudo nmap -sV -p 1-1000 <IP-серверу> виконує сканування першої тисячі портів вказаного хоста. Параметр -sV є ключовим у даному контексті, оскільки він активує режим визначення версій служб (Service Version Detection). Це дозволяє отримати інформацію не лише про те, що порт відкритий, а й про те, яка саме служба його прослуховує (наприклад, Apache 2.4.41 або Nginx 1.18.0). Знання точної версії ПЗ є критичним для аналізу безпеки, оскільки дозволяє перевірити наявність відомих CVE (Common Vulnerabilities and Exposures) для даної версії. Якщо сканування виявляє порти, які не повинні бути публічними (наприклад, порти баз даних 3306 або службові порти 8080), адміністратор повинен негайно закрити їх за допомогою брандмауера UFW.

Важливою складовою безпеки веб-сервісів є також налаштування міжмережевого екрану. В Ubuntu Server стандартним є використання UFW – інтерфейсу для спрощеного управління правилами iptables. Політика безпеки за замовчуванням має бути налаштована на заборону всіх вхідних з'єднань (default deny incoming) та дозвіл вихідних (default allow outgoing). Дозвіл на вхідні з'єднання надається виключно для необхідних протоколів: SSH (порт 22 або змінений), HTTP (80) та HTTPS (443). Це створює надійний бар'єр, що запобігає несанкціонованому доступу до внутрішніх системних служб, які можуть бути активовані за замовчуванням, але не призначені для публічного використання [40].

Захист даних під час передачі забезпечується використанням криптографічних протоколів SSL/TLS. Сучасний стандарт безпеки вимагає обов'язкового використання HTTPS для всіх веб-ресурсів. У середовищі Linux для цього широко використовується інструмент Certbot, який дозволяє автоматизувати процес отримання та оновлення безкоштовних сертифікатів від центру сертифікації Let's Encrypt. Налаштування веб-сервера повинно включати відключення застарілих версій протоколів (SSLv3, TLS 1.0, TLS 1.1) та слабких алгоритмів шифрування. Крім того, рекомендується впровадження механізму HSTS (HTTP Strict Transport Security), який примушує браузери використовувати виключно захищене з'єднання, запобігаючи атакам типу «downgrade» та перехопленню сесій.

Додатковий рівень безпеки реалізується через налаштування спеціальних HTTP-заголовків у конфігурації веб-сервера (Nginx або Apache). Заголовки, такі як X-Frame-Options (запобігає атакам Clickjacking), X-Content-Type-Options (забороняє браузеру змінювати MIME-типи файлів) та Content-Security-Policy (CSP) (обмежує джерела завантаження контенту, захищаючи від XSS-атак), є обов'язковими для сучасних веб-додатків. Впровадження CSP вимагає ретельного аналізу роботи додатку, оскільки некоректна політика може порушити функціональність сайту, блокуючи легітимні скрипти або стилі [40].

Варто зазначити, що тільки комплексне поєднання методів захисту дозволяє гарантувати стабільну та безпечну роботу веб-сервісів у мережевому середовищі.

Журнали і моніторинг

Ефективне адміністрування серверної інфраструктури неможливе без реалізації комплексної стратегії спостережуваності, яка складається з двох фундаментальних компонентів: журналювання подій (логування) та моніторингу стану системи.

Журнали забезпечують історичний контекст, фіксуючи дискретні події, що відбулися в минулому, тоді як моніторинг надає інформацію про поточний стан ресурсів та метрик продуктивності в реальному часі. У середовищі Ubuntu Server ці процеси реалізуються через взаємодію системних служб, ядра операційної системи та спеціалізованих утиліт аналізу.

Центральним елементом підсистеми журналювання в сучасних дистрибутивах Linux, включаючи Ubuntu, є служба systemd-journald. Вона перехоплює повідомлення від ядра, служб ініціалізації, стандартного виводу процесів (stdout/stderr) та системної служби журналювання syslog. На відміну від традиційних текстових файлів, journald зберігає дані у бінарному структурованому форматі, що забезпечує індексацію та швидкий пошук. Доступ до цих даних здійснюється через утиліту journalctl. Адміністратор має можливість фільтрувати події за часом (наприклад, journalctl --since «1 hour ago»), за конкретним сервісом (параметр -u, наприклад, journalctl -u nginx) або за пріоритетом повідомлення. Для перегляду подій у режимі реального часу використовується прапор -f (follow), що дозволяє відслідковувати нові записи в момент їх появи, що є аналогом команди tail -f для текстових файлів [38].

Паралельно з journald у системі функціонує служба rsyslog, яка забезпечує сумісність із класичним стандартом syslog та відповідає за запис текстових лог-файлів у директорію /var/log. Основним файлом, де агрегується більшість системних повідомлень, є /var/log/syslog (або /var/log/messages у деяких дистрибутивах). Події, пов’язані з механізмами автентифікації та авторизації, включаючи спроби входу через SSH або виконання команд через sudo, записуються у файл /var/log/auth.log. Аналіз цього файлу є обов’язковою процедурою при розслідуванні інцидентів безпеки. Ядро операційної системи веде власний кільцевий буфер повідомлень, вміст якого можна переглянути командою dmesg або у файлі /var/log/kern.log. Це джерело інформації є першочерговим при діагностиці проблем з апаратним забезпеченням, драйверами пристроїв або мережевим стеком на низькому рівні.

Окремої уваги заслуговує управління дисковим простором, що займають журнали. Оскільки сервери функціонують у режимі постіної роботи, обсяг текстових логів може зростати безконтрольно, що загрожує переповненням файлової системи. Для вирішення цієї проблеми в Linux використовується механізм ротації журналів, що реалізується утилітою logrotate. Конфігурація ротації визначається у файлі /etc/logrotate.conf та директорії /etc/logrotate.d/. Процес ротації передбачає періодичне перейменування поточного файлу журналу (наприклад, у syslog.1), його архівування (компресію у syslog.2.gz) та створення

нового порожнього файлу для запису актуальних подій. Ця процедура виконується автоматично за розкладом планувальника завдань cron, що забезпечує стабільність використання дискового простору без втручання адміністратора.

У контексті веб-сервісної інфраструктури, налаштованої на базі Apache2 та Nginx, журналювання набуває специфічної структури. Кожен веб-сервер веде два основних типи журналів: журнал доступу та журнал помилок. Для Apache стандартним розташуванням є /var/log/apache2/access.log та /var/log/apache2/error.log. Журнал доступу фіксує кожен HTTP-запит, що надходить до сервера, зберігаючи IP-адресу клієнта, час запиту, метод (GET, POST тощо), запитуваний ресурс, код відповіді статусу (наприклад, 200 або 404) та інформацію про клієнтський агент. Аналіз журналу доступу дозволяє будувати статистику відвідуваності, виявляти патерни поведінки користувачів та ідентифікувати джерела аномального трафіку. Журнал помилок, своєю чергою, містить детальну інформацію про внутрішні збої сервера, помилки в скриптах веб-додатку або проблеми з конфігурацією, що робить його основним інструментом відлагодження для розробників та системних адміністраторів [38].

Для моніторингу та отримання миттєвого зрізу стану системи в терміналі використовується утиліта top або її більш функціональний аналог htop. Ці інструменти відображають список активних процесів, відсортованих за споживанням процесорного часу або оперативної пам’яті, а також загальні показники навантаження системи (Load Average). Показник Load Average, що складається з трьох значень (за 1, 5 та 15 хвилин), відображає середню кількість процесів, що очікують на виконання або введення-виведення. Якщо це значення перевищує кількість доступних процесорних ядер, це свідчить про перевантаження системи та необхідність оптимізації або масштабування ресурсів.

Для детального аналізу підсистеми пам’яті використовується команда free -h, яка показує загальний обсяг фізичної пам’яті, обсяг використаної та вільної пам’яті, а також розмір буферів та кеш-пам’яті. Важливо розуміти, що Linux агресивно використовує вільну оперативну пам’ять для дискового кешування з метою пришвидшення роботи системи, тому низьке значення стовпця «free» при високому значенні «available» є нормальною поведінкою. Для діагностики проблем з дисковою підсистемою застосовується утиліта iostat (з пакету sysstat), яка дозволяє виявити вузькі місця у швидкості читання/запису на накопичувачі, а команда df -h надає інформацію про доступний простір на змонтованих файлових системах. Вичерпання дискового простору є типовою причиною аварійної зупинки сервісів.

Моніторинг мережевої активності у Linux є критично важливим для забезпечення доступності веб-сервісів та деяких інших ролей сервера (DNS, DHCP та ін.). Для візуального моніторингу в середовищі з графічним інтерфейсом відкриваються «Додатки», там здійнсюється пошук групи додатків «Система», і там обирається «System Monitor» (Системний монітор). У вікні «Системного монітора» здійнюється перехід на вкладку

«Resources» (Ресурси). У розділі «Мережа» відображаються: швидкість прийому/передачі даних на сервері (RX/TX) та загальний обсяг переданих даних. Це надає загальну картину завантаженості мережевого інтерфейсу. Також у вкладці «Processes» (Процеси) можна відсортувати процеси та подивитися, які програми активно використовують мережу.

У професійному адмініструванні серверів, де графічний інтерфейс часто відсутній, моніторинг мережевої активності здійснюється переважно у терміналі. Для аналізу відкритих портів та встановлених з'єднань використовується команда ss. Активні з'єднання переглядаються командою ss -tulpn. Дана команда показує активні сокети (TCP/UDP), стан з'єднання (LISTEN, ESTABLISHED), локальні та віддалені адреси й процеси, що ініціювали з'єднання. Це дозволяє швидко виявити несанкціоновані служби або перевірити, чи коректно веб-сервер прослуховує необхідні порти [38].

Для моніторингу трафіку конкретного мережевого інтерфейсу в реальному часі встановлюється в терміналі інструмент «iftop». Це виконується командою sudo apt install iftop –y. Після цього запускається даний інструмент – sudo iftop -i enp0s3. Замість «enp0s3» використовується актуальна назва інтерфейсу, яку можна дізнатися командою ip addr. Утиліта iftop візуалізує поточні з'єднання між локальним хостом та віддаленими адресами, відображаючи смугу пропускання для кожного з'єднання окремо, що дозволяє ідентифікувати клієнтів, які генерують найбільше трафіку.

У випадках, коли необхідно визначити, який саме локальний процес споживає мережевий трафік, стандартних засобів може бути недостатньо. Для моніторингу трафіку по процесах виконується встановлення «nethogs». Для цього вписується команда sudo apt install nethogs –y і встановлюється даний інструмент. Після цього запускається – sudo nethogs. Ця утиліта групує трафік не за IP-адресами, а за PID (індентифікаторами процесів), показуючи, які процеси створюють навантаження на мережу (швидкість відправки SENT та отримання RECEIVED). Це незамінний інструмент для виявлення завислих скриптів резервного копіювання або скомпрометованих процесів, що генерують паразитний трафік.

Для моніторингу статистики інтерфейсів та помилок в передачі мережевого трафіку на канальному рівні застосовується команда ip -s link. Дана команда виведе детальну статистику по кожному мережевому інтерфейсу, включаючи кількість переданих пакетів, байтів, а також лічильники помилок, відкинутих пакетів, колізій та переповнень буфера (overrun). Наявність зростаючої кількості помилок у виводі цієї команди часто свідчить про фізичні проблеми з мережевим обладнанням, кабелями або некоректні налаштування дуплексу на комутаторі.

Моніторинг мережевої активності у Linux дозволяє контролювати використання мережевих ресурсів, виявляти аномалії та потенційні загрози, а також оптимізувати продуктивність системи. Використовуючи інструменти як ss, iftop, nethogs та графічні утиліти в GNOME, адміністратор може отримувати детальну інформацію про з'єднання,

трафік та активні процеси. Регулярний моніторинг підвищує безпеку та стабільність серверного середовища. Однак, ручний моніторинг через термінал є ефективним лише для оперативної діагностики «тут і зараз». А для побудови довгострокової стратегії обслуговування та моніторингу рекомендується впровадження систем автоматизованого централізованого збору метрик (наприклад, Prometheus у зв’язці з Grafana) та систем агрегації журналів (ELK Stack: Elasticsearch, Logstash, Kibana), які дозволяють автоматизувати виявлення інцидентів та вести постійний моніторинг.

Тема 12
Комплексне адміністрування мереж і систем

Побудова корпоративної інфраструктури

Проектування та розгортання корпоративної IT-інфраструктури є фундаментальним етапом у забезпеченні безперервності бізнес-процесів сучасного підприємства. Сучасний підхід до побудови таких систем базується на відмові від монолітних одноплатформних рішень на користь гетерогенних (змішаних) середовищ, де співіснують різні операційні системи, виконуючи специфічні ролі відповідно до їх архітектурних переваг. У професійній практиці є випадки поєднання ОС Microsoft Windows Server, яка забезпечує централізоване управління ідентифікацією та робочими станціями, та Linux-серверів (зокрема, на базі дистрибутиву Ubuntu), які виступають платформою для високонавантажених веб-сервісів, баз даних та контейнеризації. Розробка архітектури такої інфраструктури вимагає глибокого розуміння принципів мережевої та операційної взаємодії Windows та Linux, протоколів автентифікації та механізмів відмовостійкості.

