ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження можливостей адміністрування корпоративної мережі на основі Windows Server 2022»

на здобуття освітнього ступеня магістра
зі спеціальності 122 Комп'ютерні науки
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні науки
(назва)

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

_____ Андрій ЛОКОЙДА
(підпис) *(Ім'я, ПРІЗВИЩЕ здобувача)*

Виконав:
здобувач вищої освіти Андрій ЛОКОЙДА
група КНДМ-61

Керівник: Юрій КАТКОВ
науковий ступінь, вчене звання д.т.н., доцент

Рецензент:
науковий ступінь, вчене звання
_____
(Ім'я, ПРІЗВИЩЕ)

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерних наук

Ступінь вищої освіти Магістр

Спеціальність 122 Комп'ютерні науки

Освітньо-професійна програма Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерних наук

_____ Віктор ВИШНІВСЬКИЙ
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Локойді Андрію Олеговичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження можливостей адміністрування корпоративної мережі на основі Windows Server 2022

керівник кваліфікаційної роботи Юрій КАТКОВ д.т.н., доцент,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» 10.2023р. №145

2. Строк подання кваліфікаційної роботи «29» грудня 2023р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література з питань, пов'язаних з темою роботи.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз основ адміністрування корпоративної мережі

Дослідження особливостей застосування Windows Server 2022 для корпоративної мережі
Моделювання процесів адміністрування корпоративної мережі у віртуальному середовищі під час застосування Windows Server 2022

5. Перелік графічного матеріалу: *презентація*
    1. Основи адміністрування корпоративної мережі
    2. Основні інструменти адміністрування корпоративної мережі
    3. Розгортання та налаштування DHCP-сервер та AD
    4. Розгортання та налаштування DNS-серверу та RRAS

6. Дата видачі завдання«19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	19.10-05.11.23	
2	Аналіз специфіки і характеристик основ адміністрування корпоративної мережі	05.11-12.11.23	
3	Дослідження методів здійснення особливостей застосування Windows Server 2022 для адміністрування корпоративної мережі	13.11-19.11.23	
4	Моделювання методів здійснення можливостей Windows Server 2022 у віртуальному середовищі	20.11-25.11.23	
5	Основні розділи.	27.11-03.12.23	
6	Розробка обов’язкових матеріалів.	04.12-10.12.23	
7	Попередній захист роботи.	11.12-20.12.23	
8	Пред'явлення роботи в деканат.	21.12-29.12.23	

Здобувач вищої освіти _____ Андрій ЛОКОЙДА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій КАТКОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 138 стор., 1 табл., 102 рис., 61 джерел.

Наукове завдання – оцінка доцільності та ефективності використання Windows Server 2022 для адміністрування сучасної корпоративної мережі.

Мета роботи – підвищити ефективність застосування можливостей Windows Server 2022 для адміністрування та управління корпоративними мережами.

Об'єкт дослідження – процес використання Windows Server 2022 для корпоративного адміністрування мережі, що включає в себе застосування функцій пропонованих Windows Server 2022, які мають відношення до управління і забезпечення безпеки корпоративної мережі.

Предмет дослідження – потенціал Windows Server 2022 в управлінні корпоративними мережами, а саме: функціональні можливості та переваги, які надає ця операційна система для створення, забезпечення та підтримки ефективних мережевих операцій.

Короткий зміст роботи: Проведено аналіз можливостей адміністрування корпоративної мережі на основі Windows Server 2022.

Проведено аналіз методів та тактик адміністрування корпоративної мережі, які можна використовувати для ефективного управління корпоративною мережею на базі Windows Server 2022.

Проведено аналіз специфіки використання платформа Windows Server 2022 для адміністрування корпоративної мережі.

Проведено моделювання та оцінка індикаторів ефективності адміністрування корпоративної мережі за допомогою основних можливостей на основі Windows Server 2022 за допомогою основного спектру можливостей.

КЛЮЧОВІ СЛОВА: WINDOWS SERVER 2022, КОРПОРАТИВНА МЕРЕЖА, АДМІНІСТРУВАННЯ

ABSTRACT

Text part of the master's qualification work: 138 pages, 102 pictures, 1 table, 61 sources.

This scientific work is aimed at evaluating the feasibility and effectiveness of using Windows Server 2022 for the administration of a modern corporate network.

Object of research – The process of using Windows Server 2022 for corporate network administration, which includes the application of features offered by Windows Server 2022 that are related to the management and security of the corporate network.

Subject of research – The potential of Windows Server 2022 in enterprise network management, namely: the functionality and benefits that this operating system provides to create, secure and maintain effective network operations.

Summary of the work: An analysis of the capabilities of corporate network administration based on Windows Server 2022 was carried out.

An analysis of the methods and tactics of corporate network administration that can be used for effective management of a corporate network based on Windows Server 2022 has been carried out.

An analysis of the specifics of using the Windows Server 2022 platform for corporate network administration was carried out.

KEYWORDS: WINDOWS SERVER 2022, CORPORATE NETWORK, ADMINISTRATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Cisco PBM	-	Cisco Plan, Build, Manage
Cisco PPDIOO	-	Cisco Prepare, Plan, Design, Implement, Operate, and Optimize
DNS-сервери	-	Domain Name System-сервери
DRTM	-	Dynamic Root of Trust for Measurement
NDLC	-	Network Device Lifecycle Services
OSI	-	Open Systems Interconnection
TCP / IP	-	Transmission Control Protocol/Internet Protocol
TPM	-	Trusted Platform Module
IT	-	Information Technology

ВСТУП

У світі, де все взаємопов’язано корпоративні мережі відіграють важливу роль в успіху будь-якої організації. Вони забезпечують інфраструктуру, яка підтримує основні бізнес-операції, від спілкування та співпраці до зберігання та доступу до даних. Як наслідок, ефективне адміністрування корпоративних мереж є ключовим фактором для забезпечення того, щоб бізнес міг продовжувати працювати безперебійно, а всі IT-системи працювали без збоїв [1,2].

Windows Server 2022 — це вершина розвитку серверних операційних систем Microsoft, яка забезпечує повний спектр функцій і інструментів для керування та захисту корпоративних мереж. Цей диплом детально дослідить особливості Windows Server 2022, надаючи учасникам знання та навички, необхідні для ефективного адміністрування корпоративних мереж і підтримки IT-інфраструктури своїх організацій [1, 2].

Обґрунтування вибору теми та її актуальність. Ця тема є вельми актуальна і своєчасна з кількох причин. Windows Server 2022 - це найновіша версія серверної операційної системи Microsoft, яка є флагманською для компанії, і вона пропонує ряд нових функцій та функцій, які можуть бути корисними для підприємств будь-якого розміру. Крім того, попит на кваліфікованих адміністраторів корпоративних мереж високий, і існує нестача кваліфікованих фахівців для заповнення цих посад [1,2].

Windows Server 2022 - це потужна і універсальна серверна операційна система, яку можна використовувати для задоволення широкого спектру бізнес-потреб. Вона пропонує ряд нових функцій і можливостей, які можуть допомогти підприємствам підвищити свою безпеку, продуктивність і керованість. Деякі з ключових сучасних особливостей Windows Server 2022 включають [1, 2].

Функції безпеки, які стали більш сучасними: Операційна система включає ряд нових функцій безпеки, які можуть допомогти підприємствам захистити свої мережі від кібератак. Ці функції включають [1, 2]:

Покращений захист від загроз: Windows Server 2022 включає розширені можливості захисту від загроз, які можуть допомогти підприємствам виявляти та запобігати кібератакам [1, 2].

Безпека з нульовою довірою: Windows Server 2022 має такі можливості як безпека з нульовою довірою, яка є моделлю безпеки, яка передбачає, що жодному користувачеві чи пристрою не можна довіряти, поки вони не будуть чітко перевірені [1, 2].

Безпечне завантаження: Windows Server 2022 включає функцію безпечного завантаження, яка допомагає забезпечити завантаження на сервер лише надійного програмного забезпечення [1, 2].

Покращені функції продуктивності: Windows Server 2022 включає ряд нових функцій продуктивності, які можуть допомогти підприємствам підвищити продуктивність своїх мереж. До таких функцій належать: Програмно-визначувана система зберігання даних: Storage Spaces Direct - це нова технологія зберігання даних, яка дозволяє підприємствам створювати програмно-визначені рішення для зберігання даних [1, 2].

Покращення мережі: Windows Server 2022 включає ряд мережевих удосконалень, які можуть допомогти підприємствам підвищити продуктивність своїх мереж. Ці покращення включають [1, 2]:

Покращена продуктивність моделі передачі даних: Windows Server 2022 включає ряд покращень продуктивності TCP / IP [1, 2].

Покращений контроль перевантаження мережі: Windows Server 2022 включає вдосконалені алгоритми контролю перевантаження мережі [1, 2].

Покращені методи управління: Операційна система для серверів від Microsoft включає ряд нових функцій управління, які можуть полегшити підприємствам управління своїми мережами. До таких функцій належать [1, 2]:

- *Центр адміністрування Windows*: Панель керування Windows для адміністраторів-це сучасний веб-інструмент управління, який дозволяє підприємствам керувати своїми мережами з будь-якого місця [1, 2].

Розширювана оболонка командного рядка Windows: Надійна та безпечна операційна система для корпоративних мереж включає розширені можливості PowerShell, які можуть допомогти підприємствам автоматизувати свої завдання управління мережею [1, 2].

Попит на кваліфікованих адміністраторів корпоративних мереж високий. За даними Державної служби статистики США, середня річна зарплата адміністраторів мереж та комп'ютерних систем у травні 2020 року становила 100 510 доларів. За прогнозами, зайнятість мережевих адміністраторів та IT-спеціалістів з підтримки комп'ютерної інфраструктури зросте на 6 відсотків між 2020 і 2030 роками, що набагато швидше, ніж у середньому для всіх професій. Очікується, що це зростання буде зумовлене зростаючим попитом підприємств на надійні та захищені мережі [1, 2].

Ступінь вивченої проблеми. Ступінь вивченості проблеми для диплома на тему «Дослідження можливостей адміністрування корпоративної мережі на базі Windows Server 2022» є складним. Це пояснюється тим, що ця тема є відносно новою, і існує не так багато досліджень на цю тему. Крім того, ця тема непроста і вимагає глибокого розуміння як корпоративних мереж, так і Windows Server 2022 [1, 2].

Однак потенційні переваги завершення диплому з цієї теми значні. Windows Server 2022 — це остання версія операційної системи для забезпечення роботи бізнесу, яка стає все популярнішою в корпоративному середовищі. Як наслідок, існує високий попит на кваліфікованих фахівців, які можуть адмініструвати мережі Windows Server 2022 [1, 2].

Цей диплом окреслює навички та знання, необхідні для досягнення успіху в цій галузі. Дипломна робота покаже налаштовування та управління основними серверними функціями Windows Server 2022 для управління корпоративними мережами. Також постане питання захисту корпоративних мереж від загроз.

Загалом ступінь дослідження проблеми для диплома непростий, але потенційні переваги значні.

Специфіка джерельної бази. База джерел для диплому є різноманітною та всебічною, охоплює як теоретичні, так і практичні аспекти Windows Server 2022 у контексті адміністрування корпоративної мережі.

Мета роботи – підвищити ефективність застосування можливостей Windows Server 2022 для адміністрування та управління корпоративними мережами.

Об'єкт дослідження – процес використання Windows Server 2022 для корпоративного адміністрування мережі, що включає в себе застосування функцій пропонованих Windows Server 2022, які мають відношення до управління і забезпечення безпеки корпоративної мережі.

Предмет дослідження – потенціал Windows Server 2022 в управлінні корпоративними мережами, а саме: функціональні можливості та переваги, які надає ця операційна система для створення, забезпечення та підтримки ефективних мережевих операцій.

Наукове завдання. - оцінка доцільності та ефективності використання Windows Server 2022 для адміністрування сучасної корпоративної мережі.

Завдання роботи:

1. Проаналізування основ адміністрування корпоративних мереж.

2. Проаналізування можливості Windows Server 2022 для корпоративного адміністрування мережі.

3. Зрозуміння аспектів Windows Server 2022, пов'язаних з адмініструванням корпоративної мережі.

4. Дослідження основних аспектів Windows Server 2022 у віртуальній обстановці для управління корпоративними мережами.

Методика дослідження. Це дипломне дослідження буде проводитися з використанням підходу змішаних методів, поєднуючи як якісний, так і кількісний збір та аналіз даних. Це дозволяє повністю зрозуміти можливості та проблеми адміністрування корпоративної мережі на основі Windows Server 2022.

Результати дослідження. Результати дослідження у цій дипломній роботі розглядають можливості Windows Server 2022 в адмініструванні корпоративної

мережі. Дослідження фокусується на чотирьох ключових сервісах: Active Directory, DNS, DHCP та RRAS. Дослідження аналізує особливості та функціональні можливості кожної служби, її роль у мережевій інфраструктурі та її вплив на управління мережею та безпеку. Дослідження також досліджує переваги та проблеми використання Windows Server 2022 для адміністрування мережі та надає рекомендації щодо його ефективної реалізації.

Апробація результатів досліджень.

Матеріали були опубліковані в статті:

Локойда А. О., Катков Ю. І. Особливості адміністрування корпоративної мережі на основі Windows Server 2022 // Наукові записки Державного університету телекомунікацій №4, 2023, Подано до друку. https://journals.dut.edu.ua/index.php/sciencenotes/issue/archive

В тезисах:

Локойда А. О., Катков Ю. І. ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК І ТЕРОРИСТИЧНИХ ЗАГРОЗ // Науково-практична конференція «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» Збірник тез. – К.: ДУІКТ, 2023. 27 жовтня 2023, С-180-182. https://duikt.edu.ua/uploads/p_2626_52007398.pdf

1 АНАЛІЗ ОСНОВ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Планування та проектування корпоративної мережі

Корпоративна мережа - це група комп'ютерів, з'єднаних між собою в будівлі або в певній області, які всі належать одній компанії або установам. Вона не прив’язана до певного місця та може включати просторово віддалені частини організації, такі як філії, дочірні компанії та навіть офіси за кордоном [33, 34, 35, 38]. Приклад архітектури корпоративної мережі наданий на Рис.1.1

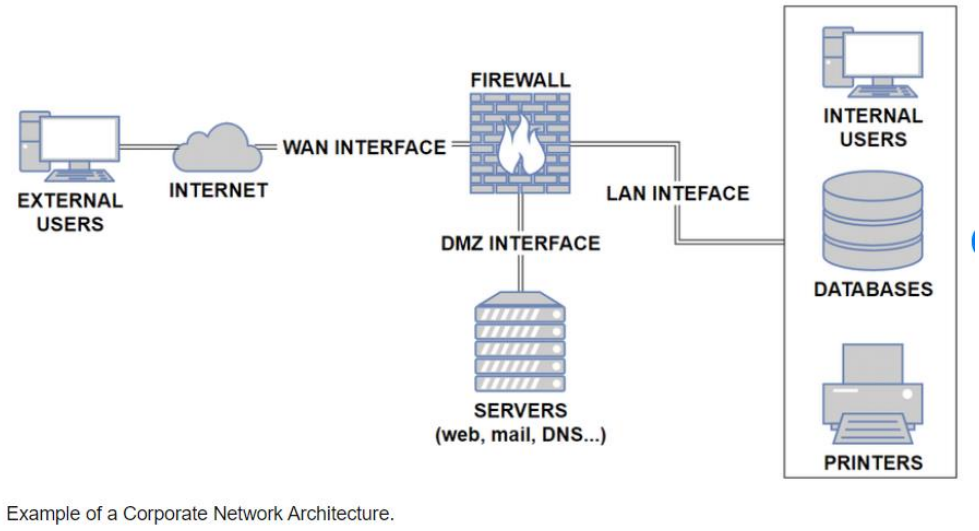


Рисунок 1.1 – Приклад архітектури корпоративної мережі [3]

На Рис.1.1 надано приклад архітектури корпоративної мережі відносно якого здійснюється планування та проектування корпоративної мережі, також відомий як проектування мережі, — це практика планування та проектування комунікаційної мережі. Цей процес починається з визначення ділових і технічних вимог і триває до моменту впровадження мережі [33, 34, 35, 38].

Ось кілька ключових етапів планування та проектування [33, 34, 35, 38]:

Підготовка: Визначити вимоги високого рівня та стратегію. Результати цього етапу можуть включати документацію щодо вимог і опитування поточного стану [33, 34, 35, 38].

Планування: вирішуйте конкретні вимоги до мережі на основі інформації, зібраної на етапах планування [33, 34, 35, 38].

Проектування: використовуйте інформацію, зібрану на попередніх двох етапах, щоб створити детальний проект мережі [33, 34, 35, 38].

Впровадження: налаштувати та розгорнути мережеву інфраструктуру. На цьому етапі часто проводиться тестування для перевірки дизайну [33, 34, 35, 38].

Експлуатація: відстежуйте мережу під час її використання, щоб переконатися, що мережа працює так, як задумано, і здатність швидко вирішувати проблеми, коли це не так [33, 34, 35, 38].

Оптимізація: визначення необхідних налаштування та оптимізацію. Для великих змін цикл починається знову, щоб спланувати та реалізувати їх [33, 34, 35, 38].

Ці кроки є частиною популярної моделі життєвого циклу мережі, відомої як модель Cisco PPDIOO. Модель життєвого циклу мережі Cisco PPDIOO надана на Рис.1.2. Інші моделі життєвого циклу мережі включають Cisco PBM (планування, створення, управління) і NDLC (життєвий цикл розробки мережі) [33, 34, 35, 38].

Рисунок 1.2 – Модель життєвого циклу мережі Cisco PPDIOO [58]

У контексті адміністрування корпоративної мережі розуміння цих етапів є фундаментальним. Це допомагає забезпечити, щоб мережа відповідала потребам організації, зберігаючи продуктивність, безпеку, резервування та економічну ефективність [33, 34, 35, 38].

1.2 Розгортання та налаштування мережі

Розгортання та налаштування мережі є важливим завданнням адміністрування корпоративної мережі. Воно включає наступні етапи:

1. Закупівля обладнання та програмного забезпечення. Приклади обладнання для корпоративної мережі надано на Рис.1.3. На цьому етапі необхідно придбати необхідне обладнання та програмне забезпечення, а також підготувати його до встановлення [21].

2. Встановлення обладнання та програмного забезпечення. На цьому етапі необхідно встановити обладнання та програмне забезпечення відповідно до схеми мережі.

3. Налаштування обладнання та програмного забезпечення. На цьому етапі необхідно налаштувати обладнання та програмне забезпечення відповідно до вимог мережі.

4. Тестування мережі. На цьому етапі необхідно протестувати мережу на працездатність.

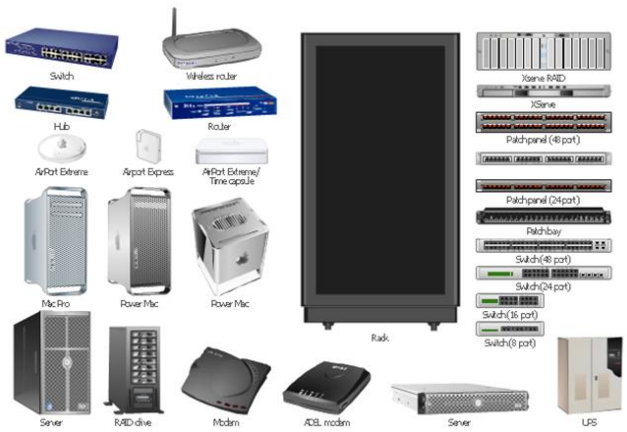


Рисунок 1.3 – Приклади обладнання для корпоративної мережі [61]

Закупівля обладнання та програмного забезпечення. При покупці обладнання та програмного забезпечення необхідно враховувати такі фактори:

- Гарантія Необхідно переконатися, що обладнання та програмне забезпечення мають гарантію.

- Повернення. Необхідно переконатися, що обладнання та програмне забезпечення можна повернути, якщо воно не підходить.
- Доставка. Необхідно переконатися, що обладнання та програмне забезпечення будуть доставлені вчасно.

Встановлення обладнання та програмного забезпечення. На етапі встановлення обладнання необхідно встановити обладнання відповідно до розробленої топології мережі та налаштувати його відповідно до вимог. Під час встановлення програмного забезпечення необхідно дотримуватися інструкцій виробника.

Налаштування обладнання та програмного забезпечення. При налаштуванні обладнання та програмного забезпечення необхідно виконати такі завдання:

- Налаштування IP-адрес. Для кожного пристрою в мережі необхідно встановити унікальну IP-адресу.
- Налаштування мережевих масок. Мережева маска визначає, яка частина IP-адреси є адресою пристрою, яка частина - адресою мережі.
- Налаштування шлюзів. Шлюз - це пристрій, який використовується для перенаправлення трафіку до інших мереж.
- Настроювання DNS-серверів. DNS-сервери використовуються для перетворення доменних імен на IP-адреси [21].
- Налаштування безпеки. Необхідно вжити заходів безпеки для захисту мережі від несанкціонованого доступу [21].