Центральним елементом управління корпоративною мережею традиційно виступає служба каталогів, реалізація якої покладається на Windows Server з роллю Active Directory Domain Services (AD DS). Ця технологія дозволяє структурувати всі об’єкти мережі – користувачів, комп’ютери, принтери та сервіси – у єдину ієрархічну базу даних. При проектуванні інфраструктури створюється логічна структура лісу та доменів, що дозволяє делегувати повноваження та застосовувати групові політики. Саме механізм GPO є критично важливим для автоматизації налаштувань безпеки, розгортання програмного забезпечення та керування конфігураціями на сотнях або тисячах клієнтських машин. Для забезпечення надійності служби каталогів розгортається мінімум два контролери домену, що забезпечує реплікацію даних та доступність сервісу автентифікації навіть у випадку виходу з ладу одного з серверів. Важливим аспектом є налаштування DNS-сервера, інтегрованого в Active Directory, оскільки коректна робота служби розв’язання імен є обов’язковою умовою функціонування протоколу Kerberos, який використовується для безпечної автентифікації клієнтів у домені [3].

Паралельно з розгортанням служби каталогів, у корпоративну інфраструктуру інтегруються сервери на базі Ubuntu Linux, які беруть на себе роль платформи для розміщення прикладних сервісів та додатків. Вибір Linux-середовища зумовлений його високою стабільністю, ефективністю використання апаратних ресурсів та гнучкістю налаштувань. У типовій архітектурі на Ubuntu Server розгортаються веб-сервери (Apache, Nginx), системи керування базами даних (PostgreSQL, MySQL/MariaDB) та сервіси кешування (Redis). Окремим вектором використання Linux у корпоративному сегменті є впровадження технологій контейнеризації (Docker) та оркестрації (Kubernetes), що дозволяє

реалізувати мікросервісну архітектуру та забезпечити швидке масштабування додатків. Адміністрування таких серверів здійснюється переважно через захищений протокол SSH, що вимагає впровадження суворих політик доступу, зокрема використання ключів шифрування замість парольної автентифікації та налаштування міжмережевих екранів на рівні хоста.

Ключовим викликом при побудові інфраструктури є забезпечення інтероперабельності – здатності різних систем ефективно взаємодіяти між собою. Для уникнення дублювання облікових записів та спрощення адміністрування, Linux-сервери інтегруються в домен Windows Active Directory. Це досягається шляхом використання протоколів LDAP (Lightweight Directory Access Protocol) та Kerberos через проміжне програмне забезпечення, таке як SSSD (System Security Services Daemon) або Winbind. Реалізація такої інтеграції дозволяє системним адміністраторам використовувати єдині доменні облікові записи для входу на Linux-сервери, а також керувати доступом до ресурсів на основі членства в групах Active Directory. Таким чином, створюється єдиний простір автентифікації (Single Sign-On), що значно підвищує рівень безпеки та зручність користування системою.

Організація файлового обміну в корпоративній мережі також передбачає використання сильних сторін обох платформ. Windows Server часто використовується для надання доступу до файлів користувачам Windows-клієнтів через протокол SMB (Server Message Block), забезпечуючи підтримку тіньових копій та детальне розмежування прав доступу. Водночас, Ubuntu Server може виступати як високопродуктивне файлове сховище для бекенд-систем, використовуючи протокол NFS (Network File System) або розгортаючи Samba-сервер для обслуговування змішаних клієнтів. Важливим елементом є побудова системи резервного копіювання, яка повинна охоплювати як дані на Windows-серверах (стан системи, бази даних AD), так і конфігурації та дані додатків на Linux-серверах. Для цього проектуються окремі мережеві сегменти (VLAN) для трафіку резервного копіювання, щоб не навантажувати основну виробничу мережу [3].

Мережева архітектура корпоративної інфраструктури проектується з урахуванням вимог безпеки та сегментації. Виконується розділення мережі на декілька логічних зон: DMZ (демілітаризована зона) для сервісів, доступних з Інтернету (наприклад, веб-фронтенди на Ubuntu), внутрішню серверну зону для баз даних та контролерів домену, та клієнтську зону для робочих станцій. Маршрутизація та фільтрація трафіку між цими зонами здійснюється на корпоративному шлюзі або за допомогою програмних маршрутизаторів. У середовищі Ubuntu Server часто реалізуються функції програмного шлюзу, VPN-сервера (OpenVPN, WireGuard) або проксі-сервера (Squid) для контролю доступу співробітників до мережі Інтернет. Windows Server, у свою чергу, може виконувати ролі DHCP-сервера для автоматичного розподілу IP-адрес та центру сертифікації (Certification Authority) для видачі внутрішніх SSL-сертифікатів, необхідних для шифрування трафіку всередині периметра [4].

Управління оновленнями та конфігураціями в такому розгалуженому середовищі вимагає використання спеціалізованих інструментів автоматизації. Для Windows-інфраструктури розгортається служба WSUS (Windows Server Update Services), яка дозволяє централізовано затверджувати та розповсюджувати оновлення безпеки на сервери та робочі станції, мінімізуючи споживання зовнішнього інтернет-трафіку. Для парку Linux-серверів застосовуються системи управління конфігураціями, такі як Ansible, Puppet або Chef. Ці інструменти дозволяють описувати бажаний стан інфраструктури у вигляді коду та автоматично приводити сервери у відповідність до заданих параметрів, встановлювати пакети та оновлювати конфігураційні файли. Такий підхід гарантує ідентичність налаштувань на всіх вузлах та значно прискорює відновлення сервісів у разі аварій.

Завершальним етапом побудови інфраструктури є впровадження системи моніторингу та журналювання. Проектується централізований сервер збору логів (наприклад, на базі стеку ELK: Elasticsearch, Logstash, Kibana або Graylog), який агрегує журнали подій як з Windows Server (Event Viewer), так і з Linux (syslog/journald). Це дозволяє оперативно виявляти аномалії, спроби несанкціонованого доступу та технічні збої. Паралельно розгортається система моніторингу продуктивності (наприклад, Zabbix або Prometheus), яка в реальному часі відслідковує стан завантаження процесорів, використання пам’яті, вільного дискового простору та доступності мережевих сервісів. Налаштування сповіщень дозволяє адміністраторам проактивно реагувати на потенційні проблеми ще до того, як вони вплинуть на бізнес-процеси компанії.

Взаємодія Windows та Linux-сервісів

Взаємодія між Windows Server 2025, що традиційно виконує роль центру керування ідентифікацією та політиками, та серверами на базі Linux (Ubuntu), які забезпечують роботу мікросервісів, веб-інфраструктури та баз даних, базується на використанні стандартизованих мережевих протоколів та спеціалізованого проміжного програмного забезпечення. Глибоке розуміння механізмів цієї взаємодії на рівнях автентифікації, файлового обміну, розв’язання імен та віддаленого керування є обов’язковим для побудови та адміністурвання стійкої та керованої IT-інфраструктури підприємства.

Фундаментальним рівнем інтеграції Linux-серверів у доменну інфраструктуру Windows є єдиний простір автентифікації та авторизації. Оскільки Windows Server використовує протокол Kerberos V5 для автентифікації та LDAP (Lightweight Directory Access Protocol) для доступу до служби каталогів Active Directory, інтеграція Ubuntu Server вимагає налаштування клієнтських служб, здатних взаємодіяти з цими протоколами. Ключовим компонентом у цій схемі виступає служба SSSD (System Security Services Daemon). Вона функціонує як посередник між системними викликами автентифікації Linux (через модулі

PAM – Pluggable Authentication Modules) та службою Active Directory. При спробі входу користувача на Linux-сервер, SSSD формує запит до контролера домену Windows Server 2025, отримує TGT (Ticket Granting Ticket) квиток Kerberos та здійснює перевірку облікових даних без необхідності створення локальних облікових записів на кожному окремому сервері [3].

Технічна складність інтеграції полягає у відмінностях систем ідентифікаторів безпеки. Windows оперує довгими ідентифікаторами SID (Security Identifier), тоді як файлова система Linux базується на числових значеннях UID та GID. Для вирішення цієї колізії використовується механізм відображення ідентифікаторів. У сучасних реалізаціях SSSD застосовується алгоритмічне відображення, яке генерує стабільні UID/GID на основі унікального SID користувача Active Directory. Це гарантує, що один і той самий користувач матиме однакові ідентифікатори на всіх Linux-серверах у мережі, що є необхідним для коректної роботи мережевих файлових систем. Альтернативний підхід передбачає зберігання UID/GID безпосередньо як атрибутів об’єкта користувача в схемі Active Directory (RFC 2307), що вимагає розширення схеми та додаткового налаштування на стороні Windows Server.

Забезпечення коректної роботи механізму автентифікації Kerberos неможливе без точної синхронізації часу, оскільки протокол використовує часові мітки для захисту від атак повторного відтворення. Максимально допустиме розходження часу за замовчуванням становить 5 хвилин. У гібридній інфраструктурі Windows Server 2025 з роллю PDC Emulator (Primary Domain Controller) виступає як авторитетне джерело часу для всього лісу доменів. На стороні Ubuntu Server налаштовується служба синхронізації часу (наприклад, chronyd або systemd-timesyncd), яка конфігурується для отримання точного часу безпосередньо від контролерів домену через протокол NTP (Network Time Protocol). Це створює ієрархічну структуру розподілу часу, де Linux-клієнти розглядають контролери домену як stratum-джерела вищого рівня, забезпечуючи криптографічну валідацію сесій.

Наступним аспектом взаємодії є спільне використання файлових ресурсів. Стандартом для цього є протокол SMB (Server Message Block). У середовищі Ubuntu Server підтримка цього протоколу реалізується за допомогою пакету програмного забезпечення Samba. Samba може виступати як у ролі клієнта, дозволяючи монтувати спільні папки Windows Server у файлову систему Linux, так і в ролі файлового сервера, надаючи ресурси для Windows-клієнтів. При конфігурації Samba як файлового сервера, що входить до складу домену Active Directory, використовується служба winbind або інтеграція з SSSD для трансляції списків контролю доступу (ACL). Це дозволяє адміністраторам призначати права доступу до файлів на Linux-сервері, використовуючи групи безпеки Windows, що забезпечує централізоване управління правами доступу [3].

Особливу увагу при налаштуванні файлового обміну слід приділяти узгодженню версій протоколу SMB. Windows Server 2025 пріоритезує використання SMB 3.1.1, який

підтримує шифрування трафіку (AES-128/AES-256) та захист від підробки. На стороні Linux необхідно явно налаштувати конфігурацію Samba (файл smb.conf) для підтримки цих функцій безпеки, відключаючи застарілий та вразливий протокол SMBv1. Крім того, при монтуванні Windows-ресурсів на Linux-сервери (наприклад, для резервного копіювання баз даних) через утиліту mount.cifs, застосовуються параметри, що визначають власника змонтованих файлів у контексті локальної системи Linux, оскільки файлова система NTFS, що використовується Windows, має складнішу структуру метаданих прав доступу, ніж стандартні права POSIX [3].

Взаємодія на рівні системи доменних імен (DNS) є основою для функціонування служби каталогів. У типовому сценарії Windows Server виконує роль основного DNS-сервера для зони Active Directory. Linux-сервери повинні бути налаштовані на використання контролерів домену як основних резолверів DNS. Це необхідно для коректного пошуку службових записів SRV (англ. Service Records), які вказують на розташування служб LDAP, Kerberos та Global Catalog. Важливим аспектом є механізм динамічного оновлення DNS (DDNS). Windows-клієнти оновлюють свої A та PTR записи автоматично. Для Linux-серверів цей процес вимагає додаткового налаштування – SSSD або DHCP-клієнт можуть бути сконфігуровані для відправки запитів на оновлення DNS-зони, використовуючи GSS-TSIG (Generic Security Service Algorithm for Secret Key Transaction) для безпечної автентифікації оновлення запису на Windows DNS сервері.

Віддалене адміністрування та управління конфігураціями в змішаному середовищі зазнало значної еволюції. Якщо раніше для керування Linux з Windows використовувалися сторонні утиліти (PuTTY), то в сучасних версіях Windows Server, включаючи редакцію 2025, клієнт і сервер OpenSSH інтегровані в операційну систему як нативні компоненти. Це дозволяє будувати уніфіковані сценарії керування, де адміністратор може ініціювати SSH-сесії між будь-якими вузлами мережі незалежно від ОС. Більше того, розвиток крос-платформної оболонки PowerShell Core дозволяє виконувати скрипти адміністрування на Linux-серверах, використовуючи звичний синтаксис командлетів Windows, або ж використовувати протокол PowerShell Remoting over SSH (PSRP) для створення захищених каналів управління [3].