Тестування мережі. На етапі тестування мережі потрібно перевірити працездатність мережі. При тестуванні мережі необхідно враховувати такі фактори [22, 23]:

- Підключення пристроїв. Перевірте підключення пристроїв до мережі.
- Обмін даними. Необхідно перевірити можливість обміну даними між пристроями мережі.
- Безпека. Необхідно перевірити безпеку мережі.
- Продуктивність. Потрібно перевірити продуктивність мережі.

1.3 Управління мережею

Управління мережею - це комплекс завдань, пов'язаних із підтриманням працездатності та ефективності корпоративної мережі. Воно включає наступні основні напрямки: обслуговування мережі, розширення мережі, управління корпоративною мережею, інструменти керування мережею [22, 23].

Обслуговування мережі. На етапі обслуговування мережі здійснюється моніторинг мережі, виявлення та усунення несправностей, оновлення обладнання та програмного забезпечення. Моніторинг мережі дозволяє відстежувати її стан та виявляти потенційні проблеми. Усунення несправностей здійснюється шляхом виявлення причин несправності та їх усунення. Оновлення обладнання та програмного забезпечення дозволяє підтримувати мережу в актуальному стані та підвищувати її безпеку та ефективність [22, 23].

Розширення мережі. На етапі розширення мережі здійснюється додавання нових пристроїв та користувачів до мережі, розширення її пропускної спроможності та функціональності. Додавання нових пристроїв та користувачів до мережі може знадобитися через зростання бізнесу або зміну потреб користувачів. Розширення пропускної спроможності мережі може знадобитися через збільшення навантаження на мережу. Розширення функціональності мережі може знадобитися для додавання нових програм або послуг [22, 23].

Управління корпоративною мережею. Управління корпоративною мережею – це складний процес, що вимагає від адміністратора мережі глибоких знань та досвіду. Адміністратор мережі повинен уміти вирішувати широке коло завдань, пов'язаних із плануванням, розгортанням, обслуговуванням та розширенням мережі. До конкретних завдань управління корпоративною мережею належать [22, 23]:

1. Адміністрування обладнання та програмного забезпечення мережі. Адміністратор мережі повинен вміти налаштовувати та керувати обладнанням та програмним забезпеченням мережі, включаючи комутатори, маршрутизатори, сервери, робочі станції та периферійні пристрої [22, 23].

2. Керування користувачами та доступом до ресурсів мережі. Адміністратор мережі повинен уміти створювати та керувати обліковими записами користувачів, а також надавати користувачам доступ до ресурсів мережі [22, 23].

3. Управління безпекою мережі. Адміністратор мережі повинен уміти забезпечувати безпеку мережі від зовнішніх та внутрішніх загроз [22, 23].

4. Моніторинг мережі. Адміністратор мережі повинен уміти відстежувати стан мережі та виявляти потенційні проблеми [22, 23].

5. Виправлення неполадок мережі. Адміністратор мережі повинен уміти виявляти причини несправності мережі та їх усувати [22, 23].

Інструменти керування мережею. Для управління корпоративною мережею використовуються різні інструменти, такі як [22, 23]:

- Мережеві операційні системи. Мережеві операційні системи, такі як Windows Server або Linux, надають набір інструментів для керування мережею [22, 23].
- Мережеві утиліти. Мережні утиліти, такі як ping, traceroute та netstat, дозволяють діагностувати проблеми з мережею [22, 23].
- Мережеві сканери. Мережеві сканери дозволяють виявляти пристрої та ресурси мережі [22, 23].
- Мережеві монітори. Мережні монітори дають змогу відстежувати стан мережі в режимі реального часу [22, 23].

Приклади мережевих операційних систем, сканерів і моніторів надано на Рис. 1.4, Рис. 1.5 і Рис.1.6.

Рисунок 1.4 – Приклади мережевих операційних систем [55]

Рисунок 1.5 – Приклади мережевих сканерів [56]

Рисунок 1.6 – Приклади мережевих моніторів [57]

Таким чином управління корпоративною мережею – це важливий процес, що забезпечує працездатність та ефективність мережі. Адміністратор мережі повинен уміти вирішувати широке коло завдань, пов'язаних із плануванням, розгортанням, обслуговуванням та розширенням мережі [22, 23].

1.4 Безпека мережі

Безпека мережі є одним із найважливіших аспектів адміністрування корпоративної мережі. Вона включає захист мережі від зовнішніх і внутрішніх загроз, таких як[22, 23] :

1. Хакерські атаки, спрямовані на крадіжку даних, порушення роботи мережі або повне її знищення [22, 23].
2. Віруси та інші шкідливі програми, здатні завдати шкоди системі або вкрасти дані [22, 23].
3. Несанкціонований доступ до мережі з боку працівників чи зовнішніх осіб [22, 23].

Для забезпечення безпеки мережі необхідно виконувати такі завдання [22, 23]:

- Розробка та впровадження політики безпеки, яка визначає правила доступу до мережі та її ресурсів [22, 23].
- Встановлення та налаштування засобів захисту, таких як брандмауери, антивірусні програми, системи запобігання вторгненням (IPS) [22, 23].
- Навчання працівників правилам безпеки [22, 23].

Розробка та впровадження політики безпеки. Політика безпеки має визначати такі аспекти [22, 23]:

- Права доступу до мережі та її ресурсів. Необхідно визначити, хто має доступ до мережі та її ресурсів, а також які дії можуть виконувати [22, 23].
- Регламентація використання мережі. Необхідно визначити правила використання мережі, такі як заборона використання несанкціонованого софта, завантаження файлів з ненадійних ресурсів тощо [17, 18].
- Заходи реагування на інциденти безпеки. Необхідно визначити дії, які необхідно вжити у разі виникнення інциденту безпеки [17, 18].

Встановлення та налаштування захисних засобів. Захисні засоби мають бути встановлені на всіх пристроях, підключених до мережі. Приклади популярних брандмауерів і антивірусів надано на Рис. 1.7, Рис. 1.8. Необхідно регулярно оновлювати програмне забезпечення засобів захисту для забезпечення їхньої актуальності [17, 18].

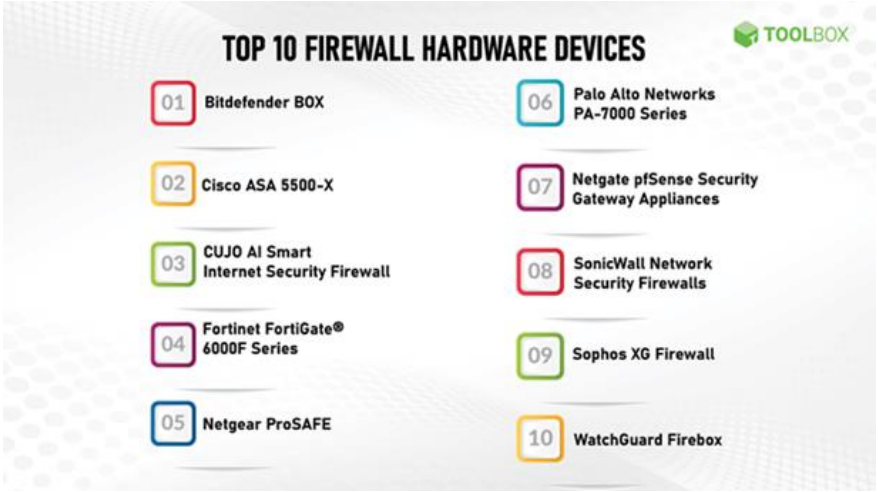


Рисунок 1.7 – Приклади популярних брандмауерів [59]

Рисунок 1.8 – Приклади популярних антивірусів [60]

Навчання працівників правилам безпеки. Співробітники повинні мати знання та розуміння правил безпеки мережі. Необхідно регулярно проводити навчання співробітників, щоб вони були обізнані про існуючі загрози і могли мати можливість вжити заходів, щоб не допустити їх [17, 18].

Захист мережі є комплексним завданням, що вимагає від адміністратора мережі знань та навичок у сфері інформаційної безпеки. Адміністратор мережі повинен постійно стежити за змінами у сфері інформаційної безпеки та своєчасно впроваджувати нові заходи захисту для захисту корпоративної мережі від несанкціонованого доступу, атак і інших загроз [17, 18].

1.5 Основні інструменти адміністрування корпоративної мережі

Корпоративні мережі відіграють вирішальну роль в успіху сучасного бізнесу. Вони забезпечують спілкування та співпрацю між співробітниками, забезпечують доступ до основних ресурсів і полегшують обмін інформацією з клієнтами та партнерами. Як наслідок, належне адміністрування корпоративних мереж має важливе значення для забезпечення їх надійності, безпеки та продуктивності. Для управління корпоративною мережею необхідно використовувати спеціалізовані інструменти. Вони дозволяють автоматизувати багато завдань, зробити мережу більш безпечною та надійною, а також

покращити її продуктивність. Існують наступні види інструментів: мережеві операційні системи, управління ресурсами, налаштування мережевих служб, моніторинг продуктивності мережі, усунення проблем мережі [17, 18].

Мережеві операційні системи — це програмне забезпечення, для керування та контролю комп'ютерних мереж. Приклади популярних мережевих операційних систем надано на Рис. 1.9. Вони надають різноманітні функції та служби, які дозволяють мережевим адміністраторам [17, 18]:

Рисунок 1.9 – Приклади популярних мережевих операційних систем [56]

Управління ресурсами: Мережеві операційні системи забезпечують засобами для керування мережевими ресурсами, такими як користувачі, групи, спільні ресурси та дозволи. Це включає створення, видалення та зміну облікових записів користувачів, призначення дозволів на доступ до мережевих ресурсів і моніторинг активності користувачів [17, 18].

Налаштування мережевих служб: Мережеві операційні системи забезпечують функціональність для налаштування мережевих служб, таких як обмін файлами, друк, електронна пошта та веб-сервери. Це включає в себе встановлення та налаштування серверних програм, визначення політик доступу користувачів і керування параметрами безпеки [17, 18].

Моніторинг продуктивності мережі: Мережеві операційні системи містять засоби для моніторингу показників продуктивності мережі, таких як використання пропускної здатності, втрата пакетів і затримка. Цю інформацію можна використовувати для виявлення та усунення проблем мережі, перш ніж вони вплинуть на користувачів [17, 18].

Усунення проблем мережі: Мережеві операційні системи дозволяють виконувати завдання для вирішення проблем мережі, таких як помилки підключення, низька продуктивність і порушення безпеки. Це включає використання інструментів діагностики мережі, аналіз журналів мережі та передачу проблем на вищі рівні підтримки [17, 18].

Для управління корпоративною мережею необхідно використовувати загальні мережеві операційні системи. Найбільш поширеними мережевими операційними системами є Windows Server, Linux та FreeBSD [17, 18].

Windows Server - це потужна операційна система, яка може використовуватися для підтримки великих мереж, розроблена корпорацією Майкрософт. Це серверна операційна система, яка забезпечує платформу для запуску різних серверних додатків, таких як файлові сервери, сервери друку, веб-сервери та сервери електронної пошти. Windows Server також використовується для управління мережами та забезпечення їх безпеки.

Переваги використання Windows Server як засобу адміністрування корпоративної мережі [17, 18]:

1. Масштабованість: Windows Server можна масштабувати для підтримки мереж широкого діапазону розмірів, від малого бізнесу до великих підприємств.
2. Надійність: Windows Server-це надійна операційна система, яка призначена для роботи в режимі 24/7.
3. Безпека: Windows Server включає ряд функцій безпеки, які можуть захистити мережу від хакерів.
4. Простота використання: Windows Server відносно простий у використанні та керуванні навіть для адміністраторів з обмеженим досвідом.
5. Сумісність: Windows Server сумісний з широким спектром апаратного та програмного забезпечення, включаючи продукти Microsoft та сторонніх виробників.

Основні можливості Windows Server [17, 18]:

- Active Directory: Доменна служба каталогів - це служба каталогів, яка дозволяє адміністраторам керувати користувачами, комп'ютерами та іншими мережевими ресурсами [17, 18].
- DHCP: Протокол динамічного налаштування хоста - це протокол, який динамічно призначає IP-адреси мережевим пристроям [17, 18].
- DNS: Система доменних імен - це система, яка зберігає інформацію про те, які доменні імена відповідають яким IP-адресам [17, 18].
- RRAS: Це служба, що забезпечує додаткову підтримку мережевої роботи TCP/IP і дозволяє серверу функціонувати як мережевий маршрутизатор. Ця роль підтримує віддалене підключення користувача або сайту до сайту через віртуальну приватну мережу або комутовані з'єднання [53, 54].
- IIS: Це гнучкий, безпечний і керований веб-сервер для розміщення будь-чого в Інтернеті. Він надає платформу для надійного хостингу веб-сайтів, послуг та додатків. Масштабована і відкрита архітектура IIS готова вирішувати найскладніші завдання - від потокового передавання мультимедіа до веб-додатків [52].

Windows Server - надійна платформа для адміністрування корпоративних мереж. Головні відмінності Windows Server 2022 показані в таблиці 1.1.

Таблиця 1.1 Головні відмінності Windows Server 2022 від інших версій

Відмінності	Windows Server 2022	Windows Server 2019	Windows Server 2016	Windows Server 2012 R2	Windows Server 2008
Випуск	18 серпня 2021 року	2 жовтня 2018 року	20 жовтня 2016 року	4 вересня 2012 року	18 жовтня 2010 року
Тип випуску	LTSC	LTSC	LTSC	Semi-Annual Channel	Semi-Annual Channel
Підтримка	10 років	5 років	3 роки	18 місяців	5 років
Процесор	Intel Ice Lake, AMD EPYC	Intel Skylake, AMD Zen+	Intel Skylake, AMD Zen	Intel Haswell, AMD Piledriver	Intel Nehalem, AMD Barcelona
Оперативна пам'ять	До 48 ТБ	До 2 ТБ	До 2 ТБ	До 1 ТБ	До 256 ГБ
Логічні ядра	До 2048	До 256	До 256	До 256	До 64
Гібридні можливості	Підтримка Azure Arc, Windows Admin Center	Підтримка Azure Stack, Windows Admin Center	Підтримка Azure Stack, Windows Admin Center	Немає	Немає
Контейнери	Підтримка Kubernetes, OCI Images, Azure Container Registry	Підтримка Kubernetes, OCI Images, Azure Container Registry	Підтримка Kubernetes, OCI Images, Azure Container Registry	Немає	Немає
Інші	Підтримка IPv6, підтримка QUIC, підтримка віртуальної машини Azure без перезавантаження	Підтримка IPv6, підтримка QUIC, підтримка віртуальної машини Azure без перезавантаження	Підтримка IPv6, підтримка QUIC, підтримка віртуальної машини Azure без перезавантаження	Підтримка IPv6, підтримка QUIC	Немає

Платформа пропонує безліч інструментів і функцій, які роблять його потужним вибором для мережевих адміністраторів [48, 49, 50, 51]:

1. Azure ar Azure Automanage може ще більше спростити досвід управління [48, 49, 50, 51].

2. Центр адміністрування Windows: це веб-інтерфейс браузера, який забезпечує повний контроль над розгортанням Windows Server і кластерів. Він пропонує модернізовані версії звичних інструментів та інтеграцію з Azure [48, 49, 50, 51].

3. System Center: це набір інструментів для управління масштабом центру обробки даних, включаючи операції, захист даних, віртуалізацію та автоматизацію [48, 49, 50, 51].

4. Інструменти локального керування: Windows Server включає інструменти локального керування, такі як менеджер сервера, MMC, PowerShell та інструменти командного рядка для загального керування сервером, налаштування ролей та усунення несправностей [48, 49, 50, 51].

5. Інструменти адміністрування віддаленого сервера (RSAT): RSAT дозволяє мережевим адміністраторам керувати функціями та ролями з комп'ютера, на якому працює підтримувана версія Windows [48, 49, 50, 51].

6. Безпека та відповідність: Windows Server містить вбудовані функції безпеки та інструменти відповідності, які допомагають захистити мережу та дані [48, 49, 50, 51].

7. Масштабованість: Windows Server дуже масштабований, що робить його придатним для підприємств будь-якого розміру [48, 49, 50, 51].

Отже, Windows Server надає повний набір інструментів і функцій, які роблять його відмінним вибором для адміністрування корпоративних мереж [48, 49, 50, 51].

Linux. Linux є популярним вибором для корпоративних мереж завдяки своїй стабільності, безпеці та гнучкості. Ось деякі ключові моменти про Linux в контексті корпоративних мереж [44, 45, 46 ,47]:

1. Різноманітність дистрибутивів: Є кілька дистрибутивів Linux, які добре підходять для корпоративного використання. Деякі з кращих включають Red Hat Enterprise Linux, Ubuntu, Linux Mint, CentOS, Debian та Fedora [44, 45, 46 ,47].

2. Серверні програми: Linux зазвичай використовується для запуску різних серверних додатків у корпоративному світі. Сюди входять файлові сервери, сервери друку, системи доставки контенту, глобальні сервери кешування, архіви даних, сервери VPN тощо [44, 45, 46 ,47].

3. Рентабельний: Linux сам по собі безкоштовний, тому це підтримка дистриб'ютора, за яку треба будете платити. Ціна на належну корпоративну підтримку все ще робить Linux набагато дешевшим варіантом порівняно з іншими операційними системами [44, 45, 46 ,47].

4. Безпека: Linux часто розглядається як більш безпечний порівняно з іншими операційними системами. Часті оновлення забезпечують своєчасне вирішення проблем безпеки [44, 45, 46 ,47].

5. Сумісність: дистрибутиви Linux можуть запускати програми Windows через віртуальні машини або підсистеми, такі як Wine. Ця сумісність з Windows може бути привабливою для компаній, які покладаються на певні програми Windows [44, 45, 46 ,47].

6. Сумісність Cloud і SaaS: велика частина корпоративних обчислень включає QuickBooks Pro, Salesforce, Google Docs, Microsoft Office, Base Camp і Skype. Всі вони доступні як програми безпосередньо на Linux або з хмарних або SaaS альтернатив [44, 45, 46 ,47].

7. Підтримка: дистрибутиви Linux, такі як Red Hat Enterprise Linux, забезпечують більше, ніж операційна система - вони також підключають вас до великої апаратної, програмної та хмарної партнерської екосистеми та мають підтримку 24x7 [44, 45, 46 ,47].

В цілому, Linux пропонує переконливий набір переваг для корпоративних мереж. Його економічна ефективність, безпека, масштабованість і гнучкість роблять його життєздатною альтернативою традиційним операційним системам.

Однак ретельний розгляд проблем впровадження має вирішальне значення для успішного розгортання [44, 45, 46 ,47].

FreeBSD: FreeBSD - це надійна, гнучка та безпечна операційна система з відкритим кодом, яка добре підходить для корпоративних мережевих середовищ. Ось деякі ключові аспекти застосування FreeBSD в мережах [40, ,41, 42, 43]:

Надійні мережеві можливості: потужний стек мереж TCP/IP від FreeBSD забезпечує високу продуктивність, безліч налаштувань та широкий спектр додаткових функцій. Це включає в себе асинхронний Sendfile, ядро рівня і NIC TLS, TCP RACK контроль перевантаження, і WireGuard [40, ,41, 42, 43].

Конфігурація та продуктивність мережі: FreeBSD дозволяє конфігурацію як дротових, так і бездротових мереж. Це включає налаштування мережевого інтерфейсу, адресацію та параметри налаштування. Мережеві можливості FreeBSD і його репутація за відмінну продуктивність мережі роблять його ідеальним вибором для корпоративних мереж [40, ,41, 42, 43].

Розширена мережа: FreeBSD підтримує ряд передових мережевих тем. Це включає в себе основи шлюзів і маршрутів, прив'язки USB, налаштування IEEE® 802.11 і Bluetooth® пристроїв, що робить FreeBSD діяти як міст, налаштування мережевого завантаження PXE, включення і використання можливостей загального протоколу резервування адреси (CARP) в FreeBSD, і налаштування декількох VLAN на FreeBSD [40, ,41, 42, 43].

Мережеві додатки: FreeBSD може перетворити будь-який комп'ютер в інтернет-брандмауер, хост електронної пошти, сервер друку, сервер ПК/NFS і більше3. Він підтримує широкий спектр мережевих служб і протоколів, з інструкціями конфігурації для DNS, DHCP і багато іншого [40, ,41, 42, 43].

Ідеально підходить для серверів: FreeBSD робить ідеальний Інтернет або Інтранет-сервер. Він забезпечує надійні мережеві послуги під найважчими навантаженнями і ефективно використовує пам'ять для підтримки хорошого часу відгуку для тисяч одночасних процесів користувача [40, ,41, 42, 43].