На рівні прикладного програмного забезпечення взаємодія часто реалізується через архітектуру «зворотного проксі». У таких сценаріях високопродуктивний веб-сервер Nginx на базі Ubuntu приймає вхідні з’єднання з Інтернету, здійснює термінацію SSL/TLS шифрування, балансування навантаження та кешування статичного контенту, а потім передає очищені запити на бекенд-сервери під управлінням Windows Server (з роллю IIS), де виконується бізнес-логіка на платформі ASP.NET. Така схема дозволяє поєднати безпеку та швидкість обробки запитів Linux з потужними можливостями розробки корпоративних

додатків стеку Microsoft. Налаштування такої взаємодії вимагає точного узгодження HTTP-заголовків, щоб бекенд на Windows коректно ідентифікував IP-адресу клієнта.

Ще одним вектором взаємодії є інтеграція баз даних. Корпоративні додатки, розгорнуті на Windows Server, часто потребують доступу до баз даних PostgreSQL або MySQL, що функціонують на Linux. Взаємодія реалізується через стандартні інтерфейси ODBC (Open Database Connectivity) або JDBC. Ключовим моментом тут є конфігурація мережевих екранів. Windows Defender Firewall на стороні клієнта та UFW або iptables на стороні Linux-сервера повинні бути налаштовані на пропуск трафіку по специфічних портах (наприклад, 5432 для PostgreSQL). Крім того, для забезпечення безпеки передачі даних між серверами різних платформ обов'язковою є активація SSL-шифрування з'єднань на рівні драйверів баз даних, що вимагає розгортання та довіри до корпоративних сертифікатів на обох кінцях з'єднання.

Окремим, але важливим аспектом є використання підсистеми WSL (Windows Subsystem for Linux) на адміністративних станціях під управлінням Windows. Хоча це технологія клієнтського рівня, вона дозволяє системним адміністраторам використовувати нативні інструменти Linux (bash, grep, sed, ansible) для керування віддаленими Linux-серверами безпосередньо з середовища Windows, без необхідності використання віртуальних машин або подвійного завантаження.

Резервування й відмовостійкість

Забезпечення високої доступності та відмовостійкості є основною вимогою у проектуванні сучасної IT-інфраструктури (мережевої та серверної інфраструктури) підприємства. У контексті комплексного адміністрування під відмовостійкістю розуміється здатність системи продовжувати функціонування без переривання сервісу або втрати даних у разі виходу з ладу одного або декількох її компонентів. Резервування, своєю чергою, виступає технічним засобом досягнення цієї мети шляхом дублювання критично важливих вузлів: мережевих інтерфейсів, дисків, блоків живлення, серверів або цілих центрів обробки даних. Реалізація цих механізмів у середовищах Windows Server 2025 та Ubuntu Server вимагає системного підходу, що охоплює апаратний, системний та прикладний рівні, спрямований на мінімізацію часу простою та досягнення цільових показників доступності.

На рівні мережевої взаємодії першочерговим завданням є усунення єдиної точки відмови у каналі передачі даних. Для цього застосовується технологія агрегації мережевих інтерфейсів. У середовищі Windows Server 2025 цей механізм реалізується через функцію NIC Teaming або через Switch Embedded Teaming (SET), що інтегрується з віртуалізацією Hyper-V. Це дозволяє об'єднати декілька фізичних мережевих адаптерів у єдиний логічний інтерфейс. У разі фізичного пошкодження кабелю або виходу з ладу порту комутатора, трафік

автоматично перенаправляється через інші активні адаптери без розриву з'єднань. Аналогічний підхід реалізується в Ubuntu Server за допомогою технології Network Bonding або Teaming, що налаштовується через утиліту Netplan. Найбільш ефективним режимом роботи в обох системах є використання протоколу LACP (IEEE 802.3ad), який забезпечує як відмовостійкість, так і балансування навантаження, збільшуючи пропускну здатність каналу.

Захист даних від втрати внаслідок апаратних збоїв накопичувачів забезпечується технологіями дискового резервування. Базовим рівнем є використання RAID-масивів (Redundant Array of Independent Disks). У сучасних корпоративних системах перевага надається програмно-визначеним сховищам (Software-Defined Storage – SDS). У Windows Server 2025 ключовою технологією є Storage Spaces Direct (S2D). Вона дозволяє об'єднувати локальні диски декількох серверів у єдиний віртуальний пул зберігання, забезпечуючи реплікацію даних між вузлами (двостороннє або тристороннє дзеркалювання). У разі виходу з ладу цілого сервера, дані залишаються доступними з інших вузлів кластера. В системі Linux (Ubuntu) подібний функціонал реалізується через файлові системи ZFS або Btrfs, які підтримують вбудовані механізми RAID, а також через використання розподілених файлових систем, таких як Ceph або GlusterFS, що забезпечують реплікацію даних на мережевому рівні [3].

Найвищий рівень відмовостійкості сервісів досягається шляхом впровадження кластеризації. Для Windows Server 2025 основним інструментом є Windows Server Failover Clustering (WSFC). Ця технологія об'єднує групу незалежних серверів (вузлів) для спільної роботи. Моніторинг стану вузлів здійснюється через обмін спеціальними сигналами. У разі, якщо один із вузлів перестає відповідати, кластер ініціює процедуру аварійного перемикання, автоматично перезапускаючи служби та переміщуючи ресурси (наприклад, віртуальні машини або ролі баз даних) на справні вузли. Критично важливим елементом конфігурації WSFC є налаштування кворуму, який запобігає сценарію «розщеплення мозку», коли при порушенні зв'язку обидві частини кластера намагаються захопити управління одними й тими ж ресурсами, що може призвести до пошкодження даних [3].

В інфраструктурі на базі Ubuntu Server побудова кластерів високої доступності базується на використанні стеку програмного забезпечення Corosync та Pacemaker. Corosync відповідає за комунікацію між вузлами та забезпечення цілісності кластера, тоді як Pacemaker виступає менеджером ресурсів, керуючи запуском та зупинкою сервісів. Для забезпечення єдиної точки входу для клієнтів використовується механізм віртуальних IP-адрес, що реалізується за допомогою протоколу VRRP (Virtual Router Redundancy Protocol) через службу Keepalived. У такій конфігурації віртуальна IP-адреса динамічно призначається активному вузлу. При виникненні збою IP-адреса миттєво переноситься на резервний сервер, забезпечуючи прозорість перемикання для кінцевих користувачів. Для синхронізації

блокових пристроїв між вузлами в Linux часто використовується DRBD (Distributed Replicated Block Device), який фактично створює «мережевий RAID-1» [38].

Важливим аспектом забезпечення безперервності є балансування навантаження, яке часто поєднується з відмовостійкістю. Для веб-додатків це реалізується шляхом розгортання ферми серверів. У Windows Server для цього передбачено компонент Network Load Balancing (NLB), який розподіляє вхідні TCP/IP запити між декількома серверами. У середовищі Linux для цього передбачено використання високоефективних проксі-серверів, таких як HAProxy або Nginx, налаштованих у режимі балансувальників. Ці інструменти постійно перевіряють стан бекенд-серверів. Якщо один із серверів веб-додатку стає недоступним (повертає помилку 5xx або не відповідає), балансувальник виключає його з пулу активних ресурсів і перенаправляє трафік на інші працюючі сервери, запобігаючи відмові в обслуговуванні.

Окремим рівнем захисту є система резервного копіювання. Стратегія резервного копіювання повинна базуватися на правилі «3-2-1»: три копії даних, на двох різних носіях, одна з яких – за межами основного офісу. У Windows Server 2025 використовується технологія Volume Shadow Copy Service (VSS), яка дозволяє створювати миттєві знімки файлової системи навіть при відкритих файлах, що є особливо важливим для резервування баз даних Active Directory та SQL Server.

В Ubuntu Server використовуються знімки на рівні LVM (Logical Volume Manager) або файлової системи, а також спеціалізовані інструменти, такі як Bacula або BorgBackup, що підтримують дедуплікацію та шифрування резервних копій.

Для захисту від фізичних збоїв (пожежа, повінь, повне знеструмлення) розробляються плани аварійного відновлення. Вони передбачають реплікацію даних. У Windows Server це реалізується через Hyper-V Replica або Azure Site Recovery, що дозволяє асинхронно реплікувати віртуальні машини та запускати їх на резервному майданчику. У Linux-середовищі застосовуються методи реплікації на рівні баз даних (MySQL Replication, PostgreSQL Streaming Replication) та синхронізація файлових сховищ через rsync або розподілені файлові системи [3].

Ефективність плану визначається двома метриками: RPO (Recovery Point Objective) – максимальний допустимий обсяг втрачених даних (час з моменту останнього бекапу), та RTO (Recovery Time Objective) – допустимий час простою до повного відновлення сервісу.

Практичні підходи до документування

Документування інформаційних систем є невід’ємною складовою професійного адміністрування. У контексті експлуатації середовищ, що включають Windows Server 2025 та/або Ubuntu Server, документація виступає, як інформаційний актив, що описує поточний стан конфігурацій, архітектурні рішення та процедури відновлення. Відсутність актуальної

документації призводить до збільшення часу реакції на інциденти, ускладнює процес масштабування мережі та адміністрування серверів, а також робить систему залежною від унікальних знань окремих спеціалістів, що є неприпустимим у корпоративному секторі. Ефективна стратегія документування повинна охоплювати всі рівні моделі OSI, від фізичної комутації до прикладного програмного забезпечення, і базуватися на принципах повноти, актуальності та доступності.

Фундаментальним рівнем документування є фіксація мережевої топології. Для цього розробляються діаграми фізичного та логічного рівнів. На фізичних схемах відображається розміщення серверного обладнання в стійках, схеми кабельної розводки та підключення до джерел безперебійного живлення. Логічні схеми повинні детально описувати сегментацію мережі, структуру VLAN, IP-адресацію підмереж та налаштування маршрутизації. У сучасних умовах для цього використовуються спеціалізовані програмні засоби візуалізації, які дозволяють створювати інтерактивні карти мережі. Важливо, щоб на схемах були позначені всі активні вузли, включаючи сервери Windows та Linux, комутатори, маршрутизатори та міжмережеві екрани, із зазначенням їхніх інтерфейсів, MAC-адрес та пропускної здатності каналів зв’язку [1].

Наступним етапом є створення та ведення бази даних управління конфігураціями (CMDB). Цей ресурс слугує центральним репозиторієм інформації про всі елементи інфраструктури та взаємозв’язки між ними. Для кожного сервера, незалежно від операційної системи, у CMDB заноситься паспорт об’єкта, що містить апаратні характеристики (ЦП, ОЗП, HDD/SSD), серійні номери, терміни гарантійного обслуговування, а також перелік встановленого системного та прикладного програмного забезпечення. Особлива увага приділяється опису ролей сервера. Для Windows Server 2025 документуються налаштування Active Directory, DNS, DHCP, структура об’єктів групових політик (GPO) та схеми реплікації. Для Ubuntu Server фіксуються версії ядра, встановлені пакунки, конфігурації служб (Apache, Nginx, PostgreSQL) та скрипти автоматизації. CMDB дозволяє адміністраторам швидко оцінювати вплив потенційних змін на систему та планувати оновлення.

Управління адресним простором вимагає впровадження системи IPAM (IP Address Management). Використання електронних таблиць для обліку IP-адрес у великих мережах вважається застарілою та неефективною практикою, що призводить до конфліктів адрес. Документування IP-плану повинно здійснюватися через спеціалізовані програмні комплекси, які автоматично сканують мережу, виявляють активні хости та оновлюють статус IP-адрес. У документації чітко розмежовуються статичні адреси, призначені для серверів та мережевого обладнання, та динамічні пули DHCP для клієнтських станцій. Окрім самої адреси, фіксується інформація про призначене доменне ім’я, приналежність до VLAN та фізичне розташування пристрою. Це забезпечує прозорість мережевої інфраструктури та спрощує

діагностику проблем з підключенням [1].

Особливе місце в системі документації займають експлуатаційні процедури, відомі як стандартні операційні процедури або Runbooks. Це покрокові інструкції, що описують алгоритми дій адміністратора в типових та аварійних ситуаціях. Для Windows-середовища розробляються інструкції зі створення облікових записів користувачів, налаштування прав доступу, розгортання оновлень через WSUS та відновлення контролера домену. Для Linux-серверів описуються процедури оновлення пакетів, ротації логів, налаштування фаєрволу iptables/ufw, резервного копіювання баз даних та компіляції програмного забезпечення з вихідних кодів. Вони повинні бути написані максимально детально та однозначно.

Важливим аспектом є документування політик безпеки та контролю доступу. Повинна бути створена матриця доступу, яка визначає, які користувачі або групи мають права на доступ до конкретних ресурсів, серверів та файлових сховищ. Для Windows Server це включає опис структури груп безпеки Active Directory, прав доступу до спільних папок (SMB Shares) та політик аудиту. Для Ubuntu Server документуються налаштування sudoers, права доступу до файлової системи (chmod/chown) та правила SSH-доступу (дозволені користувачі, використання ключів). Також фіксуються правила міжмережевого екранування, тобто які порти відкриті, для яких джерел та з якою метою. Це є обов’язковою вимогою при проведенні аудитів безпеки та розслідуванні інцидентів.