В цілому, FreeBSD є потужною і універсальною операційною системою, добре підходить для живлення корпоративних мереж. Його поєднання

стабільності, безпеки, продуктивності та гнучкості робить його переконливою альтернативою фірмовим рішенням, особливо для організацій, які шукають економічно ефективну та надійну платформу для своєї критичної інфраструктури [40, ,41, 42, 43].

Крім мережевих операційних систем, мережеві адміністратори використовують безліч інших інструментів для управління і підтримки корпоративних мереж. Ось деякі з інструментів, які зазвичай використовуються:

1. *Утиліти для установки і настройки мережевого обладнання*. Ці утиліти використовуються для встановлення та налаштування мережевих пристроїв, таких як маршрутизатори, комутатори та точки доступу. Вони дозволяють конфігурувати такі параметри, як IP-адреси, маски підмережі, шлюзи за замовчуванням, VLAN тощо. До найбільш популярних утиліт для установки і настройки мережевого обладнання відносяться: Cisco IOS CLI, Juniper JunOS CLI, Arista EOS CLI, HP Comware CLI, Cisco Prime Infrastructure, Juniper Contrail, Arista EOS CloudVision, HP Comware CloudDirector.

2. *Утиліти для конфігурації мережевих параметрів*. Ці утиліти використовуються для налаштування мережевих параметрів, таких як DHCP, DNS, маршрутизація, безпека і т.д. вони дозволяють створювати і змінювати мережеві політики, профілі користувачів та інші налаштування. До найбільш популярних утиліт для конфігурації мережевих параметрів відносяться: ISC DHCP, BIND DNS, Cisco IOS OSPF, Juniper JunOS OSPF, Arista EOS OSPF, HP Comware OSPF.

3. *Утиліти для управління доступом до мережі*. Ці утиліти використовуються для управління доступом до мережі, включаючи автентифікацію, авторизацію та аудит. Вони дозволяють створювати та керувати обліковими записами користувачів, групами та політиками доступу. До найбільш популярних утиліт для управління доступом до мережі відносяться: OpenLDAP, Kerberos, RADIUS, TACACS+, Cisco ISE, Juniper SRX, Arista EOS.

4. *Утиліти для спостереження за мережею*. Ці утиліти використовуються для моніторингу мережі, включаючи моніторинг трафіку,

продуктивності та стану обладнання. Вони дозволяють відстежувати мережеві події, виявляти проблеми та вживати заходів для їх усунення. До найбільш популярних утиліт для спостереження за мережею відносяться: SNMP, NetFlow, IPFIX, PRTG Network Monitor, SolarWinds Network Performance Monitor, Nagios, Zabbix, Prometheus.

5. *Утиліти для діагностики та усунення несправностей*. Ці утиліти використовуються для діагностики та усунення несправностей в мережі. Вони дозволяють аналізувати мережеві пакети, відстежувати стан обладнання та виявляти проблеми з продуктивністю. До найбільш популярних утиліт для діагностики та усунення несправностей відносяться: Wireshark, tcpdump, Ping, Traceroute, Netstat, Ipconfig, Nslookup.

Таким чином, при виборі інструментів адміністрування корпоративної мережі необхідно враховувати наступні фактори: розмір мережі, тип мережі, функціональні вимоги, бюджет. Для невеликих мереж можуть бути достатньо простих інструментів, таких як утиліти командного рядка. Для великих мереж та мереж з високими вимогами до безпеки та продуктивності необхідно використовувати більш складні інструменти, такі як мережеві операційні системи та системи управління мережею.

2 ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ WINDOWS SERVER 2022 ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Особливості адміністрування корпоративної мережі

Управління корпоративною мережею - складний предмет для розуміння. Більшість статей та ресурсів написані з використанням технічних термінів експертами або для аудиторії експертів. Щоб ще більше ускладнити ситуацію, в мережевому управлінні представлені різні спеціальності. Управління мережею включає все апаратне та програмне забезпечення, підключене до бізнесу. Встановлена система відповідає за моніторинг мережі, обслуговування та підготовку самих пристроїв, а також за моніторинг продуктивності мережі, яка їх з'єднує.

Мережеві операції включають моніторинг мережевого трафіку, пропускну здатність, усунення несправностей та підтримку мережевої безпеки. Також необхідно усунути будь-які проблеми з мережею, які впливають на кінцевого користувача. Насправді немає причин, щоб усі, хто не пов'язаний з технологіями, розуміли весь цей жаргон. Але важливо розуміти основні принципи управління мережею, щоб приймати обґрунтовані рішення про те, що потрібно, і найкращі практики для забезпечення безперебійної роботи бізнесу.

Мережа - це вся сукупність пристроїв, підключених для бізнесу. Колись мережа дуже просто ставилася до комп'ютерів, які були об'єднані в мережу в офісі. Підприємства мали внутрішні мережі, які дозволяли всім комп'ютерам отримувати доступ до одних і тих же баз даних - це була мережа.

Для більшої ясності та безпеки будь-який підключений до Інтернету пристрій, який також використовується для роботи або зберігання даних, повинен бути включений у мережу. Необхідно включити кожен пристрій, щоб дотримуватися рекомендацій щодо забезпечення безпеки цих пристроїв.

Що може бути включено у мережу? Для початку настільні комп'ютери, планшети, мобільні пристрої, сервери, брандмауери та маршрутизатори. Мережа включає будь-який пристрій, який може взаємодіяти з іншими пристроями, а також мережу, яка дозволяє їм взаємодіяти. Таким чином, будь-яке обладнання або програмне забезпечення, від найменшого кабелю до найбільшого сервера, включено у мережу.

Мережеві пристрої

Існує ряд пристроїв, що складають мережу. До них відносяться самі пристрої, такі як настільні комп'ютери та мобільні пристрої. Але вони також включають інше Обладнання, зокрема:

Брандмауер. Брандмауери - це функція безпеки, яка дає дозвіл на доставку даних на пристрої, а також може Блокувати дані, які не відповідають запрограмованим критеріям [19].

Сервер. Сервер керує пристроями в цій мережі. Це може бути локальний сервер, розташований локально. Або це може бути віддалений сервер, який працює через Інтернет [19].

Клієнтські додатки. Це Системи, до яких користувачі отримують доступ для виконання завдань [19].

Маршрутизатори. Маршрутизатори з'єднують мережі.

Комутатори. Комутатори створюють реальну мережу і дозволяють пристроям взаємодіяти один з одним. Комутатори та маршрутизатори суттєво відрізняються один від одного, і для функціонування мережі потрібні обидва [19].

Точки доступу. Точки доступу з'єднують кінцевий пристрій з мережею.

Типи мереж

Комп'ютерні мережі можуть бути надзвичайно великими або досить малими. Вони важливі незалежно від того, скільки людей або пристроїв підключено, але розмір часто визначає тип використовуваної мережі. На великих підприємствах у вас можуть бути сотні або тисячі пристроїв у кількох місцях. Для бізнесу у вас може бути лише кілька пристроїв в одному офісному пакеті [19].

Типи мереж - це просто тип підключення, щоб усі ці пристрої могли ефективно та безпечно взаємодіяти. Ось кілька найпоширеніших типів:

LAN. Локальна мережа з'єднує пристрої на одній відстані. Це тип мережі, який можна використовувати для з'єднання комп'ютерів усіх співробітників у невеликому офісі [19].

WLAN. Бездротова локальна мережа працює так само, як і локальна мережа, але використовує бездротові з'єднання, що може бути зручнішим в офісі, дозволяючи працівникам використовувати бездротові пристрої в мережі для мобільності [19].

VPN. Віртуальна приватна мережа – це безпечна мережа, яка дозволяє надсилати зашифровані дані. Це додатковий захід безпеки, який дозволяє співробітникам працювати віддалено з тією ж безпекою, що й у приватній або локальній мережі [19].

WAN. Глобальна мережа дозволяє з'єднувати пристрої на великій відстані [19].

Топології

Топологія в управлінні мережею – це спосіб структурування мережі. Він діє як своєрідна карта мережі та має містити список усіх пристроїв, пов'язаних із мережею, і чіткий опис їхнього розташування у зв'язку один з одним. Найчастіше треба використовувати візуальне представлення топології, щоб показати структуру, компонування та з'єднання [19].

Взаємозв'язок відкритих систем (OSI) або протокол керування передачею/Інтернет-протокол (TCP/IP) — це два варіанти, як дані переміщуються від пристрою до пристрою. Системи OSI використовують сім різних рівнів. Таке розрівнювання дозволяє керівництву мережі чітко бачити, де виникають проблеми, і дає їм більше контролю над припиненням проблеми, перш ніж вона завдасть ще більшої шкоди. Багато шарів є хорошою функцією безпеки [19].

TCP/IP використовується для пристроїв, підключених через Інтернет, а не через приватну локальну мережу [19].

Протокол керування мережею також працюватиме зі стандартним протоколом Інтернету, таким як SNMP, який упорядковує інформацію про IP-адреси [19].

Як обговорювалося раніше, управління мережею саме по собі є повним процесом моніторингу та обслуговування всього у мережі. Воно включає в себе всі підключення, апаратне та програмне забезпечення. Завдання мережевого адміністрування-забезпечити оптимальне функціонування мережі і обслуговування всіх кінцевих точок [19].

Мережевий менеджер або адміністратор мережі використовує встановлені процеси, які дозволяють їм здійснювати нагляд за мережею. Ці робочі процеси розвиваються, оскільки впроваджується так багато нових технологій та підключень. Адміністратор повинен вести фактичний облік усіх пристроїв у мережі та розробляти протокол, щоб оцінити, наскільки добре вони працюють, та керувати життєвим циклом усіх пристроїв. Застарілі пристрої, які не були виправлені або обслуговувалися належним чином, можуть становити загрозу безпеці [19].

Управління мережею стає все більш важливим у міру розвитку технологій. Мережа може включати настільні комп'ютери, підключені через локальну мережу у географічному розташуванні. Якщо співробітники також відповідають на електронну пошту зі свого телефону або використовують платформи або хмарні обчислення, все це потрібно додати до топології [19].

Багато компаній вважають, що більш продуктивно співпрацювати з MSP, що спеціалізується на управлінні мережею. Це дозволяє їхньому внутрішньому IT-відділу зосередитися на спеціальних проектах та впроваджувати інновації, які допомагають бізнесу зростати. Передача на аутсорсинг спеціалісту часто є більш вигідною з точки зору витрат, і тоді цим процесом займаються досвідчені технічні працівники, які спеціалізуються на управлінні мережею та адмініструванні [19].

Існує п'ять функціональних областей мережевого управління. Це визначено ISO, Міжнародною організацією зі стандартизації. П'ятьма областями є [19]:

Управління несправностями. Управління несправностями – це процес виявлення та усунення будь-яких помилок у системі. Виявлено проблему, ідентифіковано джерело проблеми, проблему вирішено, а процес задокументовано.

Управління конфігурацією. Це процес моніторингу та підтримки пристроїв і конфігурацій мережі. Конфігурації можуть змінюватися з новими програмами та оновленнями, тому це потрібно постійно контролювати.

Управління продуктивністю. Керування продуктивністю відстежує роботу пристроїв і мережі. Коли пристрої працюють надто повільно, це може вказувати на те, що їх потрібно оновити, або на можливу проблему.

Управління безпекою. Управління безпекою охоплює багато речей і зростає. Існує багато інструментів, які допоможуть адміністратору мережі перевіряти інформацію та контролювати мережу для дотримання стандартів кібербезпеки.

Управління бухгалтерським обліком. Облік ще називають адмініструванням. Цей процес включає надання доступу або повноважень користувачам.

Найкращі методи керування мережами

Є кілька речей, про які треба знати, щоб створити середовище, у якому керування мережею можна виконувати оптимально. Мережа постійно змінюється. Це реальність технологій. Для бізнесу важливо додати нові технології, щоб забезпечити кращу конкуренцію. Це також означає, що мережа буде розвиватися, тому процес обслуговування мережі для керування нею має наслідувати її приклад.

Управління мережею сьогодні набагато складніше, ніж це було навіть десять років тому. Можна очікувати, що продовжиться додавання нових рівнів, а адміністраторам потрібно буде навчитися складнішим навичкам підтримувати мережу. Ось кілька практичних порад, про які варто пам’ятати. За потреби додавати до них:

Топологія мережі дуже важлива. Керівництво мережею має мати точну топологію мережі, тому що сьогодні просто занадто багато рухомих частин, щоб

працювати без детальної документації. Це також слід оновлювати кожного разу, коли нові пристрої підключаються до мережі. Один неврахований пристрій може створити вразливість безпеки, чого не можна допустити.

Бюджетування та потреба в проектуванні. MSP може працювати, щоб оцінити поточну мережу та допомогти заздалегідь спланувати розвиток бізнесу. Це найкращий спосіб спрогнозувати IT-витрати, але він також допоможе підтримувати здорову поточну мережеву інфраструктуру.

Протоколи керування мережею. Керування мережею має бути детально задокументовано, щоб кожне рішення та сценарій були вже продумані. Це найкращий спосіб спланувати, щоб уникнути помилок у надзвичайних ситуаціях і вирішити будь-які простої або проблеми з продуктивністю мережі.

Проблеми управління мережею. В управлінні мережею може виникнути багато проблем. Реальність така, що успіх керування мережею залежить від ретельного планування та розуміння індивідуальних бізнес-потреб. Вибір найкращих служб керування мережею для тісної співпраці з бізнесом допоможе швидко подолати труднощі, оскільки їхній досвід допоможе впоратися з проблемами за короткий проміжок часу. Потрібно враховувати багато мережевих компонентів. Найважливішим аспектом успішної стратегії управління є чітке документування всього та підтримка оновлених записів у будь-який час.

2.2 Ефективні стратегії управління мережею

Управління мережею компанії, що займається IT-інфраструктура, є складним завданням, яке вимагає правильних стратегій та інструментів для забезпечення безперебійної роботи. Управління мережею включає планування, моніторинг, усунення несправностей та обслуговування апаратного та програмного забезпечення.

Компанії повинні ефективно управляти своїми мережами, щоб максимізувати ефективність своєї діяльності і гарантувати, що їхні клієнти залишаються задоволені якістю їх послуг. Розглядаються п'ять стратегій

управління мережею, які компанії з IT-інфраструктури можуть використовувати для досягнення цих цілей.

1. *Автоматизація та централізація*. Однією з найважливіших стратегій компаній, що займаються IT-інфраструктурою, є автоматизація та централізація процесів управління мережею. Автоматизація дозволяє компаніям скоротити час і зусилля, необхідні для вирішення завдань управління мережею, і гарантувати, що дослідження виконуються послідовно і коректне. Автоматизація також дозволяє ефективніше використовувати ресурси, оскільки уроки можна виконувати з меншими витратами ресурсів. Централізація забезпечує єдину точку управління для всієї мережі, забезпечуючи більш ефективне управління мережею.

2. *Безпека та відповідність вимогам*. Безпека та відповідність необхідні для ефективного управління мережею в сучасному світі, який стає все більш цифровим. Компанії повинні забезпечити безпеку своїх мереж і відповідність галузевим нормам і стандартам. Вони повинні вживати належних заходів для захисту своїх мереж від кіберзагроз та дотримуватися відповідних законів та нормативних актів. Компанії також можуть використовувати інструменти безпеки та відповідності для виявлення загроз та моніторингу своїх мереж.

3. *Моніторинг та усунення несправностей*. Усунення несправностей та моніторинг є важливими компонентами управління мережею. Компанії можуть виявляти та виправляти проблеми, як тільки вони виникають, за допомогою моніторингу в режимі реального часу. Усунення несправностей вимагає від компаній інструментів та досвіду для їх вирішення.

4. *Планування пропускної здатності*. Процес планування пропускної здатності включає оцінку поточних та майбутніх потреб Інтернету, а також наявних ресурсів та обладнання. Компаніям також слід розглянути можливість вжиття заходів для забезпечення того, щоб мережа могла впоратися з майбутніми змінами, такими як нове обладнання або програмне забезпечення.

5. *Оптимізація продуктивності*. Оптимізація продуктивності спрямована на забезпечення максимально ефективної роботи мережі. Компаніям потрібно визначити потенційні вузькі місця у своїй мережі та вжити заходів для їх

усунення. Частиною цього процесу може бути оптимізація Інтернету для конкретних додатків або служб, зменшення затримки та покращення пропускної здатності.

Для того, щоб випереджати конкурентів у компаніях, які займаються IT-інфраструктурою, потрібні ефективні стратегії управління мережею. Обговорювалося п’ять стратегій керування мережею для досягнення максимальної ефективності та задоволення клієнтів. Вони включають автоматизацію та централізацію, безпеку та відповідність вимогам, моніторинг та усунення несправностей, планування потужностей та оптимізацію продуктивності. IT-інфраструктурні компанії можуть забезпечити ефективну та безпечну роботу своїх мереж.

Управління мережею - це процес організації мережевого трафіку та потоків даних у корпоративній екосистемі за допомогою моніторингу мережі, безпеки мережі, автоматизації мережі та інших інструментів, розміщених локально або в хмарі.

Основною метою управління мережею є забезпечення безпечної, надійної та високопродуктивної мережі кінцевим користувачам, включаючи бізнес-користувачів на підприємстві та кінцевих клієнтів. Управління мережею завжди було важливою частиною списку IT-завдань. Розподілені компанії в першу чергу покладаються на управління мережею, щоб підтримувати зв'язок між різними корпоративними функціями та командами. Управління мережею також відповідає за управління потоками даних, що надходять і виходять з різних середовищ хостингу, таких як локальні сервери, приватні хмари та загальнодоступні хмарні платформи.

За даними міжнародної організації зі стандартизації, існує п'ять типів управління мережею, які відповідають за весь спектр процесів, пов'язаних з мережею. Ці типи включають управління збоями, конфігурацією, обліком, продуктивністю та безпекою, які зазвичай називають fcaps. Давайте розглянемо, що тягне за собою управління мережею.

Управління мережевими збоями: Можна мати призначену групу з керування мережевими збоями для передбачення, виявлення та усунення збоїв у мережі, щоб мінімізувати час простою. Окрім усунення несправностей, ця функція відповідає за реєстрацію інформації про несправності, ведення записів, проведення аналізу та допомогу в регулярних аудитах.

Потрібні чіткі канали, щоб команда керування мережевими помилками могла звітувати адміністратору мережі для забезпечення прозорості. Він також буде тісно співпрацювати з кінцевим користувачем, якщо він повідомить про помилки.

Керування конфігурацією мережі: конфігурація мережі є ключовим аспектом продуктивності. Очікується, що ці конфігурації змінюватимуться динамічно, щоб відповідати потребам даних і трафіку у великому підприємстві. Прикладом завдання керування конфігурацією мережі є IT-спеціаліст, який віддалено змінює параметри підключення для підвищення продуктивності.

Управління конфігурацією мережі значною мірою залежить від автоматизації, тому команді не потрібно вручну шукати вимоги до конфігурації, а натомість може автоматично вносити зміни. Подібно до керування несправностями мережі, команда керування конфігурацією мережі також повинна вести детальні записи про всі зміни, їхні результати та проблеми, якщо такі є.

Облік мережі та керування використанням: у міру того, як вимоги до мережі змінюватимуться, співробітники споживатимуть більше мережевих ресурсів і збільшуватимуть витрати підприємства. Команда управління мережевим обліком контролює використання, знаходить аномалії та відстежує тенденції використання для різних відділів, бізнес-функцій, офісів, онлайн-продуктів або навіть окремих користувачів.

У деяких компаніях керування мережевим обліком безпосередньо пов’язане з прибутковістю. Фірмам електронної комерції може знадобитися відстежувати використання мережі та порівнювати прибутковість у періоди піку та затишшя. На великих підприємствах управління мережевим обліком — це організація

спільного обслуговування, яка здає в оренду мережеві ресурси різним філіям і дочірнім компаніям для підтримки внутрішньої норми прибутку.

Керування продуктивністю мережі: це один із найважливіших аспектів керування мережею. Керування продуктивністю мережі включає різні завдання, які допомагають збільшити час безвідмовної роботи мережі, доступність послуг і одночасну швидкість пропускної здатності. Тут також важливу роль відіграє автоматизація.

Окрема інформаційна панель підключена до різних мережевих компонентів, які відстежують KPI продуктивності та подають сповіщення, якщо порогове значення перевищено. Команда керування продуктивністю мережі може захотіти відобразити час відповіді мережі 24/7, щоб уникнути впливу на роботу кінцевого користувача. У разі виникнення аномалії команда керування продуктивністю мережі тісно співпрацюватиме з командою керування мережевими збоями, щоб вирішити цю проблему.

Управління мережевою безпекою: оскільки більшість корпоративних процесів переходять в режим онлайн, безпека мережі є життєво важливою для стійкості, управління ризиками та успіху.

Під час DDOS-атаки кілька підключених онлайн-пристроїв націлюються на корпоративний веб-сайт із підробленим трафіком, щоб блокувати законний трафік. Управління безпекою мережі передбачає захист системи від цих та інших проблем. Корпоративна мережа також генерує регулярний потік журналів, які аналізуються групою керування безпекою мережі, щоб знайти будь-які відбитки пальців загрози.

Залежно від розміру та характеру бізнесу, у вас можуть бути призначені команди або персонал, відповідальний за всі види управління мережею. Велике, розподілене та багатонаціональне підприємство, як правило, має команду, призначену для кожного виду діяльності. Конкретні бізнес-підрозділи могли б створювати команди для одного типу мережевого управління і групувати інші в рамках загальної функції.

За останні кілька років важливість управління мережею неухильно зростала, як і пов'язані з нею проблеми. У звіті Enterprise Management Associates "Мегатренди мережевого управління 2020" було виявлено, що кожна третя проблема виявляється кінцевими користувачами і повідомляється про неї до того, як команда мережевого управління дізнається про них. Фрагментація інструментарію управління мережею також викликає занепокоєння: 64% підприємств використовують 4-10 інструментів для усунення несправностей у своїх мережах.

Надійна функція управління мережею може допомогти вирішити ці проблеми, одночасно контролюючи витрати на мережу та підвищуючи продуктивність для підтримки бізнесу. Для досягнення цієї мети команди управління мережею покладаються на набір окремих компонентів.

Управління мережею використовує багато підключених компонентів для виконання операцій. До них відносяться:

1. *Підключення кінцевої точки*. Основним призначенням мережевої інфраструктури є підключення кінцевих точок підприємства. Це можуть бути локальні робочі станції, кіоски в лобі та системи конференц-залів. Це також може включати розподілену систему, яка допомагає об’єднати віддалених співробітників і численні філії. Тип кінцевої точки також залежить від бізнес-потреб. Управління мережею допомагає забезпечити постійне підключення необхідних кінцевих вузлів, а мережеві адміністратори мають змогу в реальному часі бачити продуктивність кожного вузла. IT-команди також можуть використовувати інструменти централізованого моніторингу мережі, щоб контролювати підключення кінцевої точки одного інтерфейсу для розподілених місць.

2. *Системи журналювання*. Системи ведення журналів є важливим компонентом керування мережею, оскільки вони допомагають відстежувати продуктивність мережі відповідно до галузевих стандартів KPI та підтримувати вичерпні записи. Системи реєстрації підключаються як до мережевих апаратних пристроїв, так і до програмних компонентів. У міру використання цих апаратних і

програмних засобів система журналювання записуватиме всі дії для подальшого використання. Одним із найпопулярніших механізмів реєстрації мережевого керування є повсюдна опція Syslog — протокол, який дозволяє генерувати та зберігати записи для всіх мережевих подій у форматі даних. Але це, само по собі, мало користі. Ось чому сучасне керування мережею поєднує системи реєстрації з мережевою аналітикою, щоб могли візуалізувати дані, виявляти тенденції та отримувати сповіщення про аномалії.

3. *Автоматизація мережі.* Автоматизація мережі зменшує ручні зусилля, пов’язані з п’ятьма різними типами керування мережею. Це може допомогти автоматично вилікувати поширені проблеми на основі заздалегідь визначеного протоколу для керування мережевими збоями. Для керування конфігурацією мережі автоматизація може допомогти в автоматичному підключенні нових користувачів. Для керування мережевими обліковими записами це може допомогти автоматично запровадити заходи щодо скорочення витрат, якщо перевищено певні порогові значення. Він може автоматично коригувати політики додатків для керування продуктивністю мережі для підтримки бізнесу. Автоматизація дозволяє дізнаватися про різні типи загроз і знаходити їх з мінімальним ручним втручанням для керування безпекою мережі.

4. *Підключення до сервера.* Компонент підключення до сервера керування мережею стежить за станом підключення пристроїв, які не є кінцевими користувачами. Якщо підприємство покладається на віртуальні машини або серію приватних серверів для забезпечення процесів, пов’язаних із програмами, їх потрібно підтримувати онлайн. Керування мережею має забезпечити максимальний час безперебійної роботи серверних пристроїв, як і кінцевих точок. Це може бути проблемою, оскільки проблеми з сервером може бути складніше виявити, і проблема стає очевидною лише після того, як вона поширюється на підприємство. Ось чому більшість груп керування мережею використовують інструменти моніторингу мережі, специфічні для сервера, для підтримки та керування цим компонентом.

5. *Управління комутаторами*. Мережеві комутатори – це апаратні пристрої, які допомагають підключити кінцеві пристрої до основної корпоративної мережі, одночасно забезпечуючи необхідні IT-протоколи. Компанії можуть використовувати кілька рівнів мережевих комутаторів, починаючи від поверхових комутаторів і закінчуючи агрегаційними комутаторами та центральним розподільним пристроєм. Управління комутаторами дає змогу бачити трафік, що надходить до комутаторів і виходить із них, щоб могли діагностувати проблеми, пов'язані з передаванням, забезпечувати постійну швидкість і передбачати вузькі місця. Сьогодні компонент керування комутаторами став дуже складним. Це дозволяє контролювати та оркеструвати складні ландшафти за допомогою програмного забезпечення для керування комутаторами. Це допомагає створити візуальний план приміщення корпоративного середовища та керувати комутаторами, підключеними до кінцевих пристроїв.

6. *Гарантія мережі*. Компонент безпеки мережі в управлінні мережею передбачає застосування політики для контролю ризиків, забезпечення внутрішньої відповідності та захисту від загроз безпеці. Метою забезпечення безпеки мережі є забезпечення безпечного та надійного досвіду для всіх користувачів. Ось чому для безперебійної роботи цей компонент потребує взаємодії між усіма п'ятьма типами керування мережею. Крім того, мережеве забезпечення використовує аналітику як ключовий компонент для моніторингу динамічних рівнів ризику та сповіщення необхідних зацікавлених сторін до того, як може виникнути серйозна проблема. Зрештою, усі ці компоненти є частиною тристоронньої архітектури керування мережею, яка включає керуючий об'єкт, керований пристрій і протокол керування. Керуючий суб'єкт складається з людей і технологій, відповідальних за управління ландшафтом – IT-адміністратор або сценарій автоматизації. Керований пристрій знаходиться на приймальній стороні підключення до мережі, як-от кінцеві точки, комутатори та сервери. Протоколи керування відносяться до посередницьких правил і політик, які регулюють відносини між керуючим об'єктом і керованим пристроєм.

Ефективне управління мережею може забезпечити конкурентну перевагу для бізнесу. Ось десять найкращих практик, які потрібно впровадити у 2024 році:

1. *Регулярно проводите інвентаризацію ландшафту мережі*. Може бути важко досягти наскрізної видимості мережі в складному корпоративному середовищі. Недавнє опитування під назвою Network Field Report 2021, проведене Auvik Networks, показало, що 56% IT-спеціалістів не мають повних знань про те, як налаштована їх мережа. Це пояснюється тим, що підприємства постійно додають нові компоненти, апаратні пристрої, комутатори, кінцеві точки тощо до своєї мережі, не завжди проводячи інвентаризацію між ними. Важливо підтримувати оновлений каталог мережі, щоб керувати принципами керування мережею та запроваджувати правильні політики.

2. *Стратегічно використовувати апаратні та програмні інструменти*. Традиційні мережеві середовища були в основному апаратними. У вас було кілька кінцевих точок, комутаторів і серверів, якими керували за допомогою складних ручних і апаратних механізмів. Сьогодні прогрес у програмно-визначених мережевих технологіях дозволяє мінімізувати людські зусилля та забезпечити стандартизацію. Підприємства можуть поєднувати фізичні та програмні брандмауери, фізичні точки доступу, програмне керування мережею та різні інші інструменти для оптимізації роботи.

3. *Оновлюйте топологію мережі після кожної організаційної зміни*. Топологія мережі стосується розташування різноманітних пристроїв, мережевого обладнання, програмного забезпечення та компонентів керування мережею у корпоративному ландшафті. Коли організація змінюється, вона додаватиме нові елементи на цю карту. Однак стара топологія не завжди може бути найкращим способом керування цим нещодавно вдосконаленим ландшафтом. Рекомендується оновлювати топологію мережі після значних змін і регулярно кожні п’ять років.

4. *Ведіть детальну документацію для всіх протоколів керування мережею*. Мережа є основою сучасного підприємства, але керування мережею може ускладнитися, якщо у IT-команді зміниться ресурс. Початковий адміністратор, який створив топологію та її необхідні протоколи, може більше

бути недоступним. У таких сценаріях доведеться пройти повний ремонт керування мережею та, можливо, понести додаткові витрати. Цього можна уникнути за допомогою детальної документації. Задокументувавши конфігурації, політики безпеки та архітектурні структури, підприємства можуть гарантувати, що поточні методи керування мережею залишатимуться придатними для повторного використання з часом.

5. *Завжди вибирайте програмне забезпечення, що не залежить від OEM.* Підприємствам слід переконатися, що їх програмне забезпечення для керування мережею не є упередженим до одного чи кількох вибраних виробників оригінального обладнання (OEM). Програмне забезпечення, розроблене лише для одного варіанту мережевого обладнання, може призвести до блокування постачальника в довгостроковій перспективі. Підприємствам буде важко диверсифікувати свої IT-інвестиції, досліджувати альтернативи та змінюватись, якщо це необхідно. Запобігання цьому це вибравши інструменти керування мережею, які не залежать від OEM.

6. *Робота з MSP на стадії високого росту.* Ця найкраща практика керування мережею застосовна для постачальників цифрових послуг і стартапів, що розвиваються. За таких сценаріїв попит на мережу, ймовірно, перевищить внутрішні можливості IT, що спричинить часті простої та ризики для безпеки. Постачальник керованих послуг (MSP) діятиме як сторонній партнер, який може віддалено керувати оркестровкою мережі та надавати підтримку на місці. MSP можуть допомогти в проектуванні та реалізації мережі, а також у плановому обслуговуванні, перевірках безпеки та зміні конфігурації.

7. *Зверніться до регуляторних органів, щоб дізнатися, які стандарти відповідності застосовуються.* Дані, що надходять у мережу, можуть регулюватися галузевими або місцевими законами та регулятивними стандартами. Обмін медичними та фінансовими даними регулюється Законом про перенесення та підзвітність медичного страхування (HIPAA) і Комісією з цінних паперів і бірж (SEC), а також правилами США Стандарт безпеки даних індустрії платіжних карток (PCI DSS) також вимагає певних мережеві вимоги, такі як сегментація та

контроль доступу, щоб підприємства залишалися сумісними. Поговоріть з експертом із регулювання, перш ніж планувати методи керування мережею та відповідним чином розробляти архітектуру.

8. *Інтегруйте інструменти керування мережею, щоб уникнути фрагментації.* Фрагментація інструментарію є однією з найпоширеніших проблем, з якими стикаються під час керування мережею. Протистояти цьому це об'єднання кілька інструментів і джерел даних для подачі в єдиний інтерфейс. Технології керування мережею, повинні мати інтерфейси прикладного програмування (API) або мати відкриту архітектуру, щоб забезпечити бездоганну інтеграцію.

9. *Переконайтеся, що існують механізми відновлення після відмови на випадок непередбачуваного простою.* Навіть коли є прагнення досягти оптимальної продуктивності, важливо підготуватися до найгірших сценаріїв. Що відбувається, коли з'єднання з мережею порушується через стихійні лиха, геополітичні події чи стихійні лиха? Чи можна отримати доступ до інструментів моніторингу мережі та вирішення інцидентів, якщо вони розміщені в тій самій мережі, яка зараз не працює? Ось чому підприємствам потрібен механізм відновлення після відмови, який активується, коли основна мережа недоступна. Розміщення свого інструментарію керування мережею в окремій, незалежно керованій приватній мережі. Також можна інвестувати в інфраструктуру резервного підключення, щоб додати резервування.

10. Автоматизуйте процеси, де це можливо

Нарешті, автоматизація повинна стати головним пріоритетом для управління мережею в 2021 році. В опитуванні Net DevOps 2020, спонсорованому Red Hat, було виявлено, що підприємства вибирають автоматизувати в середньому 4,19 завдань керування мережею, причому максимальна автоматизація відбувається в управлінні конфігурацією. Однак є й інші можливості, які можна отримати це: ініціалізація користувачів, відображення топології, оновлення програмного забезпечення, виявлення аномалій тощо.

Використовуючи автоматизацію мережі, можна використовувати ці можливості та зменшити як внутрішні зусилля, так і витрати на MSP.

2.3 Загальні особливості застосування Windows Server 2022

Windows Server 2022 базується на надійній базі Windows Server 2019. І цього разу він зосереджений на трьох ключових елементах, зокрема безпеці, гібридній інтеграції та управлінні Azure і платформі додатків. Крім того, Windows Server 2022 Datacenter Azure Edition допоможе використовувати переваги хмари та скоротити час простою. Він містить багато нових функцій, які підвищать безпеку та загальну продуктивність [24].

Ось нові функції, на які варто звернути увагу в Windows Server 2022 [24]: Безпека, Гібридні можливості Azure, Платформа додатків, Вкладена віртуалізація для процесорів AMD, Браузер Microsoft Edge, Зберігання, Безпека.

Безпека була в центрі уваги в останніх збірках Windows, як і у випадку з Windows Server 2022. Він об’єднав можливості безпеки в Windows Server, а також підтримує багаторівневу безпеку для забезпечення механізму активного захисту від розширених загроз і атак. Ось дві ключові функції безпеки, які можна очікувати в Windows Server 2022 [24]: Безпечне підключення, Захищений базовий сервер

Безпечне з’єднання є обов’язковим і вкрай необхідним для серверів, особливо в сучасному світі, де щодня відбуваються нові кібератаки. Щоб забезпечити встановлення безпечних з’єднань, у Windows Server 2022 включено такі функції [24]:

HTTPS і TLS 1.3 увімкнено у Windows Server 2022 за замовчуванням. Найновішою версією протоколу безпеки в Інтернеті є Transport Layer Security (TLS) 1.3. Він забезпечує безпечний канал зв’язку між двома кінцевими точками шляхом шифрування даних. Тепер, увімкнувши HTPPS і TLS 1.3 у Windows Server 2022, він гарантує, що дані клієнтів, підключених до сервера, захищені.

Старіші криптографічні механізми відкидаються та використовуються нові алгоритми безпеки [24].

Захищений DNS — ще одна хороша розширена функція, яка забезпечує безпечне підключення. DNS-over-HTTPS (DoH) тепер підтримується DNS-клієнтом у Windows Server 2022. DoH шифрує DNS-запити за допомогою протоколу HTTPS і зберігає конфіденційність трафіку, що додатково підвищує безпеку. Крім того, через нього можна запобігти прослуховування [24].

Для шифрування та підпису серверних блоків повідомлень (SMB) у Windows Server тепер підтримуються криптографічні набори AES-256-GCM і AES-256-CCM. Надійне шифрування є необхідністю в обчисленнях, оскільки зловмисники продовжують знаходити нові способи зламати алгоритми безпеки. Використання пакетів AES-256-GCM і AES-256-CCM забезпечує вищий рівень шифрування. Хоча AES-128 для сумісності нижнього рівня все ще підтримується [24].

Для кластерних спільних томів (CSV) і рівня шини зберігання (SBL) буде жорстке й розширене шифрування та підписування внутрішньовузлових зв’язків зі сховищем, які підтримуватимуться відмовостійкими кластерами Windows Server. По суті, це означає, що тепер користувачі можуть шифрувати або підписувати комунікації схід-захід у самому кластері за допомогою Storage Spaces Direct [24].

У Windows Server 2022 Datacenter: Azure Edition і підтримуваних клієнтах Windows підтримується SMB через QUIC на додаток до TLS 1.3. Це гарантує, що користувачі та програми мають захищений доступ до даних із периферійних файлових серверів. Крім того, більше немає потреби у VPN для мобільних і дистанційних користувачів, щоб отримати доступ до своїх файлових серверів через SMB під час роботи в Windows [24].

Захищене базове обслуговування забезпечує додатковий рівень захисту від нових загроз і викликів. Він базується на трьох основних параметрах, а саме [24]: Спрощена безпека, Розширений захист, Превентивна оборона, Спрощена безпека.

Не буде складнощів у налаштуванні функцій безпеки захищених основних серверів. Можна легко налаштувати системи Windows Server з Центру адміністрування Windows [24].

Розширений захист

Оскільки захищені основні сервери повністю використовують апаратне забезпечення, вбудоване програмне забезпечення та можливості операційної системи, є покращений захист від поточних і майбутніх загроз. Він має широкий підхід у таких сферах, як [24]:

- Апаратний корінь довіри: Trusted Platform Module 2.0 (TPM 2.0) забезпечує використання безпечних основних серверів. Він забезпечує апаратний корінь довіри, що підвищує рівень безпеки, який забезпечують такі можливості, як BitLocker [24].
- Захист вбудованого програмного забезпечення: оскільки мікропрограмне забезпечення працює з вищими привілеями та пов’язано багато вразливостей у безпеці, покращення захисту мікропрограмного забезпечення є актуальною потребою. Такі функції, як технологія Dynamic Root of Trust of Measurement (DRTM), захист DMA, системи Secured-core, можуть забезпечити захист вбудованого програмного забезпечення [24].
- Безпека на основі віртуалізації (VBS): VBS і цілісність коду на основі гіпервізора (HVCI) підтримуються захищеними основними серверами [24].

Превентивна оборона

Захищені основні сервери завчасно захищають систему від зловмисників [24].

1) Гібридні можливості Azure

Вбудовані гібридні можливості Azure на Windows Server 2022 дозволяють використовувати Azure ефективніше. Ось нові функції гібридної інтеграції та керування Azure в Windows Server 2022 [24,30]:

1) Windows Server із підтримкою Azure Arc — це вдосконалена функція, якої варто очікувати. Якщо гібридна машина підключена до Azure, вона обслуговується як ресурс у Azure [24, 30].

2) Нові вдосконалення центру адміністрування Windows роблять керування Windows Server 2022 ефективнішим і простішим [24, 30].

3) Hotpatch, який є частиною Azure Automanage, тепер підтримується в Windows Server 2022. По суті, це новий метод, який дозволяє користувачам інсталювати оновлення на нових віртуальних машинах (VM) Windows Server Azure Edition. І навіть не потребує перезавантаження після встановлення [24, 30].

2) Платформа додатків

Для Windows Server 2022 є різні вдосконалення платформи для контейнерів Windows. Одним із значних удосконалень є те, що розмір зображення контейнера Windows зменшено на 40 відсотків. Це призведе до швидшого часу запуску та кращої загальної продуктивності [24, 30].

Тепер можна запускати програми, що залежать від Azure Active Directory, за допомогою групових облікових записів керованих служб (gMSA). І для цього навіть не потрібне приєднання домену до хосту контейнера. Крім того, контейнери Windows пропонують підтримку MSDTC та MSMQ [24, 30].

Робота з Windows Container із Kubernetes також спрощена завдяки кільком удосконаленням. Контейнери хост-процесів для конфігурації вузла, IPv6 і послідовної реалізації мережевої політики з Calico [24, 30].

Підтримка Windows Server 2022 для процесорів компанії Intel покоління Ice Lake дозволяє пропонувати підтримку критично важливих для бізнесу та великомасштабних програм. Крім того, розширення SGX на поколінні Ice Lake додатково підвищує безпеку додатків завдяки захищеній пам’яті [24, 30] .

3) Віртуалізація для процесорів від компанії AMD

Windows Server 2022 підтримує функцію вкладеної віртуалізації за допомогою процесорів AMD. Вкладена функція віртуалізації дозволяє користувачам запускати гіпервізор Hyper-V на віртуальній машині. Він пропонує більше варіантів апаратного забезпечення для оточення [24, 30].

4) Інтернет-браузер Microsoft Edge

Браузер Explorer тепер замінено на Microsoft Edge у новій Windows Server 2022. Новий Microsoft Edge побудовано на основі вихідного коду Chromium і має

нові та вдосконалені функції безпеки. Тепер користувачі можуть використовувати Microsoft Edge із серверним ядром або сервером разом із параметрами встановлення Desktop Experience [24, 30].

5) Зберігання

У Windows Server 2022 є кілька нових функцій, пов’язаних зі сховищем, зокрема [24, 30] :

1. Служба міграції сховища
2. Регульована швидкість ремонту зберігання
3. Кеш шини зберігання з просторами зберігання на автономних серверах
4. Стиснення SMB

Служба міграції сховища

Міграція сховища з вихідних місць на сервер Windows або Azure тепер стала простішою завдяки різноманітним удосконаленням служби міграції сховища. Можнперенести локальних користувачів і групи на новий сервер, перенести сховище до або з відмовостійких кластерів, а також автономних серверів і відмовостійких кластерів тощо. Це навіть дозволяє перенести сховище з серверів на базі Linux з допомогою набору програм Samba [24, 30] .