Завершує систему документації план аварійного відновлення та план забезпечення безперервності. Цей документ містить критичну інформацію, необхідну для відновлення працездатності інфраструктури після глобальних збоїв. У ньому вказуються пріоритети відновлення сервісів, контактні дані відповідальних осіб та постачальників послуг, розташування резервних копій та ліцензійних ключів. План повинен містити детальні сценарії відновлення для критичних компонентів: перевстановлення ОС, відновлення Active Directory з резервної копії, розгортання веб-сервера та відновлення даних із хмарних сховищ. Регулярна перевірка та актуалізація цих планів є обов’язковою, оскільки застарілий план відновлення може виявитися марним у критичній ситуації.

Перспективи автоматизації адміністрування

Еволюція системного адміністрування на сучасному етапі характеризується значним зсувом парадигми від ручного керування окремими вузлами до комплексної автоматизації та оркестрації цілих IT-інфраструктур. Якщо раніше автоматизація сприймалася як набір допоміжних скриптів для виконання рутинних задач, то сьогодні вона стає архітектурною основою побудови серверних систем.

У контексті Windows Server 2025 та останніх версій Ubuntu Server (LTS) спостерігається перехід до концепції «Infrastructure as Code» (Інфраструктура як код), де стан

операційної системи повністю описується в декларативних конфігураційних файлах. Проте, нинішній рівень розвитку технологій є лише проміжним етапом перед впровадженням автономних систем управління на базі штучного інтелекту (AIOps), які здатні до діагностики та відновлення без втручання людини (потрібно лише початкове налаштування адміністратором).

У середовищі Windows Server 2025 автоматизація досягла нового рівня інтеграції з хмарними технологіями через механізм Azure Arc. Ця технологія дозволяє поширювати принципи управління хмарними ресурсами на локальні сервери. Реалізовано функціонал «hotpatching» (гаряче оновлення), який базується на модифікації коду ядра в оперативній пам'яті без необхідності перезавантаження фізичного сервера. Це рішення кардинально змінює підхід до автоматизації обслуговування, адже замість складних сценаріїв виведення вузлів з експлуатації для перезавантаження, система оновлюється в фоновому режимі, зберігаючи безперервність надання сервісів. Управління конфігураціями здійснюється через модернізований PowerShell та платформу Desired State Configuration (DSC) третього покоління, яка дозволяє не просто застосовувати налаштування, а й автоматично відслідковувати та виправляти «дрейф конфігурацій», повертаючи систему до еталонного стану при будь-яких несанкціонованих змінах [3].

В ОС Ubuntu Server автоматизація закладається на етапі інсталяції системи за допомогою механізму Cloud-init та Subiquity. Це дозволяє реалізувати концепцію «Zero-Touch Provisioning» (розгортання без дотиків), коли сервер отримує повну конфігурацію мережі, користувачів, ключів доступу та встановленого програмного забезпечення миттєво після першого завантаження, зчитуючи метадані з джерела даних (NoCloud, HTTP або сервісу метаданих провайдера). В останніх версіях Ubuntu глибоко інтегровано технологію Netplan для декларативного опису мережевих налаштувань у форматі YAML, що спрощує автоматичну генерацію конфігурацій для складних мережевих топологій. Крім того, інструментарій Canonical Landscape забезпечує централізоване управління тисячами машин, дозволяючи виконувати масові оновлення ядра без зупинки сервісів, що є аналогом Hotpatching у світі Linux [38].

Перспективним напрямком, що активно досліджується та вже частково впроваджується, є автоматизація на основі намірів. На відміну від імперативного підходу, де адміністратор описує послідовність дій (наприклад, «встановити пакет, відкрити порт, запустити службу»), підхід на основі намірів дозволяє оперувати кінцевим результатом (наприклад, «забезпечити захищений веб-сервер»). Майбутні версії серверних ОС будуть оснащені інтелектуальними агентами, здатними транслювати високорівневі вимоги в конкретні низькорівневі команди. У Windows Server це розвивається через інтеграцію з Microsoft Copilot for Security, який може генерувати складні політики безпеки та скрипти

PowerShell на основі запитів природною мовою, аналізуючи контекст інфраструктури.

Окремої уваги заслуговує розвиток AIOps (Artificial Intelligence for IT Operations) – застосування штучного інтелекту та машинного навчання для аналізу великих даних, що генеруються серверами. У майбутніх релізах Ubuntu Server та Windows Server очікується нативна інтеграція нейромережевих моделей для предиктивного обслуговування. Система не просто реагуватиме на збій, а прогнозуватиме його виникнення на основі аналізу патернів поведінки, таких, як зміни температури процесора, аномалії у використанні пам'яті або нетиповий мережевий трафік. Досліджуються алгоритми, які дозволять операційній системі автоматично ініціювати міграцію віртуальних машин з фізичного сервера, на якому прогнозується апаратний збій, ще до моменту його настання.

Вагомим вектором розвитку є перехід до концепції «незмінної інфраструктури» на рівні операційної системи. Традиційний підхід до адміністрування передбачає постійне внесення змін у працюючі сервери (оновлення, патчі, зміна конфігурацій), що з часом може призвести до накопичення помилок та нестабільності. Перспективні розробки, такі як Windows Server vNext та дистрибутиви типу Ubuntu Core, пропонують модель, де оновлення системи відбувається шляхом повної заміни образу ОС, а не модифікації окремих файлів. Атомарність оновлень гарантує, що система завжди перебуває у відомому та протестованому стані. У разі невдалого оновлення автоматично відбувається миттєвий відкат до попередньої версії, що зводить до мінімуму ризики, пов'язані з людським фактором при встановленні патчів [3].

Плюси впровадження таких високоавтоматизованих рішень є очевидними та вимірюваними. По-перше, це радикальне зниження операційних витрат (OPEX) за рахунок вивільнення часу системних адміністраторів від виконання рутинних завдань. Замість моніторингу фахівці можуть зосередитися на архітектурному плануванні та оптимізації. По-друге, виключається людський фактор, який є причиною більшості збоїв у конфігурації та безпеці. Машини виконують інструкції з абсолютною точністю та повторюваністю. По-третє, значно підвищується швидкість реакції на інциденти, оскільки автоматизовані системи здатні виявити та нейтралізувати загрозу за мілісекунди, тоді як людині на це потрібні хвилини або години.

Організація обміну файлами між Linux та Windows на основі протоколу SMB

Основним інструментом для організації прозорого, надійного та безпечного файлового обміну в середовищах з Windows та Linux виступає протокол SMB (Server Message Block), який, будучи нативним для Windows, реалізується в середовищі Linux за допомогою програмного комплексу Samba або модулів ядра. Проектування такої взаємодії передбачає не лише встановлення мережевого з'єднання, але й коректне узгодження атрибутів файлів,

кодувань символів та ідентифікаторів безпеки (SID у Windows та UID/GID у Linux), що є критичним для забезпечення цілісності даних при спільному доступі [3].

Реалізація файлового серверу на базі Windows Server 2025 для доступу клієнтів Linux починається з налаштування ролі файлових служб та конфігурації мережевих спільних ресурсів. У цьому процесі ключова увага приділяється дворівневій системі прав доступу: дозволам на рівні спільного ресурсу та спискам контролю доступу файлової системи NTFS (ACL). Для забезпечення максимальної сумісності та безпеки рекомендується на рівні спільного ресурсу надавати повний доступ групі автентифікованих користувачів, тоді як гранулярне розмежування прав здійснюється виключно засобами NTFS. При взаємодії з клієнтами Linux, які використовують сучасні версії ядра та пакету cifs-utils, Windows Server 2025 автоматично узгоджує використання діалекту протоколу SMB 3.1.1, що забезпечує підтримку шифрування AES-128-GCM або AES-256-GCM. Це нівелює ризики перехоплення даних у локальній мережі без необхідності додаткового налаштування VPN-тунелів, за умови, що адміністратором активовано вимогу шифрування для конкретного спільного ресурсу або всього сервера [41].

З боку клієнта Linux (на прикладі Ubuntu Server) доступ до ресурсів Windows здійснюється шляхом монтування віддаленої файлової системи у локальне дерево каталогів. Ця операція виконується за допомогою системного виклику mount із зазначенням типу файлової системи cifs. Важливим аспектом тут є передача параметрів монтування, які визначають, яким чином атрибути файлів Windows будуть інтерпретуватися ядром Linux. Оскільки NTFS має розширені атрибути (Hidden, System, Archive), які не мають прямих аналогів у стандартній моделі прав POSIX (rwx), драйвер CIFS виконує емуляцію. Адміністратором повинні бути чітко визначені параметри UID та GID, які вказують, під яким локальним користувачем та групою будуть відображатися змонтовані файли. Без цього кроку файли можуть належати користувачеві root, що унеможливить роботу звичайних додатків. Для автоматизації цього процесу запис про монтування вноситься до файлу /etc/fstab, де також рекомендується використовувати файл з обліковими даними з обмеженими правами доступу, щоб уникнути зберігання паролів у відкритому вигляді.

Зворотна задача – надання доступу до файлової системи Linux для клієнтів Windows – реалізується шляхом розгортання та конфігурації служби smbd зі складу пакету Samba. Більш глибока інтеграція досягається при включенні сервера Ubuntu в домен Active Directory (AD). У такому сценарії управління ідентифікацією делегується контролерам домену Windows, а Samba виступає в ролі рядового члена домену.

Окремої уваги заслуговує новітній підхід до реалізації SMB-сервера в Linux за допомогою модуля ядра ksmbd (Kernel SMB Daemon), який став доступним у нових версіях ядра Ubuntu Server. На відміну від традиційної Samba, яка працює в просторі користувача і

вимагає постійного копіювання даних між простором ядра та користувача для кожної операції вводу-виводу, ksmbd обробляє запити SMB безпосередньо в ядрі. Це архітектурне рішення спрямоване на підвищення пропускної здатності, особливо на високошвидкісних мережевих інтерфейсах (10Гбіт/с і вище) та при використанні технології RDMA (SMB Direct). Конфігурація ksmbd також використовує файл, сумісний за синтаксисом з smb.conf, або спеціалізовані утиліти управління, проте його функціонал наразі зосереджений на файловому сервісі, тоді як задачі контролера домену залишаються прерогативою класичної Samba [42].

Забезпечення узгодженості прав доступу між Windows та Linux є однією з найскладніших задач при налаштуванні SMB. Файлова система Linux (наприклад, EXT4) використовує POSIX ACL, які відрізняються від більш гнучких та детальних Windows ACL (NFSv4 ACL є ближчими, але не ідентичними). Samba виконує трансляцію цих прав, намагаючись максимально точно відобразити наміри адміністратора. Для коректної роботи часто використовується модуль VFS (Virtual File System) vfs_acl_xattr, який дозволяє зберігати Windows ACL у розширених атрибутах файлової системи Linux. Це дозволяє клієнтам Windows переглядати та редагувати права доступу через стандартну вкладку «Безпека» у властивостях файлу, при цьому Samba прозоро зберігає ці метадані, не порушуючи при цьому роботу локальних Linux-процесів. Адміністратору необхідно переконатися, що файлова система змонтована з підтримкою розширених атрибутів (user_xattr), що є стандартним для Ubuntu Server, але вимагає перевірки при використанні нестандартних файлових систем.

Моніторинг та діагностика з’єднань SMB здійснюються за допомогою спеціалізованих утиліт. На стороні Linux команда smbstatus надає детальну інформацію про поточні сесії, заблоковані файли та версії протоколу, що використовуються кожним клієнтом. Це дозволяє оперативно виявляти клієнтів, які намагаються підключитися з використанням застарілих протоколів, або діагностувати проблеми з блокуванням файлів, коли один користувач унеможливлює редагування документу іншим. На стороні Windows Server аналогічні функції виконуються через консоль управління «Computer Management» або за допомогою командлетів PowerShell Get-SmbSession та Get-SmbOpenFile. Аналіз логів /var/log/samba/ на Linux дозволяє відстежувати помилки автентифікації та проблеми доступу, при цьому рівень деталізації логів може бути динамічно змінений через smbcontrol без перезавантаження служби, що є важливим для діагностики в середовищі без переривання сервісу.

Протокол SMB

Впровадження технології SMB over QUIC у Windows Server 2025 є трансформаційним досягненням у сфері мережевих комунікацій. Шляхом поєднання усталеного,

багатофункціонального протоколу SMB із передовим, високопродуктивним протоколом QUIC, ця інтеграція забезпечує потужне рішення для підприємств, які прагнуть оптимізувати свої цифрові інфраструктури. Використовуючи можливості SMB у сфері спільного використання файлів і безпеки в парі зі здатністю QUIC підвищувати швидкість та зменшувати затримки, IT-фахівці отримують інструменти для значного підвищення ефективності передачі даних, посилення надійності мережі та покращення заходів безпеки. У цьому розділі досліджується еволюція SMB over QUIC, пропонується детальний аналіз його функціональності та висвітлюються ключові переваги, що роблять його важливим компонентом сучасних мережевих екосистем [3].

SMB та QUIC є критично важливими компонентами сучасних мережевих комунікацій, кожен з яких відіграє окрему, але доповнювальну роль. Для IT-фахівців, які працюють із Windows Server 2025, розуміння перетину цих двох технологій є ключовим для оптимізації продуктивності мережі, безпеки та ефективності.