Регульована швидкість ремонту зберігання

Нова функція в якій користувач може регулювати швидкість відновлення сховища. в Storage Spaces Direct забезпечує більший контроль над процесом повторної синхронізації даних. Це призводить до підвищення доступності, гнучкості та ефективності [24, 30].

Кеш шини зберігання з просторами зберігання на автономних серверах

Для автономних серверів тепер доступний кеш шини зберігання. Це покращує продуктивність читання та запису. Однак ефективність зберігання зберігається, а експлуатаційні витрати залишаються низькими [24, 30].

Звуження SMB

Для серверної операційної системи Windows Server 2022 удосконалено можливості стиснення SMB. Це усуває необхідність ручного архівування файлів,

дозволяючи користувачу або програмі стискати файли під час їх передачі через мережу [24, 30].

2.3.1 Особливості застосування Windows Server 2022 для корпоративної мережі

Серверна операційна система Windows Server 2022 - це остання версія флагманської серверної операційної системи Microsoft, що пропонує широкий вибір функцій і можливості для призначених для задоволення вимог сучасних корпоративних мереж. Він забезпечує надійну і безпечну основу для широкого спектру робочих навантажень, від традиційного обміну файлами і друком до просунутих хмарних додатків [24, 30].

Графічна оболонка серверної операційної системи Windows Server 2022 надана на Рис.2.1

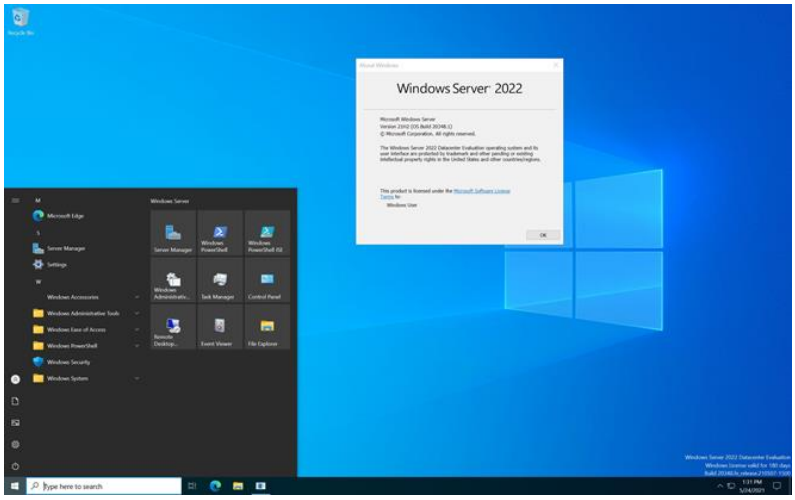


Рисунок 2.1 – Графічна оболонка Windows Server 2022 [61]

Підвищена безпека

Windows Server 2022 надає багато нових функцій. і покращених функцій безпеки, які можуть допомогти організаціям захистити свої корпоративні мережі. Ці функції можна використовувати для захисту від широкого спектру загроз, зокрема шкідливих програм, програм-вимагачів і фішингових атак [24, 30].

Деякі з найважливіших удосконалень безпеки Windows Server 2022 включають [24, 30]:

- Безпека на основі підтримуваного певного заліза: Windows Server 2022 представляє низку нових функцій безпеки на основі апаратного забезпечення, таких як наявність модуля TPM 2.0 і SEV. Ці функції можуть допомогти захистити від атак, націлених на мікропрограмне або апаратне забезпечення сервера [33, 34, 35].
- Безпека на основі софту: Серверна операційна система Windows Server 2022 включає низку нових функцій безпеки на основі програмного забезпечення [33, 34, 35].
- Система управління на основі ідентифікації та доступом: Windows Server 2022 забезпечує низку нових функцій керування ідентифікацією та доступом (IAM), умовний доступ до хмарної служби управління ідентифікацією та доступом, яка може допомогти контролювати, хто може отримати доступ до корпоративних ресурсів [33, 34, 35].
- Захист від загроз: Windows Server 2022 пропонує низку нових функцій захисту від загроз, таких як мережевий захисник Windows із інтелектуальною безпекою мережі (INS), який може допомогти захистити від мережевих атак [33, 34, 35].

Окрім цих загальних методів захисту, Windows Server 2022 також включає ряд функцій безпеки для окремих підрозділів, які можуть допомогти захистити певні типи корпоративних мереж. Windows Server 2022 має ряд нових функцій безпеки для таких типів мереж [33, 34, 35]:

- Сервер керування домену: Сервер каталогу AD є серцем домену Active Directory, тому вони є основною мішенню для атак. Windows Server 2022 включає низку нових функцій безпеки для контролерів домену, таких як розширений захист від крадіжки облікових даних і атак на підвищення привілеїв [33, 34, 35].
- Файловий сервер: файловий сервер використовується для зберігання корпоративних даних, і тому вони є ще однією головною ціллю для ударів. Windows Server 2022 підтримує низку нових функцій безпеки для файлових серверів [33, 34, 35].

- Веб-сервер: Сервер, який забезпечує доступ до веб-ресурсів використовуються для розміщення корпоративних веб-сайтів, тому вони є ще однією головною мішенню для ударів. Windows Server 2022 містить низку нових функцій безпеки для веб-серверів, таких як захист від шкідливого коду на веб-сайтах [33, 34, 35].

Windows Server 2022 включає нові і розширених функцій безпеки, які можуть допомогти організаціям захистити свої корпоративні мережі. Ці функції можна використовувати для захисту від широкого спектру загроз, зокрема шкідливих програм, програм-вимагачів і фішингових атак. Організаціям слід розглянути можливість використання Windows Server 2022, щоб скористатися цими новими функціями безпеки [33, 34, 35].

Покращена продуктивність та масштабованість

Windows Server 2022 оснащена значними покращеннями продуктивності та масштабованості для функцій розподілу корпоративних мереж. Ці вдосконалення задовольняють зростаючі вимоги сучасного бізнесу та дозволяють організаціям ефективно керувати своєю IT-інфраструктурою для підтримки збільшення робочого навантаження та збільшення бази користувачів [33, 34, 35].

Покращена масштабованість для великомасштабних розгортань: Windows Server 2022 може підтримувати масштабування до 48 ТБ пам’яті та 2048 логічних процесорів, що дозволяє організаціям масштабувати свою серверну інфраструктуру для роботи з ресурсомісткими програмами та справлятися зі зростаючими навантаженнями. Ця масштабованість особливо корисна для підприємств, які швидко розвиваються або працюють у динамічному середовищі [33, 34, 35].

Покращена щільність емуляції фізичної машини на програмному рівні: у Windows Server 2022 пропонує кілька оптимізацій, які покращують продуктивність і щільність віртуальних машин на сервері. Це включає вдосконалення гіпервізора, підсистеми зберігання та мережевого стеку, що дозволяє організаціям запускати більше віртуальних машин на сервер,

зменшуючи вимоги до обладнання та оптимізуючи використання ресурсів [33, 34, 35].

Зменшена затримка для покращення взаємодії з користувачем: Windows Server 2022 пропонує такі можливості як різні оптимізації, які мінімізують затримку та підвищують продуктивність мережі. Сюди входять такі функції, як TCP FastOpen і Reduced Packet Size, які скорочують час зворотного зв’язку та покращують реакцію програми. Ці оптимізації особливо корисні для додатків у реальному часі та робочих навантажень, які потребують низької затримки [33, 34, 35].

Підвищена продуктивність зберігання за допомогою мережевого сховища: Windows Server 2022 включає такі вдосконалення Storage Spaces Direct, програмно визначеного рішення для зберігання, яке дає змогу створювати високодоступні та масштабовані пули зберігання даних із звичайного обладнання. Ці вдосконалення включають покращену продуктивність до доступу даних, а також підтримку великих конфігурацій кластера [33, 34, 35].

Підвищена продуктивність мережі за допомогою QUIC і прямий доступ до пам'яті через SMB: Windows Server 2022 містить протокол QUIC, новий транспортний протокол, створений на основі UDP, який пропонує покращену продуктивність і меншу затримку порівняно з TCP для певних типів трафіку. Крім того, SMB Direct забезпечує прямий зв’язок між серверами без залучення мережевого стеку, ще більше підвищуючи продуктивність передачі файлів [33, 34, 35].

Покращена продуктивність для віддаленого доступу: Windows Server 2022 відображає SMB Direct через QUIC, нову функцію, яка дозволяє користувачам віддалено копіювати файли без потреби VPN, використовуючи протокол QUIC для швидшої та безпечнішої передачі файлів. Це особливо корисно для організацій із віддаленими працівниками або філіями [31, 32].

Покращена продуктивність для мережевих адаптерів із підтримкою RDMA: Ця функція в Windows Server 2022 може підвищити продуктивність мережевих адаптерів що підтримують прямий віддалений доступ до пам’яті (RDMA), які

дозволяють здійснювати прямий зв’язок між серверами пам’ять-пам’ять, минаючи ЦП і зменшуючи затримку. Це вдосконалення особливо корисно для робочих навантажень високопродуктивних обчислень (HPC) і програм, які вимагають низької затримки передачі даних [31, 32].

Спрощене управління та автоматизація

У Windows Server 2022 присутня низка нових функцій і вдосконалень, призначених для спрощення завдань керування й автоматизації для IT-адміністраторів. Ці функції допомагають скоротити необхідний час, необхідні для керування складним IT-середовищем, підвищити ефективність і зменшити ризик людської помилки [31, 32].

Центр адміністрування Windows

Центр адміністрування Windows — це веб-інструмент, який надає централізовану платформу для керування серверами Windows Server 2022. WAC Windows містить широкий спектр можливостей, як-от [31, 32]:

- Керування сервером: керуйте серверами, включаючи встановлення ролей і функцій, налаштування мережі та керування сховищем [31, 32].
- Моніторинг: відстежуйте продуктивність і працездатність сервера, включаючи використання ЦП, пам’яті та диска [31, 32].
- Усунення несправностей: вирішуйте проблеми сервера, включаючи перегляд журналів подій і виконання діагностики [31, 32].

Azure Arc

Azure Arc — це інструмент, який дозволяє IT-адміністраторам керувати серверами Windows Server 2022 незалежно від того, чи працюють вони локально, у хмарі чи на периферії. Azure Arc забезпечує узгоджений досвід керування всіма серверами, незалежно від їх розташування [31, 32].

З Azure Arc IT-адміністратори можуть [31, 32]:

- Інвентаризуйте та керуйте своїми серверами Windows Server 2022 незалежно від їх розташування [31, 32].
- Застосуйте політики та конфігурації до своїх серверів, щоб забезпечити відповідність і безпеку [31, 32].

- Слідкуйте за справністю та продуктивністю своїх серверів [31, 32].
- Автоматизуйте завдання, такі як виправлення та оновлення [31, 32].

Azure Arc може допомогти IT-адміністраторам спростити керування середовищами Windows Server 2022 і зменшити ризик помилок [31, 32].

Конфігурація бажаного стану (DSC)

DSC — це модуль PowerShell, який дозволяє IT-адміністраторам визначати бажаний стан своїх інфраструктурних ресурсів. Потім DSC може автоматично застосувати потрібний стан до ресурсів, гарантуючи, що вони завжди перебувають у потрібному стані [31, 32].

DSC можна використовувати для автоматизації широкого кола завдань, таких як [31, 32]:

- Конфігураційне налаштування серверів, включаючи встановлення ролей і функцій, налаштування мережі та керування сховищем [31, 32].
- Розгортання програм і керування ними [31, 32].
- Забезпечення політики безпеки [31, 32].

DSC може допомогти IT-адміністраторам автоматизувати складні завдання та зменшити ризик людської помилки [31, 32].

Windows PowerShell

Оболонка PowerShell — це потужна скриптова мова, що використовується для автоматизації широкого кола завдань у серверній системі Windows Server 2022. Інструмент PowerShell — це засіб, який можна використовувати для автоматизації таких завдань, як [31, 32]:

- Керування серверами, включаючи встановлення ролей і функцій, налаштування мережі та керування сховищем [31, 32].
- Розгортання програм і керування ними [31, 32].
- Забезпечення політики безпеки [31, 32].

PowerShell може допомогти IT-адміністраторам автоматизувати завдання та зменшити ризик людської помилки [31, 32].

Повний набір можливостей

У Windows Server 2022 є багатий набір можливостей, які задовольняють широкий спектр корпоративних навантажень, включаючи [31, 32]:

1. Active Directory: основна служба управління ідентифікацією та доступом для мереж Windows, що забезпечує централізоване управління користувачами та групами, автентифікацію та авторизацію [31, 32].

2. DNS-сервер: Це служба, яка перетворює читабельні доменні імена в цифрові IP-адреси, зрозумілі комп'ютерам. Вона використовується для вирішення доменних імен, коли користувачі отримують доступ до веб-сайтів або інших ресурсів в Інтернеті [31, 32].

3. DHCP-сервер: Це мережева служба, яка автоматично призначає IP-адреси та інші параметри конфігурації мережі пристроям у корпоративній мережі. Це допомагає гарантувати, що всі пристрої в мережі можуть взаємодіяти один з одним [31, 32].

4. RRAS: Служба маршрутизації та віддаленого доступу (RRAS), яка дозволяє користувачам віддалено підключатися до корпоративної мережі. Це також дозволяє користувачам ділитися файлами та папками з іншими користувачами в мережі [31, 32].

5. Спільний доступ до файлів і друку: підтримує служби спільного доступу до файлів і друку для користувачів по всій корпоративній мережі, забезпечуючи безпечний і ефективний доступ до спільних ресурсів [31, 32].

6. Віртуалізація Hyper-V: дозволяє створювати та керувати віртуальними машинами, дозволяючи організаціям консолідувати кілька робочих навантажень на одному фізичному сервері.

7. Підтримка контейнеризації: підтримує контейнерні технології, такі як Docker та Kubernetes, дозволяючи організаціям розгортати та керувати контейнерними програмами.

8. Віддалений робочий стіл: надає можливості віддаленого доступу, дозволяючи користувачам підключатися до своїх робочих столів і додатків з будь-якої точки світу.

Windows Server 2022 пропонує привабливий набір функцій і можливостей, які роблять його ідеальним вибором для корпоративних мереж. Його підвищена безпека, продуктивність, спрощене управління, інтеграція з гібридною хмарою та повний набір функцій дозволяють організаціям відповідати вимогам сучасних IT-середовищ.

2.3.2 Особливості Windows Server 2022 з можливостями адміністрування корпоративної мережі

Особливості Windows Server 2022 можуть бути корисними для адміністрування корпоративної мережі в таких аспектах:

1. Планування та проектування мережі.

Windows Server 2022 включає в себе таку функцію, яка може бути корисна для планування та проектування мережі. До неї відноситься:

- Підтримка IPv6 - Windows Server 2022 підтримує IPv6, що дозволяє створювати мережі, які є більш масштабованими та стійкими.

2. Розгортання та налаштування мережі.

До складу Windows Server 2022 входять такі ролі та компоненти, необхідні для розгортання та налаштування корпоративної мережі:

- Active Directory - служба каталогів, яка забезпечує централізоване керування користувачами, групами та ресурсами мережі.
- DHCP – служба автоматичного призначення IP-адрес.
- DNS - служба доменних імен, яка забезпечує перетворення доменних імен на IP-адреси.

3. Управління мережею.

Windows Server 2022 включає такі функції для управління мережею:

- Служба маршрутизації та віддаленого доступу (Routing and Remote Access Service) - це служба, яка дозволяє серверу виконувати функції маршрутизатора та шлюзу.

- Служба DNS (Domain Name System) – це служба, яка відповідає за дозвіл доменних імен в IP-адреси.
- Служба DHCP (Dynamic Host Configuration Protocol) - це служба, яка надає IP-адреси та інші параметри мережі комп'ютерам у мережі.

4. Безпека мережі.

Таким чином Windows Server 2022 включає широкий набір функцій для забезпечення безпеки, включаючи:

- Windows Defender - вбудований антивірусний та антишпигунський пакет.
- Firewall – брандмауер для захисту мережі від несанкціонованого доступу.
- IPsec – протокол для забезпечення захищеного обміну даними.
- Віртуалізація - технологія, що дозволяє ізолювати віртуальні машини одна від одної.

Таким чином розглянути особливості Windows Server 2022, які можуть бути корисними для адміністрування корпоративної мережі в таких аспектах:

3 МОДЕЛЮВАННЯ ПРОЦЕСІВ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ ПІД ЧАС ЗАСТОСУВАННЯ WINDOWS SERVER 2022

Налаштування середовища моделювання мережі може бути складним завданням, але за допомогою EVE-ng воно стає набагато більш керованим. У цьому розглянути кроки для створення середовища мережевого моделювання та розглянемо його корисність при тестуванні, усуненні неполадок та вивченні мережевих концепцій. Середовище мережевого моделювання - це програмний інструмент, який дозволяє користувачам моделювати різні мережеві сценарії. Він забезпечує віртуальну платформу для тестування та аналізу продуктивності, поведінки та масштабованості мережевих систем. Завдяки мережевому моделюванню користувачі можуть експериментувати з різними мережевими конфігураціями, протоколами та обладнанням без необхідності фізичної реалізації. EVE-ng може бути використаний для моделювання поведінки великомасштабної мережі центрів обробки даних або тестування впливу мережевих вузьких місць на програми реального часу. Моделюючи реалістичні умови мережі, організації можуть приймати обґрунтовані рішення щодо своєї мережевої інфраструктури перед розгортанням.

Переваги використання EVEN для моделювання мережі

EVE-NG є цінним інструментом для моделювання мережі завдяки своїм численним перевагам.

По-перше, він забезпечує ідеальне середовище для тестування мережевих конфігурацій та усунення потенційних неполадок. Користувачі мають можливість створювати віртуальні мережі, які дуже нагадують сценарії реального життя, що дозволяє проводити точне моделювання та аналіз.

Крім того, EVEN g пропонує економічне рішення, яке усуває потребу в дорогому фізичному обладнанні. Це робить його високодоступним як для

приватних осіб, так і для організацій. Нарешті, зручний інтерфейс дозволяє мережевим інженерам різного рівня кваліфікації легко орієнтуватися в платформі і ефективно використовувати її. За допомогою EVEN користувачі можуть вдосконалити свої навички моделювання мереж та оптимізувати процеси розробки мереж.

Передумови

Щоб успішно орієнтуватися в світі мережевих середовищ моделювання, необхідна певна підготовка. Розуміння основ комп'ютерних мереж, включаючи протоколи та мережеві рівні, має вирішальне значення. Глибоке розуміння протоколів TCP/IP та Ethernet забезпечить міцну основу. Крім того, необхідні базові знання концепцій мережевої безпеки, таких як брандмауери та шифрування. Знайомство з технологіями віртуалізації також може бути корисним, оскільки дозволяє створювати багато віртуальних мереж для тестування та аналізу.

Установка

Установка є важливим кроком у налаштуванні середовища мережевого моделювання. Вона включає в себе підготовку необхідної інфраструктури та програмних компонентів для забезпечення безперебійної роботи. Одним із практичних прикладів є встановлення програмного забезпечення для віртуалізації, яке дозволяє одночасно запускати кілька операційних систем на одному комп'ютері. Іншим прикладом є конфігурація мережевих пристроїв, таких як Маршрутизатори та комутатори, для забезпечення зв'язку між модельованими мережевими вузлами. Крім того, процес встановлення може включати встановлення необхідних бібліотек або модулів для запуску середовища моделювання. Ці приклади підкреслюють важливість добре виконаного процесу встановлення для створення надійного та ефективного середовища моделювання мережі.

Створення мережевої топології

Створення мережевої топології є фундаментальним кроком у створенні надійного середовища мережевого моделювання. Вона дозволяє представляти і

аналізувати фізичну і логічну структуру мережі. Ретельно розробляючи топологію мережі, адміністратори можуть виявити потенційні вузькі місця, усунути неполадки та оптимізувати продуктивність мережі. Зіркоподібна топологія з'єднує кілька пристроїв з центральним вузлом, забезпечуючи ефективний зв'язок між пристроями. З іншого боку, сітчаста топологія забезпечує надмірність, з'єднуючи пристрої в мережеву структуру, забезпечуючи безперервне підключення, навіть якщо одне з'єднання виходить з ладу. Ці практичні приклади ілюструють важливість вибору відповідної топології мережі для середовища моделювання.

Налаштування пристроїв

Налаштування пристроїв в середовищі мережевого моделювання є фундаментальним завданням, що забезпечує безперебійне підключення і оптимальну продуктивність. Правильно налаштувавши пристрої, адміністратори мережі можуть точно налаштувати такі параметри, як IP-адреси, протоколи маршрутизації та функції безпеки. У модельованій мережі налаштування маршрутизаторів з відповідними IP-адресами забезпечує ефективну маршрутизацію даних між різними сегментами мережі. Крім того, налаштування віртуальних брандмауерів з необхідними правилами контролю доступу забезпечує безпечний зв'язок всередині модельованої мережі.

Середовище мережевого моделювання

Середовище мережевого моделювання є безцінним інструментом для підприємств і організацій для ефективного управління своїми мережами. Вона дозволяє тестувати і тиражувати сценарії реального світу без необхідності у фізичному обладнанні або дорогих інвестиціях. Адміністратори мережі можуть моделювати різні мережеві умови, такі як високий обсяг трафіку або збої в мережі, щоб оцінити продуктивність та стійкість своїх систем [36]. Крім того, середовище мережевого моделювання дозволяє організаціям перевіряти нові мережеві проекти або впроваджувати зміни, не порушуючи роботу своїх діючих мереж, забезпечуючи більш плавний перехід і скорочуючи потенційні простої. Цей практичний підхід до управління мережею сприяє більш ефективному

прийняттю рішень і може призвести до підвищення надійності та продуктивності мережі [36].

3.1 Методи мережевого моделювання

У дослідженнях комп'ютерних мереж мережеве моделювання - це метод, який дозволяє програмному забезпеченню моделювати роботу реальної мережі. Моделювання досягається на розрахунку взаємодій між різними пристроями, що є частинами мережі такими пристроями як: маршрутизаторами, комутаторами, вузлами та точками доступ, канали зв'язку і т.д. Більшість симуляторів моделюють систему як послідовність дискретних подій, при якому моделюються системи, в яких змінні стану змінюються в дискретні моменти часу. Потім у тестовій лабораторії можна спостерігати за поведінкою мережі та різних додатків та служб, які вона підтримує; різні атрибути середовища також можуть бути змінені контрольованим чином, щоб оцінити, як мережа/протоколи будуть поводитися в різних умовах [36].

Мережевий симулятор. Мережевий симулятор - це програмне забезпечення, яке може прогнозувати продуктивність комп'ютерної мережі або мережа з бездротовим зв'язком. Розвиток комунікаційних мереж призвів до їхньої надмірної складності, що ускладнює управління ними, щоб традиційні аналітичні методи могли точно зрозуміти поведінку системи, використовуються мережеві симулятори. У симуляторах комп'ютерну мережу можна уявити як систему, що складається з елементів, додатків і т.д., і повідомляється про продуктивність мережі [36]. Тренажери підтримують найпопулярніші технології і мережі, використовувані сьогодні, такі як п'яте покоління технології стільникового зв'язку, мережі, що об'єднують фізичні об'єкти, оснащені датчиками та іншими пристроями, WLAN, мережі, що створюються безпроводовими пристроями без використання базової станції, мережі, що складаються з датчиків, які збирають та обмінюються даними, взаємопов'язані мережі транспортних засобів, когнітивні радіомережі, LTE і т. д [36].

Моделювання. Більшість комерційних симуляторів керуються графічним інтерфейсом, тоді як деякі мережеві симулятори керуються CLI. Мережева модель / конфігурація описує мережу а також події. Вихідні результати будуть включати показники мережевого рівня, показники каналів, показники пристроїв і т.д. крім того, також будуть доступні файли трасування з докладним описом симуляцій. Файли трасування збирають дані про всі пакети та події, що відбулися в симуляціях, і використовуються для аналізу. Мережеві симулятори розбивають час на дискретні ітерації. У кожній ітерації симулятор обробляє одну подію з попереднього списку, причому деякі події запускають. Майбутні події — такі як прибуття пакета до вузла, що запускає подію прибуття цього пакета на низхідний вузол [36].

Мережева емуляція. Емуляція мережі дозволяє створювати тестові сценарії, які імітують реальні умови використання мереж, яка вносить зміни до потоку пакетів, щоб відтворити певну поведінку реальної мережі. Трафік в реальному часі може проходити через симулятор і піддаватися впливу об'єктів в рамках симуляції [36].

Типовий метод обробки реальних пакетів полягає в тому, що реальні пакети з реальної програми передаються на сервер емуляці. Реальний пакет "модулюється" в пакет моделювання. Імітаційний пакет демодулюється в реальний пакет після виникнення ефектів втрати, помилок, затримки, тремтіння і т.д., тим самим реалізуючи ці мережеві ефекти в реальному світі. Отже, це так, ніби реальний пакет проходить через реальну мережу, але насправді він проходить через мережу, яка імітує поведінку реальної мережі [36].

Емуляція дозволяє моделювати роботу системи в умовах на етапі проектування для перевірки комунікаційних мереж перед розгортанням [36].

Список мережевих симуляторів

Доступні як безкоштовні / з відкритим кодом, так і власні мережеві симулятори. Відомі мережевих симуляторів / емуляторів є [36]:

ns simulator

OPNET (Riverbed)

NetSim (Tetcos)

GloMoSim

Усі вони мають відкритий код, доступний для редагування, тоді як деякі з них є комерційними [36].

Використання мережевих симуляторів

Симулятори мережі забезпечують економічно ефективний метод для аналізу ємності, пропускної здатності та затримки 5G-NR [36].

Оборонні програми, такі як HF / UHF / VHF Radio MANET Radio, тактичні канали передачі даних тощо [36].

Моделювання IOT, VANET

Симуляція зв’язку між мережею БПЛА та дронами.

Машинне навчання: тестування алгоритмів ML для оптимізації параметрів мережі, генерування синтетичних даних, навчання алгоритмів ML у мережах

Освіта: онлайн-курси, лабораторні експерименти та дослідження та розробки. Більшість університетів використовують мережевий симулятор для навчання/досліджень та розробок, оскільки купувати апаратне обладнання занадто дорого.

Існує велика різноманітність мережевих симуляторів, від дуже простих до дуже складних. Як мінімум мережевий симулятор повинен дозволяти користувачеві

Моделювання топології мережі, вказавши вузли в мережі та зв’язки між цими вузлами:

- Моделювання потіку програми між вузлами
- Надання показників продуктивності мережі як результат
- Візуалізація потоку пакетів
- Оцінка технології/протоколу та конструкції пристроїв
- Реєстрація пакетів/подій для детального аналізу/налагодження

3.2 Програмне забезпечення для мережевого моделювання

1. PRTG. PRTG Network Monitor-це флагманська пропозиція німецької компанії-розробника програмного забезпечення Paessler для моніторингу локальних і глобальних мереж (LANs & WAN), серверів, веб-сайтів, додатків і багато чого іншого.

2. Riverbed Modeler. Riverbed OPNET Network Modeler від компанії Riverbed Technology, що базується в Сан-Франциско, являє собою технологію мережевої оптимізації.

3. Packet Tracer. Packet Tracer - це інструмент моделювання мережі, який дозволяє користувачеві створювати мережеві моделі, корисні у випадках, коли доступне обладнання є дорогим. Packet Tracer можна використовувати на навчальних курсах або для моделювання різних сценаріїв.

4. GNS3. GNS3 - це програмне забезпечення з відкритим кодом, яке візуалізує, планує, тестує та усуває неполадки в мережевих середовищах на будь-якій платформі постачальника в масштабі-без необхідності безпосередньої взаємодії з мережевим обладнанням.

5. SecureCRT. SecureCRT забезпечує безпечний віддалений доступ, передачу файлів і тунелювання даних для всіх співробітників компанії.

6. EVE-NG LTD. Платформа EVE-NG PRO дозволяє підприємствам, постачальникам/центрам електронного навчання, окремим особам і групам співробітників створювати віртуальні докази концепцій, рішень і навчальних середовищ.

7. CyberBattleSim. CyberBattleSim, випущений Microsoft 365 Defender Research, — це набір інструментів для атак з відкритим кодом, який дає змогу моделювати мережу для дослідників, щоб спостерігати, як їхні мережі справляються з атаками з боку противників.

8. InfoVista Planet. InfoVista Planet — це програмне забезпечення для планування та оптимізації радіочастот, розроблене для бездротових мереж. Відповідно до InfoVista, це рішення призначене для малих і великих підприємств і

обслуговує широкий спектр професіоналів і галузей, включаючи фахівців з телекомунікацій, мережевих інженерів, радіочастотних інженерів.

9. Plixer Replicator. Plixer Replicator дозволяє організаціям максимізувати цінність існуючих мережевих метаданих. Він централізовано збирає, балансує навантаження та пересилає потоки та дані журналів до інструментів аналізу, таких як Plixer Scrutinizer, SIEM (Splunk, Elasticsearch, IBM QRadar тощо) та інших засобів керування.

10. Gambit MIMIC NetFlow Simulator. Gambit MIMIC NetFlow Simulator від компанії Gambit Communications із Нью-Гемпширу — це технологія моделювання мережі.

11. PacketStorm Hurricane. Hurricane від компанії PacketStorm Communications із Нью-Джерсі – це технологія мережевого симулятора.

12. iTrinegy INE. iTrinegy INE від iTrinegy з Вобурна, штат Массачусетс, — це технологія симулятора мережі.

13. Forward Enterprise. Forward Enterprise — це платформа мережевого моделювання та верифікації, розроблена компанією Forward Networks, Inc. Вона надає математично точні представлення мережевих інфраструктур, що дозволяє користувачам шукати, перевіряти та прогнозувати поведінку мережі. Це програмне рішення спрямоване.

14. Cisco VIRL (part of The Cisco Learning Network). VIRL — це повна мережева платформа моделювання для тестування, навчання та навчання.

15. Mininet. Mininet надає віртуальний тестовий стенд і середовище розробки для програмно-визначених мереж (SDN).

16. Paragon Planner. Paragon Planner, developed by Juniper Networks, is a cloud-native modeling tool designed for offline visualization and detailed architectural planning of production networks. According to the vendor, this software enables network operators, architects, and planners to accurately forecast the impact.

17. WANem. WANem (Wide Area Network Emulator) — це технологія моделювання мережі з відкритим кодом, спочатку розроблена компанією Tata Consultancy Services у Мумбаї.

18. Gambit MIMIC IOS Simulator. Gambit MIMIC IOS Simulator від Gambit Communications із Нью-Гемпширу — це технологія моделювання мережі.

19. Boson NetSim. Boson спеціалізується на наданні матеріалів для підготовки до технологічного обстеження, які використовуються окремими особами, компаніями, науковими установами та державними установами.

20. Gambit MIMIC SNMP Simulator.Gambit MIMIC SNMP Simulator від компанії Gambit Communications із Нью-Гемпширу — це технологія моделювання мережі.

21. Argus. Argus, розроблений компанією QoSient, — це засіб реєстрації мережевої активності, який має на меті надавати комплексні дані про мережевий потік і аналітику. Він в основному використовується для безпеки, операцій і управління продуктивністю. Argus призначений для обслуговування широкого кола організацій, у тому числі.

3.3 Моделювання процесів адміністрування корпоративної мережі у віртуальному середовищі

3.3.1 Розгортання та налаштування DHCP-серверу

DHCP-сервер у Windows Server 2022 – це служба, яка дозволяє автоматично призначати IP-адреси та інші параметри мережі комп'ютерам та іншим пристроям у корпоративній мережі. Це дозволяє адміністраторам мережі уникнути необхідності вручну налаштовувати кожен пристрій зі статичною IP-адресою.

DHCP-сервер у Windows Server 2022 має такі функції:

- Автоматичне призначення IP-адрес: DHCP-сервер автоматично призначає IP-адреси, маски підмереж, адреси шлюзів за замовчуванням, адреси DNS-серверів та інші параметри TCP/IP клієнтам DHCP.
- Резервування IP-адрес: DHCP-сервер дозволяє резервувати IP-адреси для конкретних комп'ютерів або пристроїв.
- Авторизація DHCP: Авторизація DHCP дозволяє переконатися, що DHCP-сервери в мережі є справжніми.

- Статистика DHCP: DHCP-сервер надає статистику про те, як він використовується в мережі.

Крім основних функцій, DHCP-сервер у Windows Server 2022 також підтримує такі додаткові можливості:

- IPv6: DHCP-сервер може використовуватися для автоматичного призначення IP-адрес IPv6.
- DHCP Failover: DHCP Failover дозволяє забезпечити безперервність роботи DHCP-сервісу у разі відмови одного із DHCP-серверів.
- DHCPv6 Failover: DHCPv6 Failover дозволяє забезпечити безперервність роботи DHCPv6-сервісу у разі відмови одного з DHCPv6-серверів.
- DHCP Option 82: DHCP Option 82 дозволяє DHCP-серверу передавати додаткову інформацію про клієнта DHCP маршрутизатор.
- DHCP Snooping: DHCP Snooping дозволяє DHCP-серверу відстежувати DHCP-трафік у мережі та запобігати атакам, пов'язаним з DHCP.

На рисунку 3.1 зображено вибраний тип установки "Role-based or feature-based installation".

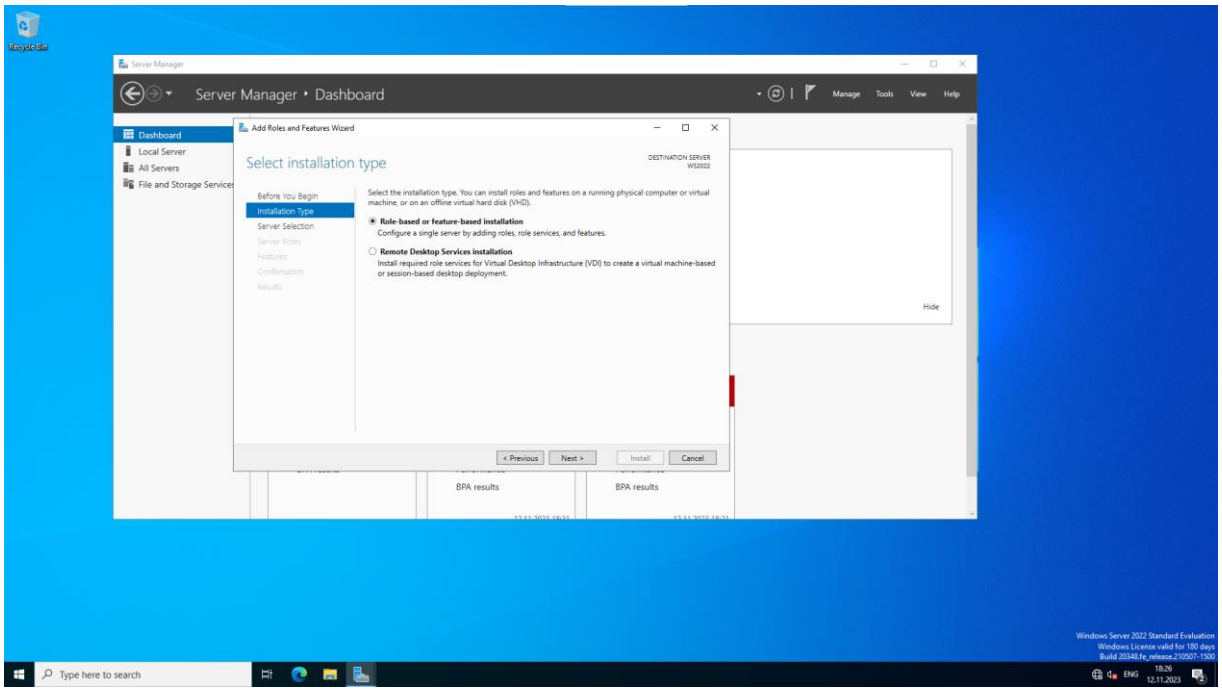


Рисунок 3.1 – Вибір типу конфігурації

На рисунку 3.2 зображено сервер, на який буде проводитися установка ролі.

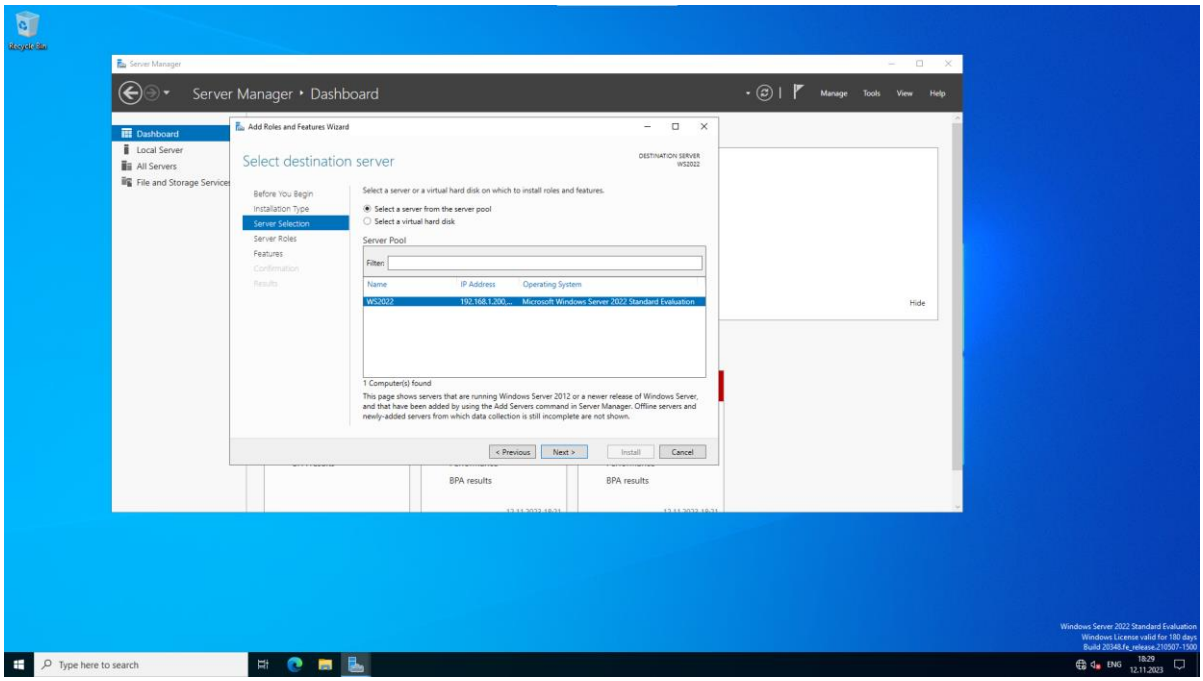


Рисунок 3.2 – Вибраний сервер на який буде проводитися установка ролей

На рисунку 3.3 зображено вибрані ролі для сервера.

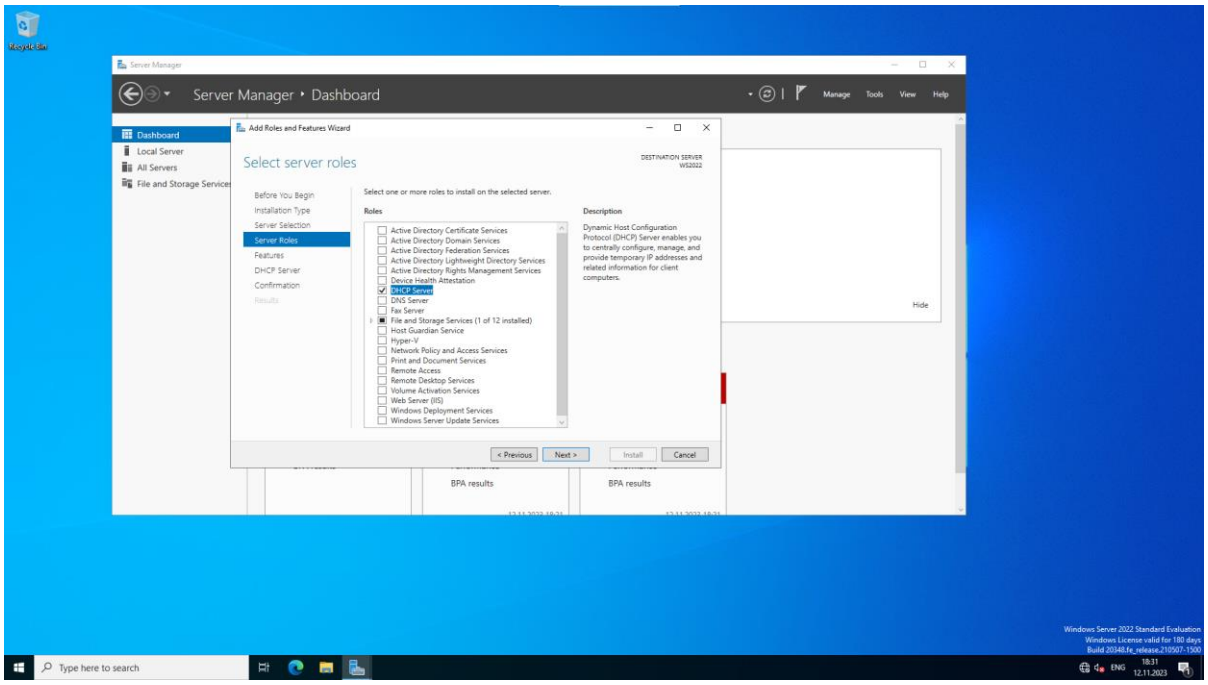


Рисунок 3.3 – Вибрана роль для сервера

На рисунку 3.4 зображено вибір компонента.