SMB (Server Message Block) – це давній протокол, що використовується корпорацією Microsoft як у клієнтських, так і в серверних операційних системах, забезпечуючи спільне використання файлів, принтерів та пристроїв у мережах. Протягом багатьох років він еволюціонував із покращеннями функціональності, безпеки та продуктивності. Працюючи переважно поверх TCP/IP, SMB надає критичні функції, такі як шифрування, підписування та версійність, що гарантують безпечний та надійний обмін даними між різними платформами та пристроями [3].

Проткол SMB став рішенням для підприємств, які потребують надійних можливостей кросплатформного обміну даними. На відміну від нього, QUIC (Quick UDP Internet Connections) є відносно новим протоколом, розробленим компанією Google. Працюючи на транспортному рівні, QUIC використовує протокол користувацьких датаграм (UDP) – швидкий протокол без встановлення з’єднання, що застосовується для передачі даних без корекції помилок або гарантій доставки – замість TCP для встановлення швидших з’єднань зі зменшеною затримкою. Його інноваційні функції, включаючи мультиплексування без блокування початку черги, пряму корекцію помилок та покращений контроль перевантаження, роблять QUIC особливо придатним для високопродуктивних застосунків із низькою затримкою. Ці атрибути є важливими для вебсервісів та сервісів реального часу, де швидкість та стійкість мають першорядне значення.

Інтеграція SMB понад QUIC у Windows Server 2025 поєднує багатофункціональне середовище SMB з можливостями високошвидкісного з’єднання QUIC з низькою затримкою, що дозволяє здійснювати швидшу та стійкішу передачу даних навіть у менш надійних мережевих умовах. Це особливо корисно для віддалених або мобільних користувачів, які часто стикаються з коливаннями якості мережі.

З погляду безпеки, SMB посилює захист даних, використовуючи вбудоване шифрування QUIC, що забезпечує безпечну передачу даних за замовчуванням. Ця надійна структура безпеки зміцнює заходи захисту SMB, оберігаючи чутливі дані від несанкціонованого доступу.

Процес безпечного обміну файлами через Інтернет без необхідності використання VPN починається з рукостискання TCP, що встановлює надійне з'єднання між клієнтом і сервером. За цим слідує рукостискання TLS для узгодження протоколів шифрування. Після встановлення зашифрованого каналу передача даних відбувається з використанням SMB, що забезпечує ефективний та безпечний обмін файлами. Цей процес виграє від низької затримки, швидшого встановлення з'єднання та покращеного відновлення після помилок. На рисунку 12.1 порівнюється час повного обороту (RTT), необхідний для встановлення з'єднань та передачі даних між клієнтами та серверами з використанням різних протоколів: TCP+TLS1.2, TCP+TLS1.3 та SMB з QUIC. Це підкреслює, що SMB значно зменшує затримку, вимагаючи менше RTT порівняно з іншими протоколами, що робить його ефективнішим для швидшої та надійнішої передачі даних.

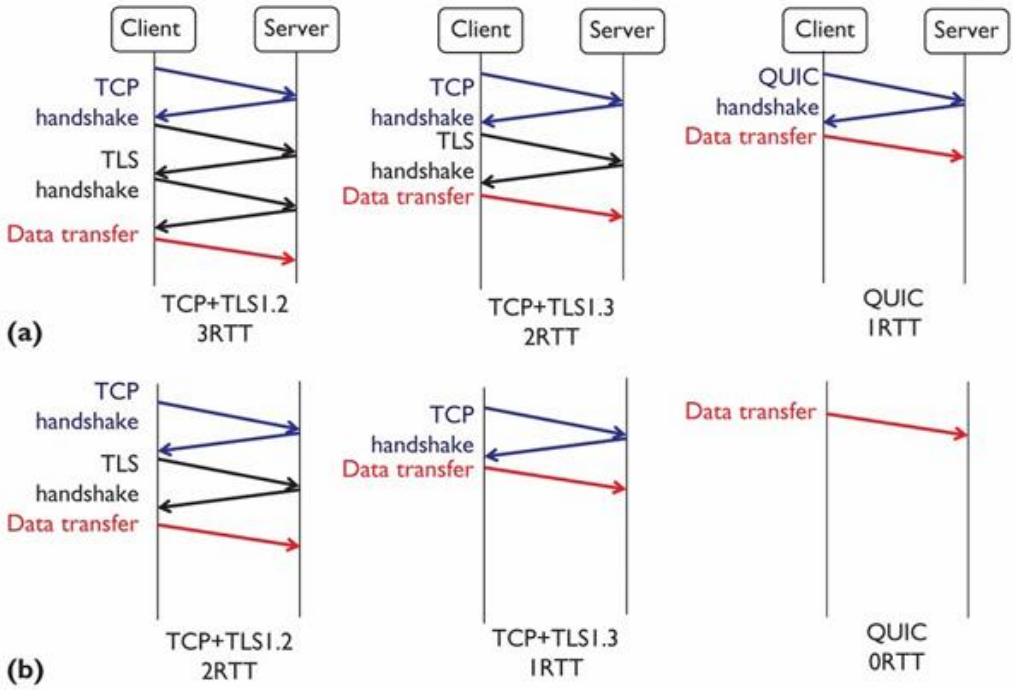

Рисунок 12.1 – Обмін файлами через Інтернет без VPN з використанням SMB з QUIC [3]

Адміністратори також виявлять, що розгортання SMB з QUIC у Windows Server 2025 є зручним для користувача. Процес інтеграції було спрощено, мінімізуючи час простою та перебої в роботі. Завдяки знайомим інструментам управління та інтерфейсам, IT-команди можуть легко налаштовувати та підтримувати SMB та QUIC, забезпечуючи плавний перехід без необхідності значного перенавчання. Загалом, інтеграція SMB та QUIC у Windows Server

2025 пропонує динамічне рішення, яке підвищує швидкість передачі даних, покращує надійність мережі та посилює безпеку. Ця комбінація оснащує IT-фахівців передовими інструментами, необхідними для вирішення викликів сучасного цифрового ландшафту, сприяючи більшій ефективності та захисту корпоративних мереж. При реалізації SMB з QUIC необхідно переконатися, що як клієнтське, так і серверне середовище підтримують протокол QUIC. Крім того, слід забезпечити правильну конфігурацію портів брандмауера для дозволу трафіку QUIC, оскільки це може суттєво вплинути на з'єднання та продуктивність.

Інтеграція SMB та QUIC у Windows Server 2025 базується на багатій історії обох протоколів, кожен з яких еволюціонував для задоволення мінливих вимог цифрової комунікації та корпоративних мереж. Компанія IBM вперше представила SMB у середині 1980-х років як протокол, призначений для полегшення спільного використання файлів та принтерів у локальних мережах (LAN). З часом SMB постійно вдосконалювався, включаючи такі значні покращення, як підтримка Unicode, здатність обробляти файли великого розміру та вдосконалені механізми контролю доступу. Ці вдосконалення зробили SMB надійним, безпечним та важливим інструментом для доступу до мережевих ресурсів та обміну даними в корпоративних середовищах.

Розглядаючи хронологію розвитку SMB, можна виділити ключові етапи. У 1983 році Баррі Фейгенбаум в IBM розробив SMB 1.0, який працював поверх кадрів NetBIOS і підтримувався Microsoft для LAN Manager. У 1990 році Microsoft інтегрувала SMB 1.0 у LAN Manager для OS/2. У 1992 році SMB 1.0 продовжив еволюцію з Windows for Workgroups, яка спочатку використовувала недосконалу автентифікацію на основі DES. У 1996 році протокол було перейменовано на Common Internet File System (CIFS), додано такі функції, як символічні/жорсткі посилання, підтримку великих файлів та експериментальний TCP. У 2006 році з виходом Windows Vista та Windows Server 2008 було представлено SMB 2.0, що додало підтримку конвеєрної обробки і стійких файлових дескрипторів. Версія SMB 2.1 з'явилася у 2009 році з Windows 7 та Server 2008 R2, додавши покращення блокування [4].

Значний крок вперед відбувся у 2012 році з випуском SMB 3.0 у Windows 8 та Server 2012, де було додано SMB Direct, SMB Multichannel, Transparent Failover та шифрування AES. У 2013 році Microsoft оголосила SMB 1.0 застарілим через проблеми з безпекою та продуктивністю, а також представила SMB 3.0.2 у Windows 8.1 та Server 2012 R2 з покращеною безпекою. Нарешті, у 2016 році з Windows 10 та Server 2016 з'явився SMB 3.1.1, що додав шифрування AES-128 GCM та перевірку цілісності попередньої автентифікації за допомогою SHA-512 [4].

Паралельно з цим, QUIC виник як новаторський протокол, розроблений Google у 2013 році. Створений для подолання обмежень традиційного TCP, QUIC використовує UDP для зменшення затримки та прискорення часу з'єднання, що робить його ідеальним для високих

вимог до продуктивності сучасних вебзастосунків. QUIC був розроблений для мінімізації буферизації, покращення ефективності потоку даних та посилення безпеки за допомогою вбудованого шифрування. Його офіційна стандартизація Інженерною групою Інтернету (IETF) у 2021 році ще більше закріпила його роль як ключової інновації.

Історія впровадження QUIC демонструє стрімку динаміку. У 2012 році код QUIC було експериментально розроблено в Google Chrome. У серпні 2013 року про QUIC було оголошено як частину релізу Chromium 29. У липні 2016 року підтримку розпочала Akamai Technologies. У липні 2017 року LiteSpeed Technologies офіційно підтримала QUIC у своїх продуктах. У вересні 2019 року cURL 7.66 додав підтримку HTTP/3 та QUIC. Станом на жовтень 2019 року 88,6% вебсайтів з QUIC використовували LiteSpeed, а 10,8% – Nginx [3].

У квітні 2020 року Apple додала експериментальну підтримку в Safari Technology Preview 104. У жовтні 2020 року Facebook перевів 75% свого інтернет-трафіку на QUIC. У березні 2021 року QUIC використовували 5% усіх вебсайтів, а в травні того ж року підтримку додав Firefox. У березні 2022 року експериментальну підтримку додав HAProxy, а у 2022 році Microsoft Windows Server 2022 отримав підтримку HTTP/3 та SMB над QUIC через MsQuic. У березні 2023 року HAProxy оголосив про готовність підтримки QUIC, і до квітня 2023 року частка вебсайтів, що використовують QUIC, досягла 8,9% [3].

Конвергенція SMB та QUIC у Windows Server 2025 представляє собою стратегічне узгодження їхніх сильних сторін, що відповідає на постійно зростаючу потребу у швидкості, безпеці та стійкості мережі. Розуміння історичної еволюції SMB та QUIC має вирішальне значення для забезпечення зворотної сумісності. Перед оновленням слід переконатися, що застарілі системи обробляються належним чином для запобігання проблемам сумісності.

Впровадження SMB у Windows Server 2025 пропонує унікальний набір переваг, що задовольняють динамічні потреби сучасних підприємств. Найбільш переконливою перевагою є значне підвищення швидкості передачі даних, яке стало можливим завдяки використанню протоколом QUIC протоколу UDP для швидшого встановлення з’єднань та меншої затримки. Це призводить до швидкої та ефективної передачі файлів, що особливо корисно для сценаріїв, які включають великі обсяги даних або доступ у реальному часі. Другою важливою перевагою є посилена безпека, оскільки вбудоване шифрування QUIC у поєднанні з усталеними функціями безпеки SMB формує надійний захист від несанкціонованого доступу та порушень. Усі дані, що передаються через SMB та QUIC, автоматично шифруються, забезпечуючи надійний захист чутливої корпоративної інформації. Третім аспектом є покращена надійність мережі, адже завдяки таким функціям, як мультиплексування та вдосконалений контроль перевантаження, QUIC ефективно працює в нестабільних мережах і забезпечує плавну передачу даних навіть у складних умовах, що є цінним для мобільних користувачів. Четвертою перевагою є покращений користувацький

досвід, оскільки функції на кшталт прямої корекції помилок та зменшеного блокування початку черги мінімізують буферизацію та оптимізують потік даних. П’ятим фактором є простота розгортання, бо спрощений процес інтеграції мінімізує час простою, дозволяючи адміністраторам швидко налаштовувати систему за допомогою знайомих інструментів. Для максимізації цих переваг необхідно переконатися, що мережева інфраструктура та обладнання оптимізовані для використання можливостей зменшеної затримки та покращених функцій безпеки, властивих протоколу QUIC [3].

Підвищення продуктивності SMB з QUIC є вирішальним для IT-фахівців, які прагнуть максимізувати ефективність та надійність своїх мережевих систем. Оскільки організації все частіше приймають цей передовий протокол комунікації, важливо тонко налаштувати різні аспекти розгортання для досягнення пікової продуктивності. Для цього необхідно застосовувати ретельний підхід до конфігурації мережі.

Процес починається із забезпечення того, що мережева інфраструктура є достатньо надійною для підтримки високошвидкісної передачі даних. Це включає оновлення мережевого обладнання, такого як маршрутизатори та комутатори, до останніх стандартів та перевірку того, що мережеві інтерфейси можуть обробляти гігабітні або вищі швидкості.

Належна конфігурація налаштувань якості обслуговування дозволяє пріоритезувати трафік SMB разом з QUIC над іншими типами трафіку, зменшуючи затримку. Мінімальною вимогою для впровадження є забезпечення підтримки протоколів на основі UDP, а також сумісність ОС (Windows Server 2022 або 2025) та застосунків із QUIC. Оптимізація налаштувань TCP, зокрема розмірів вікон та включення розвантаження TCP, може значно підвищити пропускну здатність. Також слід застосовувати сегментацію мережі, щоб ізолювати трафік SMB з QUIC від інших типів трафіку, як показано на рисунку 12.2, захищаючи його від перешкод.

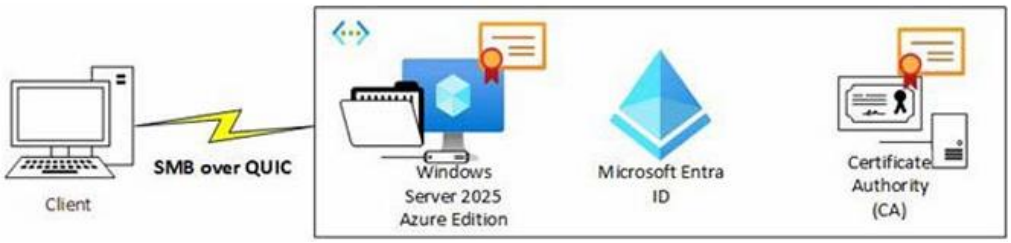

Рисунок 12.2 – Розкриття всіх даних у файлах Azure через SMB over QUIC [3]

Додатково слід увімкнути та налаштувати явне повідомлення про перевантаження (ECN), що допомагає зменшити втрату пакетів, дозволяючи мережі сигналізувати про перевантаження без відкидання пакетів. Використання сучасних рішень для балансування навантаження може рівномірно розподілити навантаження між серверами, запобігаючи вузьким місцям. Включення стратегій резервування та відмовостійкості, таких як

впровадження кількох мережевих шляхів та систем резервного копіювання, забезпечує безперервну доступність. Регулярний моніторинг та налаштування продуктивності є важливими для адаптації до змінних умов. Необхідно переконатися, що мережу налаштовано з належними параметрами якості, оскільки нехтування цим може призвести до затримок.

Оптимізація продуктивності також вимагає ретельної оцінки апаратних компонентів. Критичним кроком є оновлення мережевих інтерфейсів (NIC) для підтримки гігабітних швидкостей та використання карток із можливостями розвантаження (наприклад, TCP Offload Engine), що зменшує навантаження на процесор. Високопродуктивні маршрутизатори та комутатори гарантують ефективне керування потоком даних. У підсистемах зберігання заміна HDD на SSD (особливо NVMe) забезпечує значні покращення швидкості доступу та IOPS.

Сервери повинні бути оснащені багатоядерними процесорами та достатнім обсягом оперативної пам’яті для обробки шифрування QUIC. Системи резервного живлення та ефективне охолодження є життєво важливими для запобігання простоям та перегріву. Регулярне оновлення прошивки та драйверів є обов’язковим для підтримки сумісності та пікової потужності обладнання.

Налаштування та моніторинг продуктивності є невіддільною частиною процесу. IT-фахівці повинні використовувати інструменти моніторингу, такі як Системний монітор Microsoft (Performance Monitor), Wireshark та SolarWinds NPM, для отримання інсайтів у реальному часі щодо трафіку та затримок (рис. 12.3). Постійне налаштування параметрів TCP (розмірів вікон, ECN) та оптимізація забезпечують плавний потік даних. Регулярні аудити продуктивності, включаючи стрес-тестування, дозволяють оцінити масштабованість. Автоматизовані системи сповіщення допомагають оперативно реагувати на відхилення від порогових значень. Безперервна освіта персоналу гарантує готовність до нових викликів.

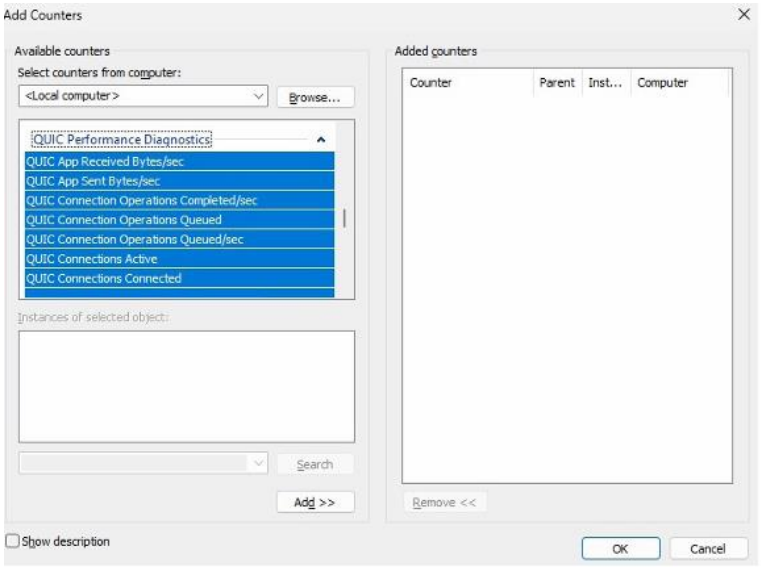

Рисунок 12.3 – Лічильники QUIC у Системному моніторі [3]

Впровадження SMB з QUIC у Windows Server 2025 передбачає навігацію через ряд складних технічних викликів, і ефективне усунення несправностей є вирішальним для підтримки надійності. IT-фахівці часто стикаються з конкретними проблемами, які потребують діагностики.

Однією з найпоширеніших проблем є нестабільність з'єднання, що проявляється спорадичними втратами зв'язку або частими відключеннями. Це часто виникає через неправильні конфігурації мережі або несумісність обладнання, тому важливо перевіряти сумісність пристроїв зі стандартами QUIC.

Другою проблемою є погіршення продуктивності, викликане неадекватними налаштуваннями мережі, недостатньою смугою пропускання або перевантаженим обладнанням. Вирішенням є моніторинг трафіку та оновлення прошивки компонентів.

Третім викликом є проблеми безпеки, такі як ризики несанкціонованого доступу або збої шифрування. Для їх зменшення необхідно впроваджувати надійні протоколи шифрування та проводити аудити.

Четвертою проблемою є затримка та висока втрата пакетів, що можуть бути результатом перевантаження мережі або неправильних параметрів TCP. Використання інструментів моніторингу та тонке налаштування параметрів (ECN, розмір вікон) покращує потік даних.

П'ятим аспектом є проблеми сумісності між різними версіями програмного забезпечення або пристроями, що вимагає забезпечення регулярного оновлення всіх компонентів інфраструктури. Систематичне усунення несправностей дозволяє організаціям досягти стабільної роботи SMB з QUIC.

Вирішення проблем, що виникають під час впровадження SMB з QUIC у Windows Server 2025, вимагає комплексного та індивідуального підходу. Нестабільність з'єднання, яка часто спричинена неправильною конфігурацією мережі або несумісністю обладнання, може бути усунена шляхом забезпечення оновлення всіх мережевих пристроїв для підтримки останніх стандартів протоколу QUIC. Це передбачає перевірку наявності оновлень мікропрограмного забезпечення та драйверів на маршрутизаторах, комутаторах та мережевих інтерфейсних платах (NIC). Проведення ретельних аудитів конфігурації допоможе виявити та виправити будь-які невідповідності. Для вирішення проблем затримок та високої втрати пакетів, які можуть суттєво погіршити ефективність передачі даних, необхідне розгортання передових інструментів моніторингу мережі. Інструменти, такі як SolarWinds Network Performance Monitor та Wireshark, пропонують інсайти в реальному часі щодо патернів трафіку та точок перевантаження. Тонке налаштування параметрів TCP, зокрема коригування розмірів вікон та увімкнення ECN, може значно покращити потік даних та зменшити затримки [3].

Особливої уваги потребують питання безпеки, особливо в середовищах із суворими вимогами до захисту даних. IT-фахівцям слід впроваджувати надійні протоколи шифрування, такі як AES-256, що проілюстровано на рисунку 12.4, для захисту даних під час передачі. Регулярні аудити безпеки та перевірки на відповідність стандартам є важливими для виявлення та усунення вразливостей. Застосування суворого контролю доступу та багатофакторної автентифікації може додатково захистити від несанкціонованого доступу та підвищити безпеку розгортання SMB з QUIC. Погіршення продуктивності, часто спричинене субоптимальними налаштуваннями мережі або недостатніми апаратними ресурсами, керується шляхом регулярного моніторингу та оптимізації. IT-команди повинні часто переглядати та коригувати налаштування для забезпечення достатньої смуги пропускання для трафіку SMB та QUIC. Оновлення апаратних компонентів, включаючи NIC, маршрутизатори та комутатори, для підтримки вищих швидкостей та розширених можливостей розвантаження може допомогти усунути вузькі місця. Крім того, забезпечення серверів багатоядерними процесорами та достатнім обсягом пам’яті сприятиме обробці обчислювальних вимог процесів шифрування та дешифрування.

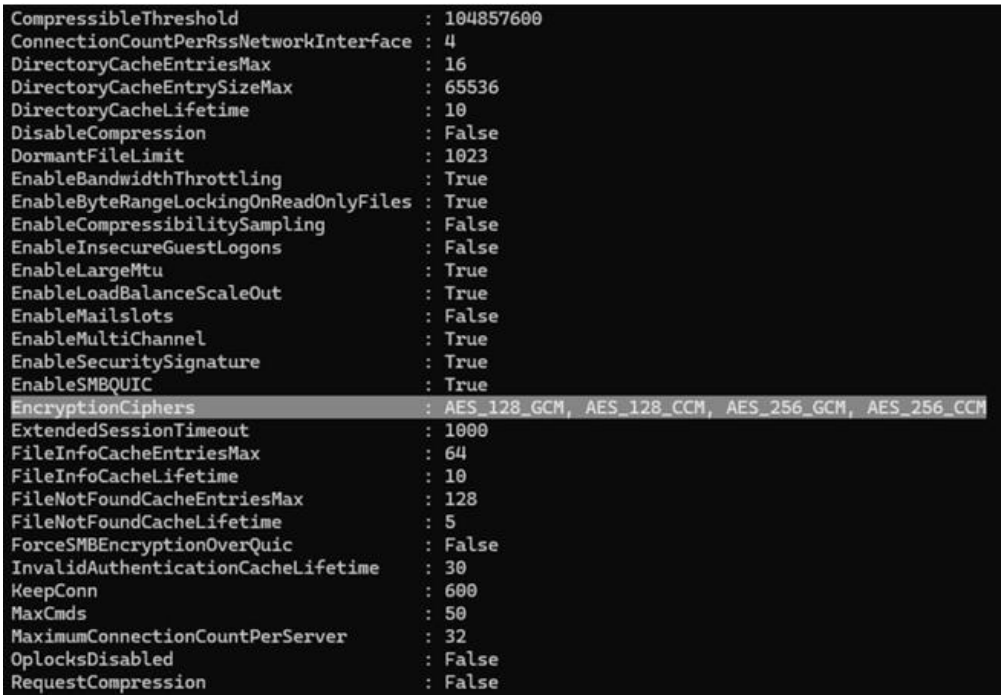

Рисунок 12.4 – Шифри шифрування AES [3]

Проблеми сумісності між різними версіями програмного забезпечення або мережевими пристроями можуть перешкоджати розгортанню SMB разом з QUIC. Важливо підтримувати оновлений інвентар компонентів мережевої інфраструктури та забезпечувати сумісність з останніми оновленнями програмного забезпечення. Програми безперервної освіти та сертифікації для IT-персоналу нададуть їм знання та навички, необхідні для ефективного управління цими викликами. Проактивний та систематичний підхід до

налаштування та моніторингу продуктивності є важливим для оптимізації SMB та QUIC [3].

Необхідно використовувати передові інструменти для аналізу метрик продуктивності мережі, виявлення вузьких місць та впровадження коригувальних заходів. Регулярні аудити продуктивності, включаючи стрес-тестування в умовах пікового навантаження, допоможуть оцінити стійкість та масштабованість інфраструктури. Шляхом імітації сценаріїв із високим трафіком потенційні проблеми можна виявити та усунути до того, як вони вплинуть на кінцевих користувачів. Інтегруючи детальний аналіз продуктивності, ітеративне налаштування, регулярні аудити та постійний професійний розвиток, IT-фахівці можуть ефективно усувати несправності та оптимізувати реалізації SMB з QUIC. Цей комплексний підхід забезпечує високопродуктивне, стійке та надійне мережеве середовище, що відповідає вимогам сучасної цифрової інфраструктури. При застосуванні виправлень для вирішення проблем SMB та QUIC слід переконатися, що будь-які зміни, внесені до мережевих конфігурацій або конфігурацій безпеки, ретельно протестовані в контрольованому середовищі перед застосуванням їх у виробничій мережі. Це запобігає ненавмисним перебоям у наданні послуг.