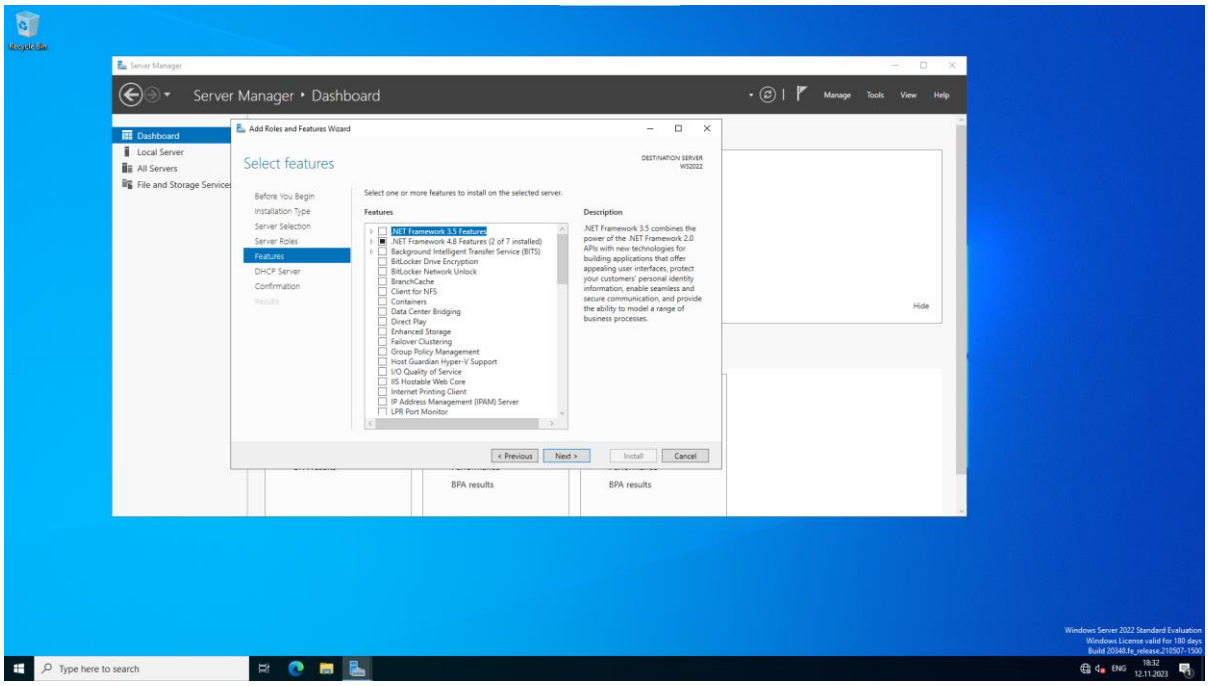


Рисунок 3.4 – Вибір компонента

На рисунку 3.5 зображено нагадування про необхідність заздалегідь спланувати структуру мережі, а також про те, що для роботи DHCP на сервері повинен бути хоча б один статичний IP адреса.

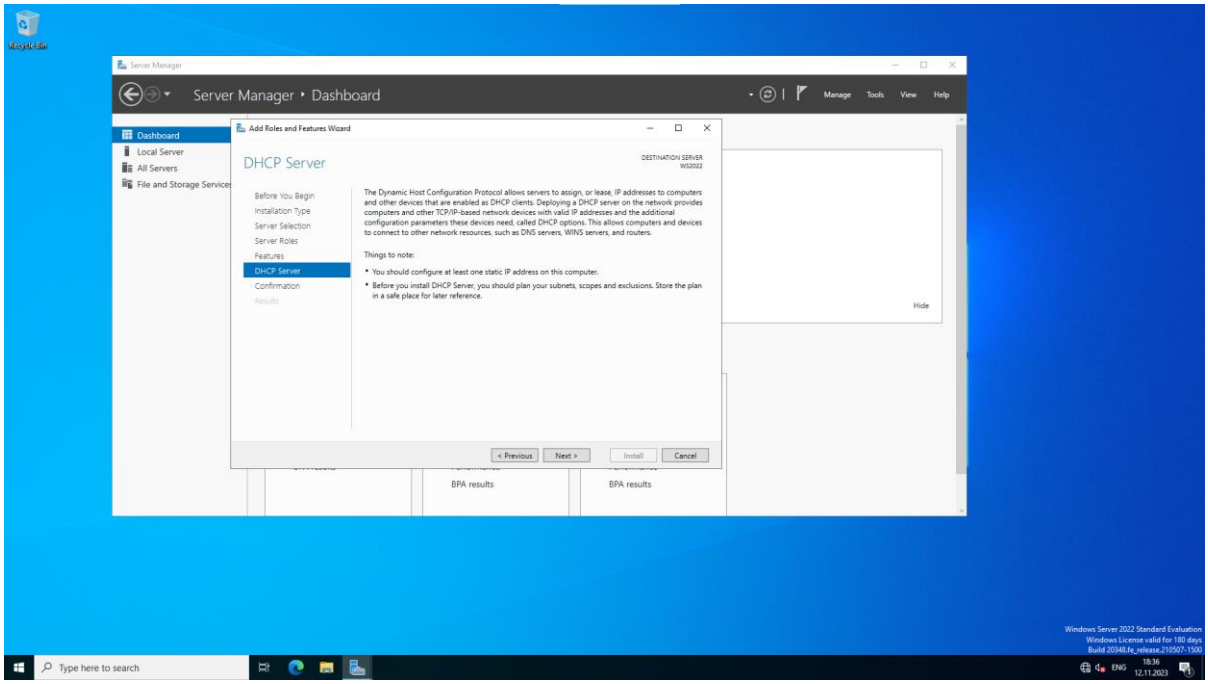


Рисунок 3.5 – Інформаційне нагадування

На рисунку 3.6 зображено список встановлюваних компонентів.

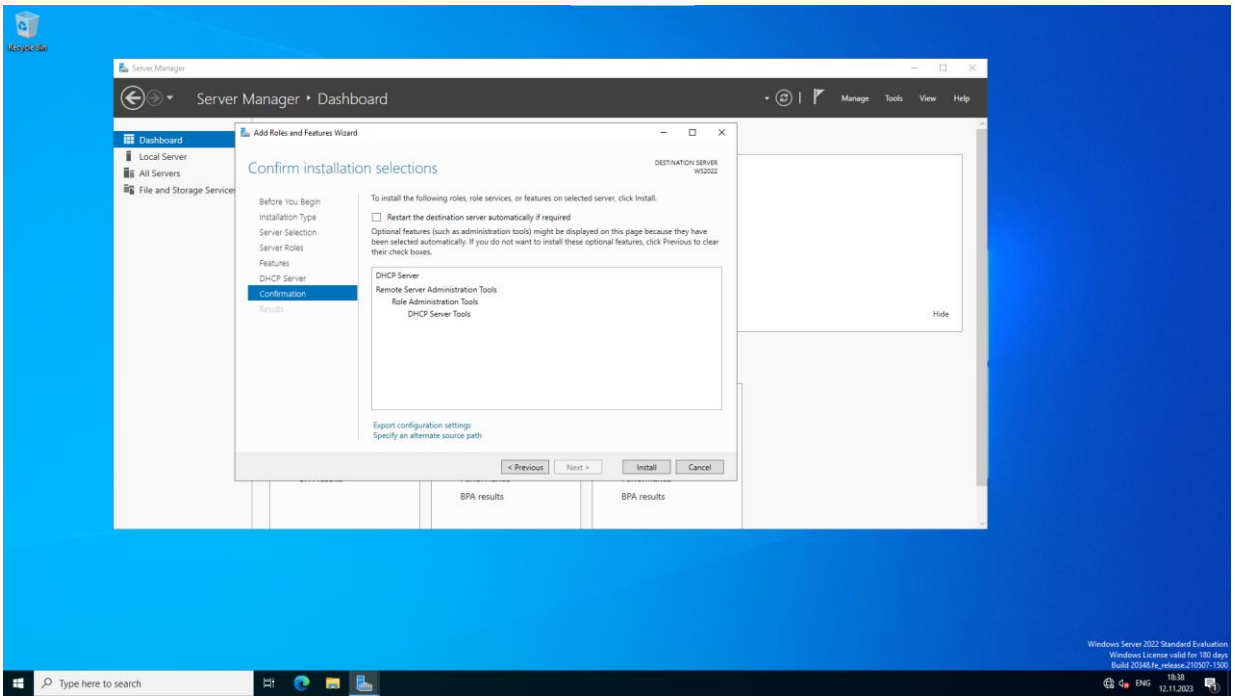


Рисунок 3.6 – Список встановлюваних компонентів

На рисунку 3.7 зображено початок процесу установки обраних ролей і необхідних компонентів.

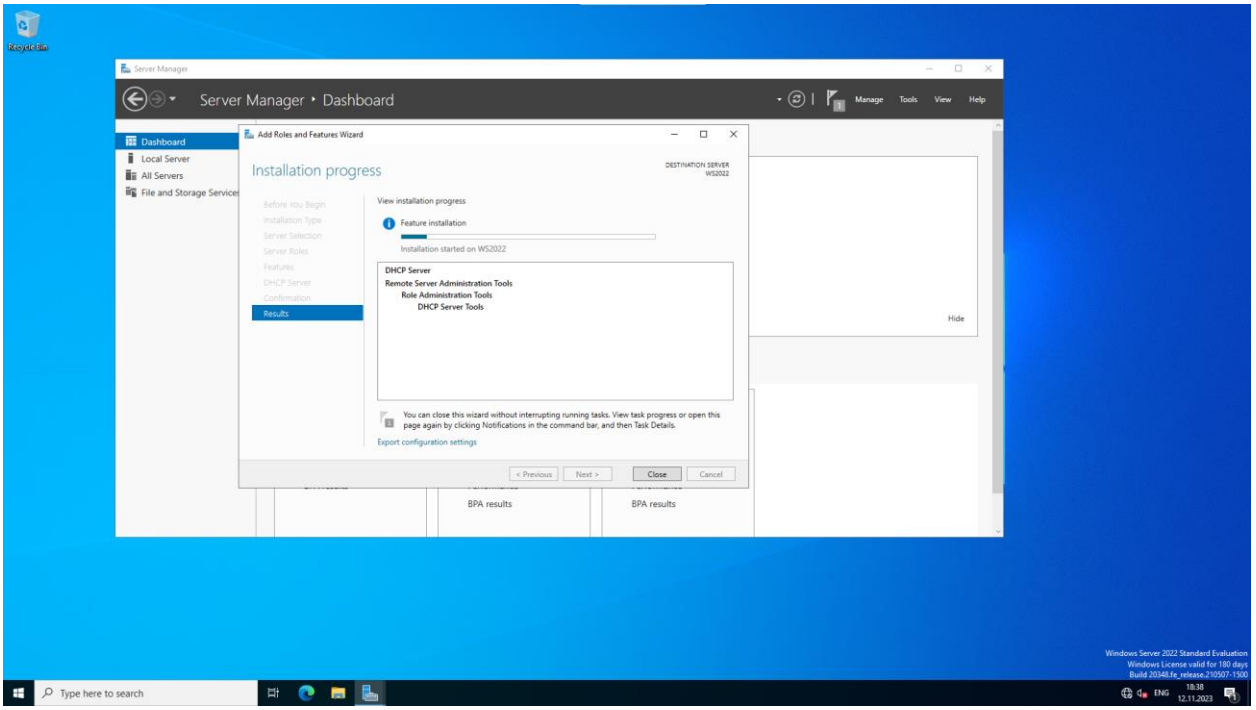


Рисунок 3.7 – Процес установки обраних ролей і необхідних компонентів

На рисунку 3.8 зображено кінець установки обраних ролей і необхідних компонентів.

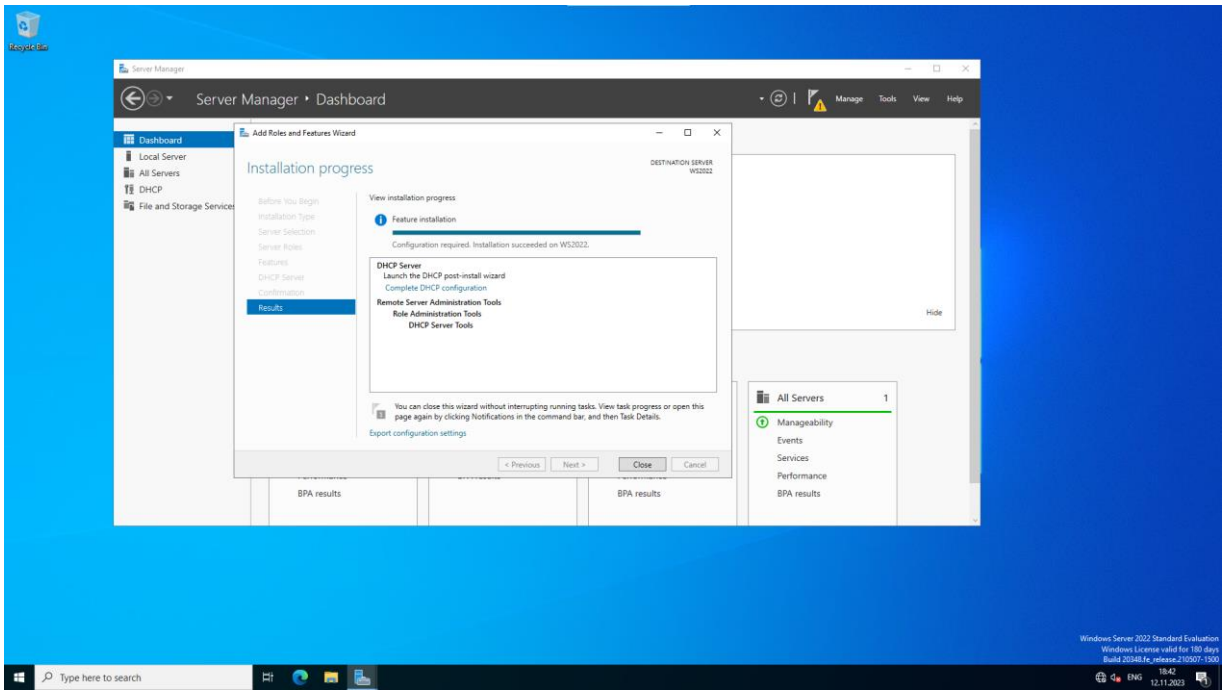


Рисунок 3.8 – Кінець установки обраних ролей і необхідних компонентів.

На рисунку 3.9 зображено початок автоматичного створення груп безпеки, яким буде дозволено управляти даними DHCP сервером.

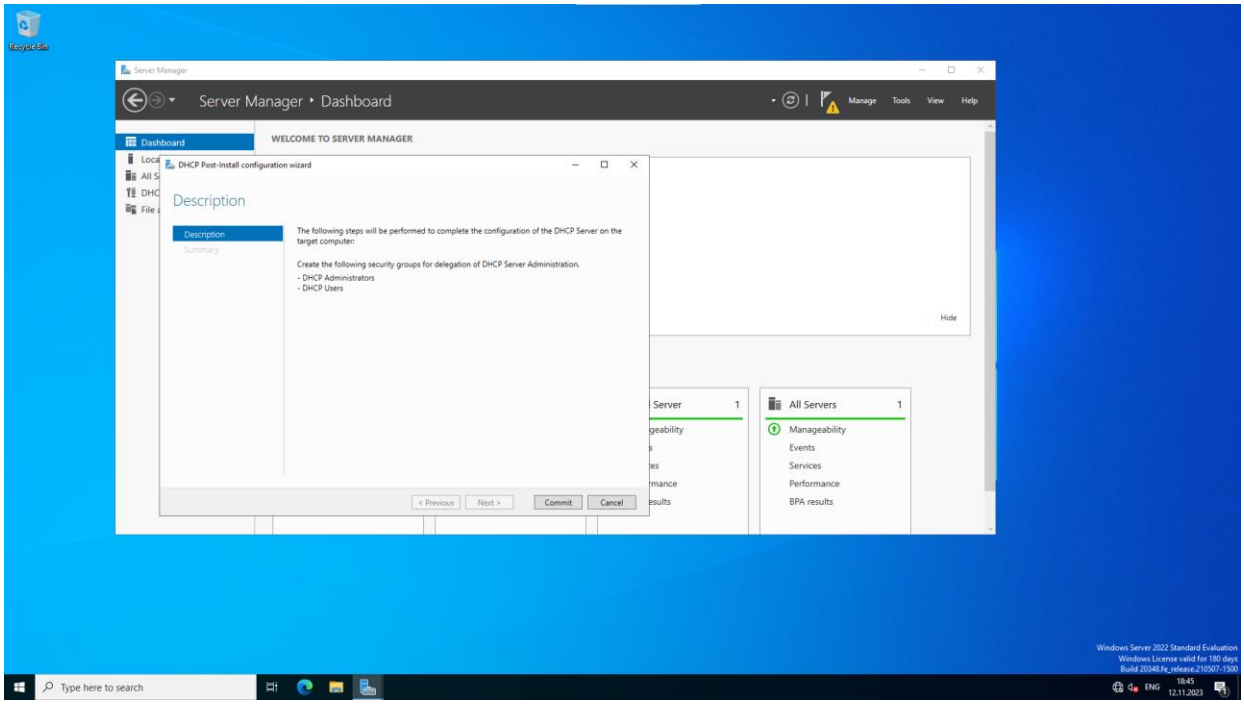


Рисунок 3.9 – Початок автоматичного створення груп безпеки

На рисунку 3.10 зображено кінець автоматичного створення груп безпеки, яким буде дозволено управляти даними DHCP сервером.

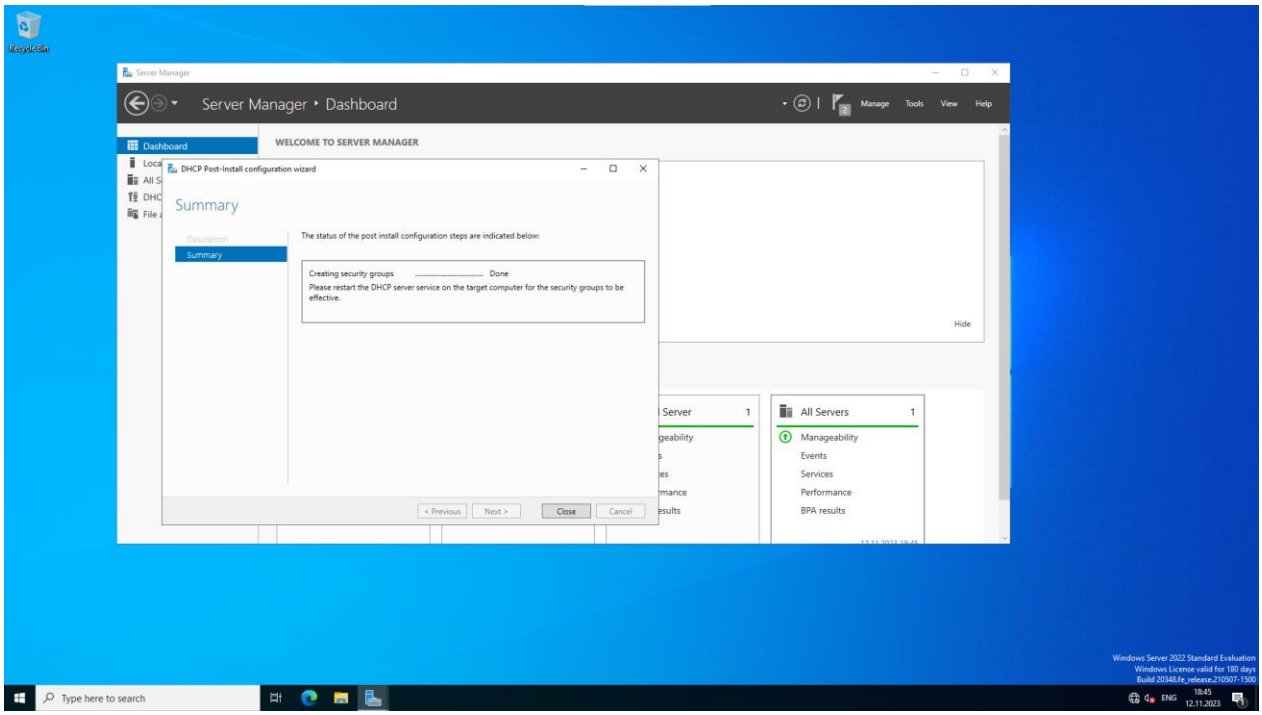


Рисунок 3.10 – Кінець автоматичного створення груп безпеки

На рисунку 3.11 зображено майстер створення області.