Проактивний розподіл ресурсів шляхом виділення достатньої смуги пропускання для трафіку SMB з QUIC через політики QoS, допомагає запобігти перевантаженню та гарантує належну пріоритезацію потоків даних. Регулярний перегляд та коригування цих політик на основі фактичних патернів використання мережі дозволяє динамічно адаптуватися до змінних вимог, підтримуючи таким чином оптимальну продуктивність. Надійні заходи безпеки, такі як використання сильних протоколів шифрування (AES-256) у поєднанні з багатофакторною автентифікацією (MFA), посилюють захист від несанкціонованого доступу та витоків даних. Проведення регулярних аудитів безпеки та оцінок вразливостей допомагає виявляти та усувати потенційні загрози. Крім того, впровадження суворого контролю доступу та сегментації мережі додатково знижує ризик порушень безпеки шляхом мінімізації поверхні атаки [3].

SMB з QUIC пропонує значні переваги в покращенні продуктивності мережі та безпеки, особливо в середовищах із віддаленою роботою або інтеграцією гібридних хмар. Однак його застосовність може варіюватися залежно від розміру та складності мережі. SMB з QUIC є вдосконаленням традиційного протоколу SMB, що використовує QUIC для покращення продуктивності мережі та безпеки. Використовуючи UDP, QUIC зменшує затримку та підвищує безпеку за допомогою наскрізного шифрування, що робить його ідеальним для сучасних гібридних та віддалених мережевих середовищ.

Варто зазначити, що впровадження SMB з QUIC, хоча й надає значні переваги, не є обов’язковим для кожного типу мережі. Воно є особливо корисним для організацій, які покладаються на безпечний, високопродуктивний обмін файлами через ненадійні мережі,

такі як віддалені офіси, гібридні середовища або хмарні системи. Для менших, виключно внутрішніх мереж, де проблеми безпеки та продуктивності є мінімальними, традиційного SMB (через TCP/IP) може бути достатньо.

Розглядати впровадження SMB з QUIC доцільно у випадках, коли мережа працює у віддалених або гібридних середовищах з підвищеними потребами у безпеці, або коли є необхідність у передачі чутливих даних через публічні або ненадійні мережі. Також це рішення є актуальним для оптимізації продуктивності, зменшення затримок та забезпечення більш надійного доступу до файлів через VPN або подібні віддалені налаштування, а також при впровадженні хмарних застосунків, що вимагають безпечного доступу до даних.

Специфічні умови, за яких SMB з QUIC стає необхідним, включають гібридні та віддалені робочі середовища, інтеграцію з хмарою, а також погані мережеві умови з високою затримкою, де протокол на базі UDP забезпечує надійнішу роботу, ніж традиційний SMB на базі TCP. Найбільшу вигоду від цієї технології зазвичай отримують великі підприємства та організації зі значними вимогами до віддаленого доступу або багатоофісною структурою, проте зростаючі малі підприємства також можуть скористатися перевагами підвищеної безпеки.

Порівнюючи з традиційним SMB, який покладається на TCP і може вносити вищі затримки, SMB з QUIC використовує UDP для швидшої передачі даних з меншою затримкою, що робить його більш придатним для сучасних сценаріїв мережевої взаємодії. Це забезпечує вбудовану безпеку з шифруванням та покращену надійність у різних мережевих умовах.

Інтеграція протоколу SMB у середовище Linux, зокрема в дистрибутивах класу Enterprise, таких як Ubuntu Server, реалізується переважно за допомогою програмного пакету Samba. Цей набір інструментів з відкритим вихідним кодом забезпечує безшовну взаємодію між Unix-подібними системами та мережами Windows, виступаючи як у ролі контролера домену, так і в ролі звичайного файлового сервера або клієнта. Samba базується на зворотній розробці протоколу SMB/CIFS і дозволяє серверам Linux виглядати для Windows-клієнтів як рідні вузли мережі. Завдяки цьому системні адміністратори можуть розгортати гетерогенні мережеві інфраструктури, де сервери Ubuntu забезпечують надійне зберігання даних, використовуючи стабільність файлових систем Linux (наприклад, EXT4, XFS або ZFS), водночас надаючи доступ користувачам через звичний протокол SMB [3].

Проект SAMBA, його призначення та основні можливості

Проект Samba являє собою реалізацію мережевого протоколу SMB/CIFS, яка забезпечує безшовну інтеграцію Unix-подібних операційних систем, таких як Linux, Solaris, AIX та BSD, у мережеве середовище Microsoft Windows. Розроблений на принципах зворотної інженерії, цей програмний комплекс виступає головним компонентом для побудови

гетерогенних інформаційних систем, дозволяючи серверам на базі вільного програмного забезпечення взаємодіяти з пропрієтарними клієнтами та серверами на рівному рівні.

Призначення Samba виходить далеко за межі простого файлового сервера. Це потужна інфраструктурна платформа, що здатна виконувати ролі контролера домену Active Directory, сервера друку, а також члена домену для аутентифікації та авторизації користувачів. Важливою характеристикою проекту є його відповідність стандартам, що дозволяє емулювати поведінку Windows NT, 2000, 2003 і новіших версій, забезпечуючи при цьому стабільність та гнучкість, властиві Unix-системам [42].

Архітектурно Samba побудована за модульним принципом, де ключову роль відіграють спеціалізовані служби, кожна з яких відповідає за певний аспект мережевої взаємодії. Основним компонентом є служба smbd, яка безпосередньо обробляє запити на доступ до файлової системи та принтерів, керує сесіями користувачів та забезпечує перевірку прав доступу. Паралельно функціонує служба nmbd, яка реалізує протокол NetBIOS понад TCP/IP, відповідаючи за перетворення імен NetBIOS у IP-адреси та участь у процесах вибору майстер-браузера мережі.

У сучасних конфігураціях, особливо при інтеграції з Active Directory, критично важливу роль відіграє служба winbindd. Її завдання полягає у вирішенні проблеми ідентифікації користувачів шляхом трансляції ідентифікаторів безпеки Windows (SID) у зрозумілі для Unix ідентифікатори користувачів (UID) та груп (GID), що дозволяє системі прозоро оперувати обліковими записами, створеними на контролерах домену Windows.

Однією з найбільш значущих можливостей Samba, починаючи з версії 4.0, є здатність функціонувати як повноцінний контролер домену Active Directory (AD DC). Ця функціональність реалізується завдяки вбудованому LDAP-серверу та центру розподілу ключів Kerberos (KDC), які повністю сумісні з протоколами Microsoft. Це дозволяє адміністраторам розгортати доменну структуру без використання ліцензійного програмного забезпечення Windows Server, підтримуючи при цьому групові політики, реплікацію каталогів з іншими контролерами домену та управління через стандартні засоби адміністрування Windows (RSAT). Інтеграція DNS-сервера (вбудованого або через BIND_DLZ) забезпечує необхідну інфраструктуру для динамічного оновлення записів, що є обов’язковою умовою функціонування Active Directory [42].

У контексті файлового обслуговування Samba надає розширені можливості через підсистему віртуальної файлової системи (VFS). Модульна архітектура VFS дозволяє перехоплювати системні виклики перед тим, як вони досягнуть реальної файлової системи сервера, і виконувати над ними додаткові операції. Це відкриває шлях до реалізації таких функцій, як «тіньові копії», що інтегруються з механізмами знімків файлових систем (наприклад, ZFS або LVM), мережевий кошик для відновлення видалених файлів, а також

аудит доступу до даних на рівні окремих операцій. Використання модулів VFS також дозволяє адаптувати поведінку сервера до специфічних вимог, наприклад, для забезпечення сумісності з Time Machine від Apple або для реалізації перевірки файлів на віруси в реальному часі при записі на диск. Така гнучкість дозволяє перетворити стандартний файловий сервер на складне рішення для управління даними з розширеною функціональністю.

Безпека в Samba реалізується на декількох рівнях, починаючи від шифрування транспортного каналу і закінчуючи гранулярним контролем доступу. Проект підтримує сучасні протоколи аутентифікації, включаючи Kerberos та NTLMv2, відмовляючись від застарілих та вразливих методів, таких як LANMAN, за замовчуванням. Інтеграція з підсистемою PAM (Pluggable Authentication Modules) операційної системи дозволяє уніфікувати процеси входу в систему [42].

Важливим аспектом є можливість шифрування трафіку SMB 3.x, що забезпечує захист конфіденційних даних від перехоплення в ненадійних мережах без необхідності використання VPN. Крім того, Samba надає інструменти для управління списками контролю доступу (ACL), дозволяючи відображати складні схеми прав доступу Windows NT ACL на POSIX ACL або розширені атрибути файлової системи Linux, забезпечуючи точне дотримання політик безпеки.

Особливе місце в проєкті Samba займає можливість кластеризації за допомогою CTDB (Clustered Trivial Database). Цей компонент дозволяє об’єднувати декілька фізичних серверів у єдиний високодоступний кластер, що надає спільний доступ до файлів. CTDB забезпечує розподіл метаданих та управління блокуваннями файлів між вузлами кластера, що дозволяє клієнтам підключатися до будь-якого вузла та продовжувати роботу навіть у разі виходу з ладу одного з серверів. Така архітектура є критично важливою для корпоративних середовищ з високими вимогами до доступності сервісів та масштабованості. Використання кластерних файлових систем, таких як GPFS, GlusterFS або CephFS, у поєднанні з Samba та CTDB, дозволяє створювати рішення для зберігання петабайтних обсягів даних з високою пропускною здатністю.

Крім файлових сервісів, Samba забезпечує потужну підтримку служб друку, виступаючи посередником між клієнтами Windows та підсистемою друку Unix (зазвичай CUPS). Використовуючи механізм SPOOLSS, сервер Samba може автоматично надавати драйвери принтерів для клієнтських машин (функція Point’n’Print), що значно спрощує адміністрування парку друкуючої техніки. Сервер приймає завдання на друк у форматі RPC, перетворює їх та передає локальному спулеру, забезпечуючи при цьому контроль доступу та облік використання ресурсів. Це дозволяє централізувати управління друком у гетерогенній мережі, використовуючи надійність та масштабованість Linux-серверів для обробки великої

кількості завдань [42].

Для управління та діагностики проект Samba пропонує широкий набір утиліт командного рядка, які дозволяють адміністраторам взаємодіяти з сервером та клієнтськими машинами. Інструменти на кшталт smbclient надають FTP-подібний інтерфейс для доступу до ресурсів, rpcclient дозволяє виконувати віддалені виклики процедур для адміністрування Windows-машин, а команда net є потужним аналогом однойменної утиліти Windows для управління доменом, обліковими записами та сесіями. Завдяки наявності бібліотеки libsmbclient, функціональність Samba може бути інтегрована у сторонні додатки, файлові менеджери та медіа-центри, розширюючи сферу застосування протоколу SMB на різноманітні пристрої та платформи.

Особливості налаштування Samba-серверу на Ubuntu

Практична реалізація файлового обміну в мережах, де сервери під управлінням Ubuntu Linux взаємодіють із клієнтськими станціями Windows, найчастіше базується на використанні проєкту Samba.

Налаштування Samba як файлового сервера є стандартною процедурою для забезпечення прозорого доступу до даних. У цьому контексті розглядається конфігурація сервера для обміну файлами з будь-яким клієнтом у мережі без необхідності проходження процедури автентифікації за паролем, що є типовим сценарієм для публічних файлових ресурсів або внутрішніх мереж довіри. Проте, якщо архітектура інформаційної системи вимагає суворішого контролю доступу та розмежування прав користувачів, адміністратору необхідно буде застосувати додаткові механізми безпеки, які виходять за межі базової конфігурації.

Початковим етапом розгортання сервісу є інсталяція необхідного програмного забезпечення. У середовищі Ubuntu Server це виконується за допомогою менеджера пакетів APT. Перший крок передбачає встановлення пакету Samba, що містить необхідні бінарні файли серверної частини, утиліти конфігурації та документацію. У термінальному інтерфейсі це реалізується шляхом введення команди sudo apt install samba. Після успішного завершення інсталяції система готова до налаштування параметрів спільного використання файлів, а відповідні служби автоматично реєструються в системі ініціалізації.

Важливо відзначити, що коректність роботи Samba залежить від узгодженості ідентифікаторів користувачів та груп у системі. Зокрема, якщо в інфраструктурі одночасно використовуються Samba та authd, виникає необхідність явного вказання зіставлення користувачів та груп (ID mapping). Ігнорування цієї вимоги призведе до конфліктів дозволів через невідповідність числових ідентифікаторів UID/GID, тому при спільній роботі з authd слід суворо дотримуватися інструкцій, викладених у відповідній документації.

Основним інструментом адміністрування сервісу Samba є файл конфігурації /etc/samba/smb.conf. Цей файл має структуру, подібну до INI-файлів Windows, і за замовчуванням містить значну кількість коментарів, які документують призначення різних директив. Файл конфігурації за замовчуванням не охоплює всі можливі опції, повний перелік яких доступний у сторінці довідки man smb.conf або в офіційній документації Samba HOWTO [42].

Процес налаштування розпочинається з редагування секції «global», яка визначає загальні параметри поведінки сервера. Ключовим параметром тут є workgroup, який забезпечує логічне групування комп'ютерів у мережевому оточенні. Значення цього параметра має бути змінено так, щоб воно відповідало робочій групі або домену, що використовується в конкретному середовищі, наприклад: workgroup = EXAMPLE. Це забезпечує видимість сервера для Windows-клієнтів під час перегляду мережі [42].

Наступним кроком є визначення безпосередніх ресурсів спільного доступу. Для цього в кінці файлу конфігурації створюється новий розділ або розкоментується один із наявних прикладів. Назва розділу в квадратних дужках, наприклад [share], визначатиме ім'я, під яким ресурс буде відображатися для мережевих клієнтів.

Усередині секції задаються параметри, що регулюють доступ та властивості ресурсу. Параметр comment використовується для надання короткого опису ресурсу, наприклад «Ubuntu File Server Share», що полегшує ідентифікацію призначення папки користувачами. Параметр path є важливим, оскільки він вказує абсолютний шлях до каталогу у локальній файловій системі Linux, до якого надається спільний доступ, наприклад /srv/samba/share.

Вибір шляху до каталогу має базуватися на загальноприйнятих стандартах. Наприклад, використовується шлях /srv/samba/share, оскільки, згідно зі Стандартом ієрархії файлової системи (Filesystem Hierarchy Standard – FHS), каталог /srv призначений саме для даних, які обслуговуються системою для зовнішніх клієнтів. Хоча технічно спільні ресурси Samba можна розміщувати в будь-якому місці файлової системи за умови наявності відповідних дозволів, дотримання стандартів FHS спрощує адміністрування та структурування даних. Для забезпечення видимості ресурсу у провіднику Windows використовується директива browsable = yes. Це дозволяє клієнтам виявляти папку автоматично при перегляді списку ресурсів сервера [42].

Механізм доступу без пароля реалізується за допомогою директиви guest ok = yes. Ця опція дозволяє клієнтам підключатися до спільного ресурсу без надання облікових даних, що відповідає сценарію публічного обміну файлами. При цьому Samba автоматично зіставляє такі підключення з локальним гостьовим акаунтом (зазвичай nobody). Режим доступу до файлів (читання або запис) регулюється параметром read only. Якщо встановлено значення no, як у розглянутому прикладі, клієнтам надаються права на запис, зміну та видалення

файлів. Якщо ж значення дорівнює yes, доступ обмежується лише читанням. Додатково, для контролю прав доступу до новостворених файлів використовується директива create mask, наприклад 0755. Вона визначає бітову маску дозволів, які будуть автоматично присвоєні файлам, створеним клієнтами через мережу, забезпечуючи прогнозований рівень безпеки на рівні файлової системи Linux.

Після завершення редагування конфігураційного файлу необхідно підготувати файлову систему. Це передбачає створення відповідного каталогу та налаштування прав власності. У терміналі виконується команда sudo mkdir -p /srv/samba/share, де перемикач -p вказує утиліті mkdir на необхідність створення всього дерева каталогів, якщо батьківські директорії ще не існують. Оскільки доступ до ресурсу налаштовано для гостьових користувачів, права власності на каталог повинні бути передані користувачеві та групі, які використовуються Samba для гостьових сесій. Це виконується командою sudo chown nobody:nogroup /srv/samba/share/. Такий крок гарантує, що процес Samba, діючи від імені гостя, матиме достатні повноваження файлової системи для запису даних у цей каталог [42].

Фінальним етапом налаштування є застосування змін шляхом перезапуску служб. Для того щоб нова конфігурація набула чинності, адміністратор повинен перезапустити служби smbd та nmbd за допомогою системи ініціалізації. Виконання команди sudo systemctl restart smbd.service nmbd.service зупиняє поточні процеси та запускає їх знову з урахуванням оновленого файлу smb.conf. Необхідно ще раз наголосити на важливості розуміння наслідків обраної конфігурації, оскільки вищезазначені налаштування надають повний доступ на читання та запис будь-якому клієнту в локальній мережі.

Перевірка працездатності налаштованого сервера здійснюється з боку клієнтської машини Windows. Користувач повинен мати змогу перейти на файловий сервер Ubuntu через мережеве оточення та побачити спільний каталог. У випадках, коли механізми виявлення мережі (NetBIOS або WS-Discovery) не спрацьовують миттєво і клієнт не відображає спільний ресурс автоматично, рекомендується спробувати отримати доступ до сервера напряму за його IP-адресою. Введення шляху у форматі UNC, наприклад \\192.168.1.3, в адресному рядку Провідника Windows ініціює примусове з’єднання. Успішне створення нової папки або текстового файлу всередині відкритого ресурсу підтвердить коректність налаштування прав доступу на запис [42].

Масштабування файлового сервера для обслуговування додаткових задач здійснюється шляхом додавання нових секцій у файл конфігурації. Щоб створити додаткові спільні ресурси, адміністратор просто додає нові розділи у /etc/samba/smb.conf та перезапускає службу Samba.

При цьому критично важливо переконатися, що відповідний каталог у файловій системі дійсно існує, а права доступу Linux дозволяють операції читання та запису для

цільових користувачів Samba. Рекомендується дотримуватися логічного іменування, називаючи спільний ресурс відповідно до імені каталогу у файловій системі, наприклад, створення ресурсу [qa] для шляху /srv/samba/qa, що спрощує навігацію та адміністрування системи в майбутньому [42].

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

Базова

1. Комп’ютерні мережі. Книга 1: навчальний посібник / Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Львів: «Магнолія 2006», 2023. 256 с.
2. Комп’ютерні мережі. Книга 2: навчальний посібник / Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Львів: «Магнолія 2006», 2023. 312 с.
3. Dauti B. Windows Server 2025 Administration Fundamentals: A beginner’s guide to managing and administering Windows Server environments: Fourth Edition. Birmingham : Packt Publishing, 2025. 634 p.
4. Morimoto, R., Noel, M., Yardeni, G., Droubi, O., Abbate, A., & Amaris, C. Windows Server 2012 Unleashed. Indianapolis : Pearson Education. URL: https://api.pageplace.de/preview/DT0400.9780133115970_A23602136/preview-9780133115970_A23602136.pdf (дата звернення: 05.04.2025).

Допоміжна

1. Introduction To Subnetting - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/computer-networks/introduction-to-subnetting/ (дата звернення: 05.05.2025).
2. Subnetting: Brushing up on the fundamentals. Network World. URL: https://www.networkworld.com/article/969792/subnetting-brushing-up-on-the-fundamentals.html (дата звернення: 06.05.2025).
3. IPv4 Subnet Cheat Sheet. StationX. URL: https://www.stationx.net/ipv4-subnet-cheat-sheet/ (дата звернення: 05.05.2025).
4. A complete beginner's guide to subnetting. network fun-times. URL: https://www.networkfuntimes.com/a-complete-beginners-guide-to-subnetting/ (дата звернення: 09.05.2025).
5. Windows Server 2019 Beginners Video Tutorials. URL: http://surl.li/mkrxs (дата звернення: 10.05.2025).
6. CodeUA. Курс Основи адміністрування Windows Server Огляд серверних операційних систем (ОС), 2023. YouTube. URL: https://www.youtube.com/watch?v=JA2Gjz9Sibg (дата звернення: 10.05.2025).
7. CodeUA. Курс Основи адміністрування Windows Server Базові інструменти адміністрування ОС, 2023. YouTube. URL: https://www.youtube.com/watch?v=rWLgcbixkF8 (дата звернення: 12.05.2025).
8. Огляд Microsoft Windows Server 2025. URL: https://softlist.com.ua/ua/news/oglyad-microsoft-windows-server (дата звернення: 12.05.2025).
9. Операційна система Windows Server. Microsoft. Чому варто вибрати Windows Server 2025? URL: https://www.microsoft.com/uk-ua/windows-server (дата звернення: 12.05.2025).
10. Discover what’s new in Windows Server 2025. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/windows-server-2025-data-sheet.pdf (дата звернення: 12.05.2025).
11. Windows Server 2025 URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2025 (дата звернення: 12.05.2025).
12. What is Windows Server?. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/uk-ua/windows-server/get-started/overview (дата звернення: 12.05.2025).
13. Install Hyper-V in Windows and Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-hyper-v?utm_source=chatgpt.com&tabs=powershell&pivots=windows (дата звернення: 18.05.2025).
14. Create a virtual machine in Hyper-V. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-

started/create-a-virtual-machine-in-hyper-v?utm_source=chatgpt.com&tabs=hyper-v-manager (дата звернення: 18.05.2025).

15. What's new in Windows Server 2025. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-windows-server-2025 (дата звернення: 18.05.2025).

16. Hyper-V virtualization in Windows Server and Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/overview (дата звернення: 05.05.2025).

17. System Requirements for Hyper-V on Windows and Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/host-hardware-requirements&pivots=windows (дата звернення: 25.05.2025).

18. Windows Server 2025 | Microsoft Evaluation Center. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2025 (дата звернення: 25.05.2025).

19. Active Directory overview – Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/active-directory-overview (дата звернення: 25.05.2025).

20. Install Active Directory Domain Services on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100- (дата звернення: 25.05.2025).

21. Install Active Directory Domain Services on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100- (дата звернення: 28.05.2025).

22. Active Directory Domain Services overview. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата звернення: 28.05.2025).

23. Group Policy overview for Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview (дата звернення: 28.05.2025).

24. Group Policy preferences in Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-preferences (дата звернення: 05.05.2025).

25. Group Policy Management Console in Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-management-console (дата звернення: 28.05.2025).

26. The Admin's Guide to Group Policy Best Practices | Netwrix. Data Security that Starts with Identity| Netwrix. URL: https://netwrix.com/en/resources/guides/group-policy-best-practices/ (дата звернення: 02.06.2025).

27. Group Policy Management Guide. Active Directory Pro. URL: https://activedirectorypro.com/group-policy-guide/ (дата звернення: 02.06.2025).

28. Group Policies and Group Policies Preferences (2025). Hybrid Infrastructure and Cloud Architecture. URL: https://hartiga.de/windows-server/group-policies-foundation/ (дата звернення: 02.06.2025).

29. Install and Configure DNS Server on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/quickstart-install-configure-dns-server&tabs=powershell (дата звернення: 02.06.2025).

30. Manage DNS zones using DNS server in Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/manage-dns-zones&tabs=powershell (дата звернення: 02.06.2025).

31. What is DHCP Server in Windows Server?. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top (дата звернення: 02.06.2025).

32. Install and configure DHCP Server on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server?tabs=powershell (дата звернення: 06.06.2025).

33. Guidance for troubleshooting DHCP - Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/troubleshoot-dhcp-guidance (дата звернення: 06.06.2025).

34. Migrate existing DHCP failover deployment on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/migrate-existing-dhcp-failover?tabs=powershell (дата звернення: 06.06.2025).

35. Windows Server Security documentation. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/security/security-and-assurance (дата звернення: 06.06.2025).

36. Windows Server 2025: Install IIS Web Server - RDR-IT. RDR-IT. URL: https://rdr-it.com/en/windows-server-2025-install-iis-web-server/ (дата звернення: 02.06.2025).

37. Configuring IIS for Web Hosting on Windows: A Step-by-Step Guide. Kamatera. URL: https://www.kamatera.com/knowledgebase/configuring-iis-for-web-hosting-on-windows/ (дата звернення: 08.06.2025).

38. Ubuntu Server documentation. Ubuntu Server. URL: https://documentation.ubuntu.com/server/ (дата звернення: 08.06.2025).

39. Munna R. Linux DNS Server Configuration: Detailed Guide [2025]. MailServerGuru. URL: https://mailserverguru.com/linux-dns-server/#Master-Update-the-System (дата звернення: 08.06.2025).

40. Imron M. Guide to Creating a Simple Web Server Using Nginx and Apache2. Medium. URL: https://medium.com/@muhammadimron1410/guide-to-creating-a-simple-web-server-using-nginx-and-apache2-ae7d27b421c6 (дата звернення: 10.06.2025).

41. Microsoft Learn. Server Message Block (SMB) protocol overview. – URL: https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview (дата звернення: 10.06.2025).

42. Ubuntu Documentation. Setting up Samba as a File Server. – URL: https://ubuntu.com/server/docs/samba-file-server (дата звернення: 10.06.2025).

Для нотаток

Для нотаток

Для нотаток

Для нотаток

А31 Адміністрування комп’ютерних мереж та систем: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп’ютерна інженерія» галузі знань 12 (F) Інформаційні технології спеціальності 123 (F7) Комп’ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2026. 328 с.

Конспект лекцій з дисципліни «Адміністрування комп’ютерних мереж та систем» складено відповідно до діючої програми курсу.

Призначено для здобувачів вищої освіти спеціальності 123 (F7) Комп’ютерна інженерія освітньої програми «Комп’ютерна інженерія».

Комп’ютерний набір Н. В. Багнюк

Редактор Н. В. Багнюк

Підп. до друку «___» _____ 2026р.

Формат 60х84/16. Папір офс. Гарнітура Таймс.

Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій

Луцького національного технічного університету

43018, м. Луцьк, вул. Львівська, 75