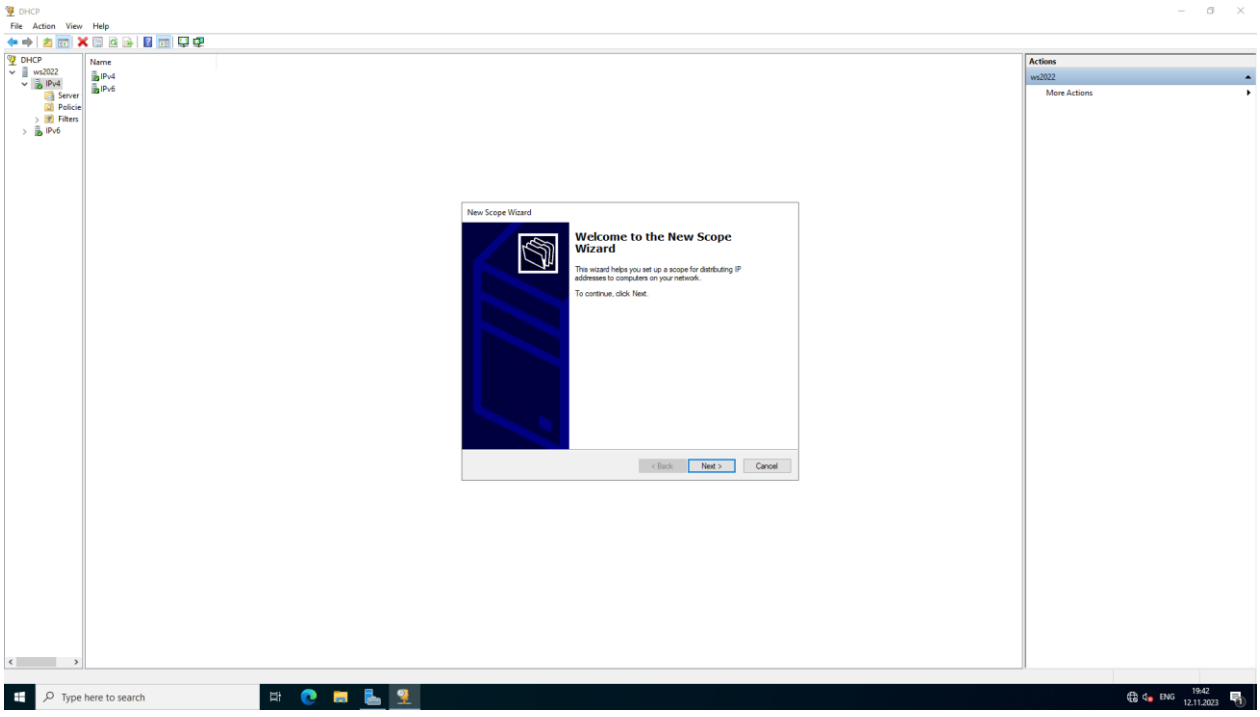


Рисунок 3.11 – Майстер створення області

На рисунку 3.12 зображено вказану назву DHCP області.

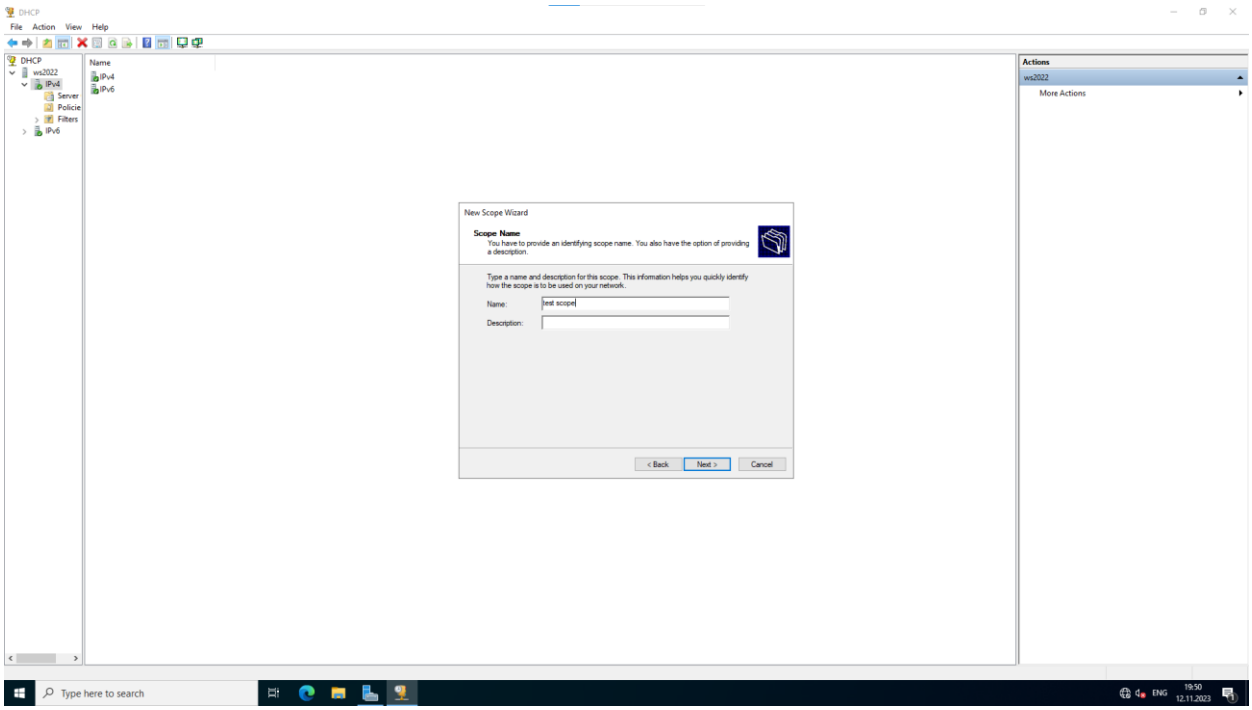


Рисунок 3.12 – Назва DHCP області

На рисунку 3.13 зображено вказаний діапазон IP-адрес і маска мережі.

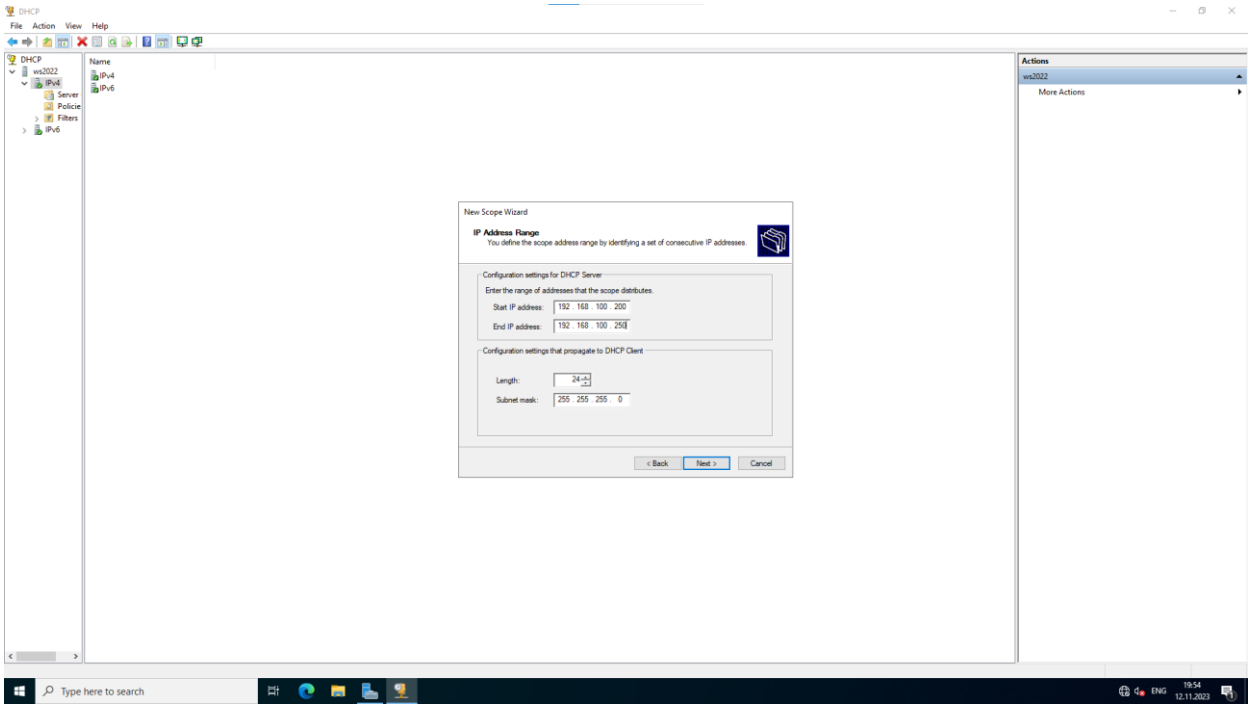


Рисунок 3.13 – Вказаний діапазон IP-адрес і маска мережі

На рисунку 3.14 зображено вказаний термін дії оренди адрес області.

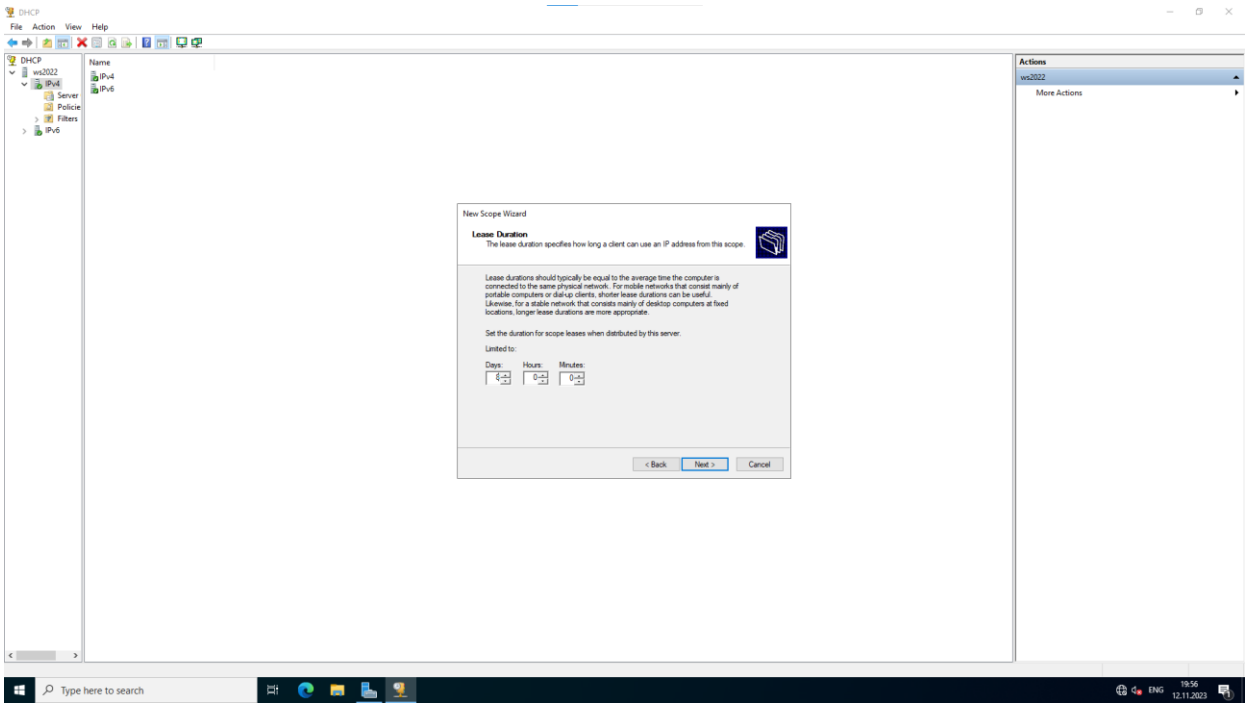


Рисунок 3.14 – Термін дії оренди адрес області

На рисунку 3.15 зображено налаштування додаткових параметрів DHCP області.

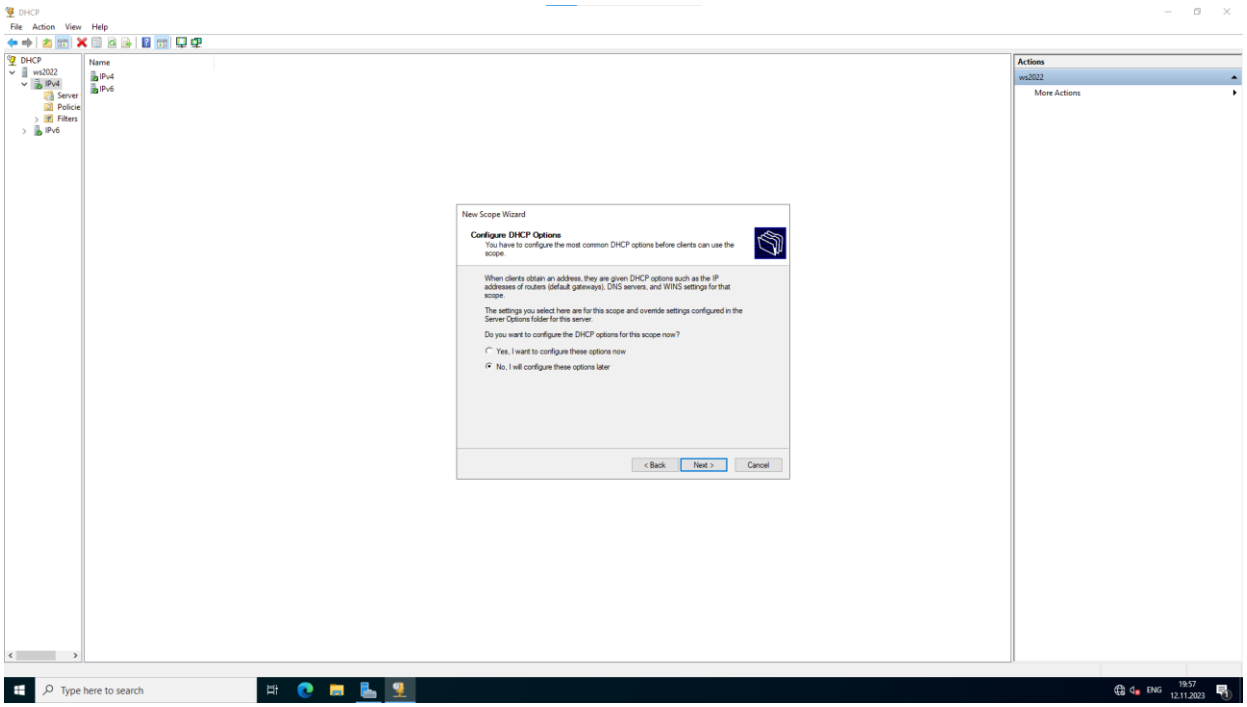


Рисунок 3.15 – Налаштування додаткових параметрів DHCP області

На рисунку 3.16 зображено завершення налаштування області в DHCP-сервері.

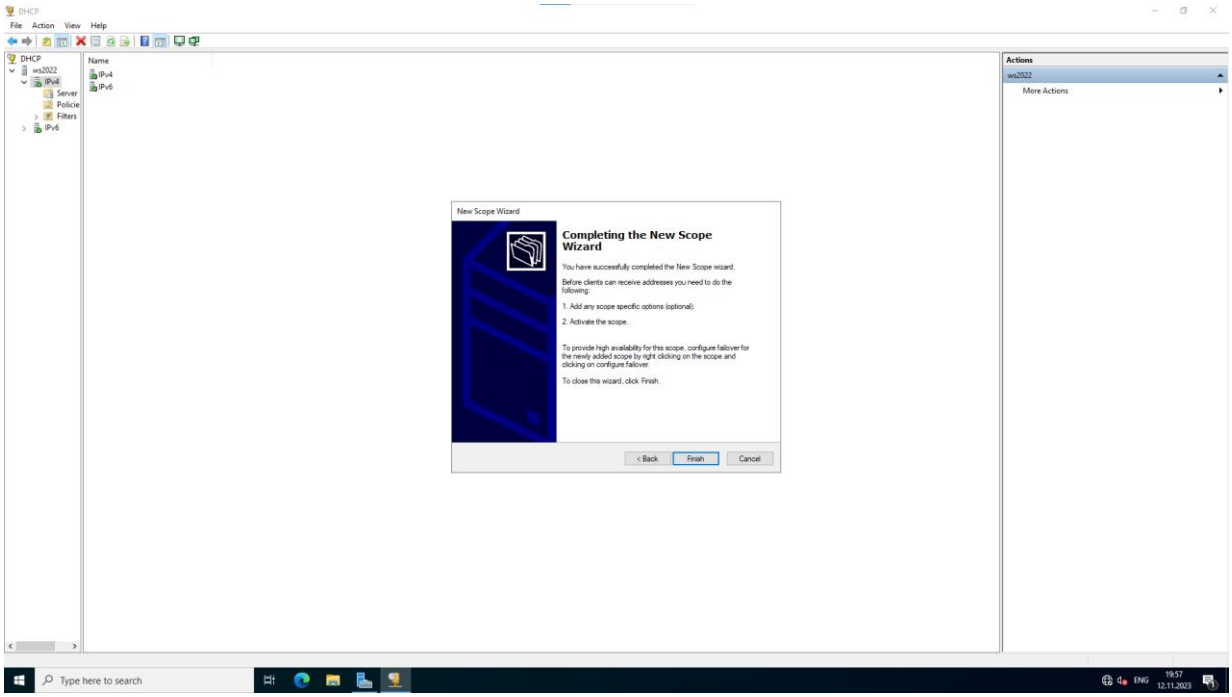


Рисунок 3.16 – Завершення налаштування області в DHCP-сервері

На рисунку 3.17 зображено створену область DHCP.

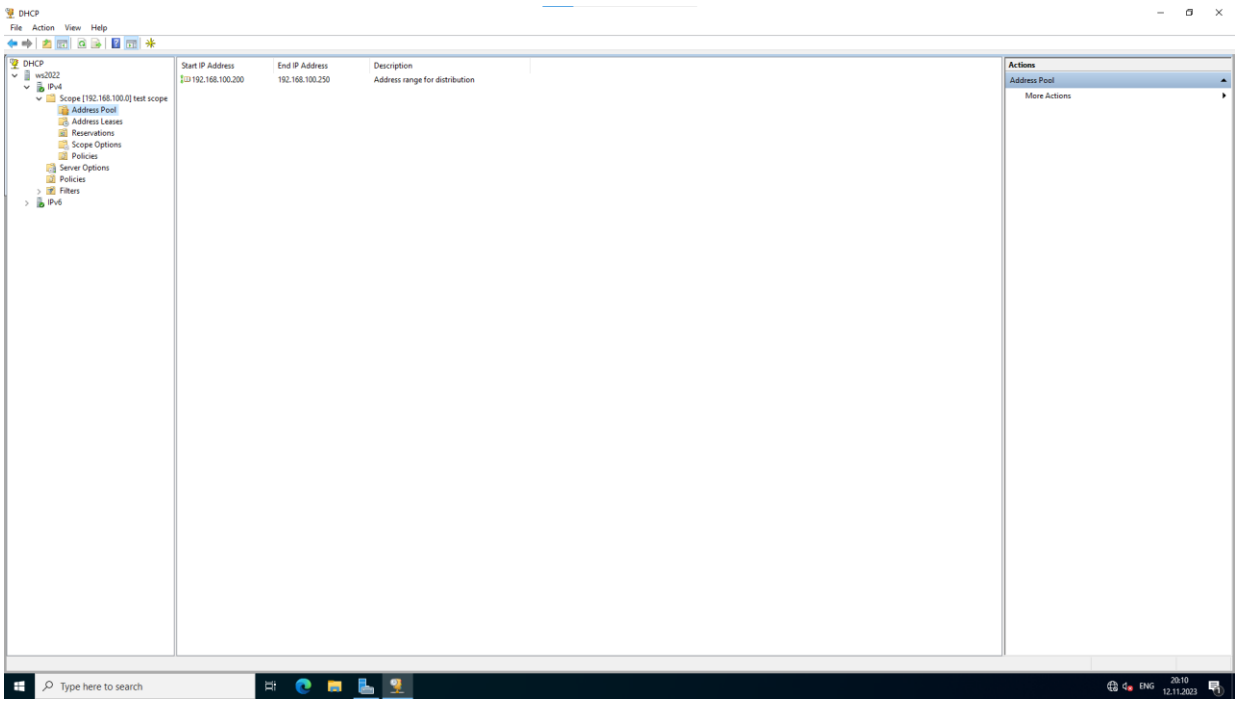


Рисунок 3.17 – Створена область DHCP

На рисунку 3.18 зображено орендовану адресу, яку отримала клієнтська машина.

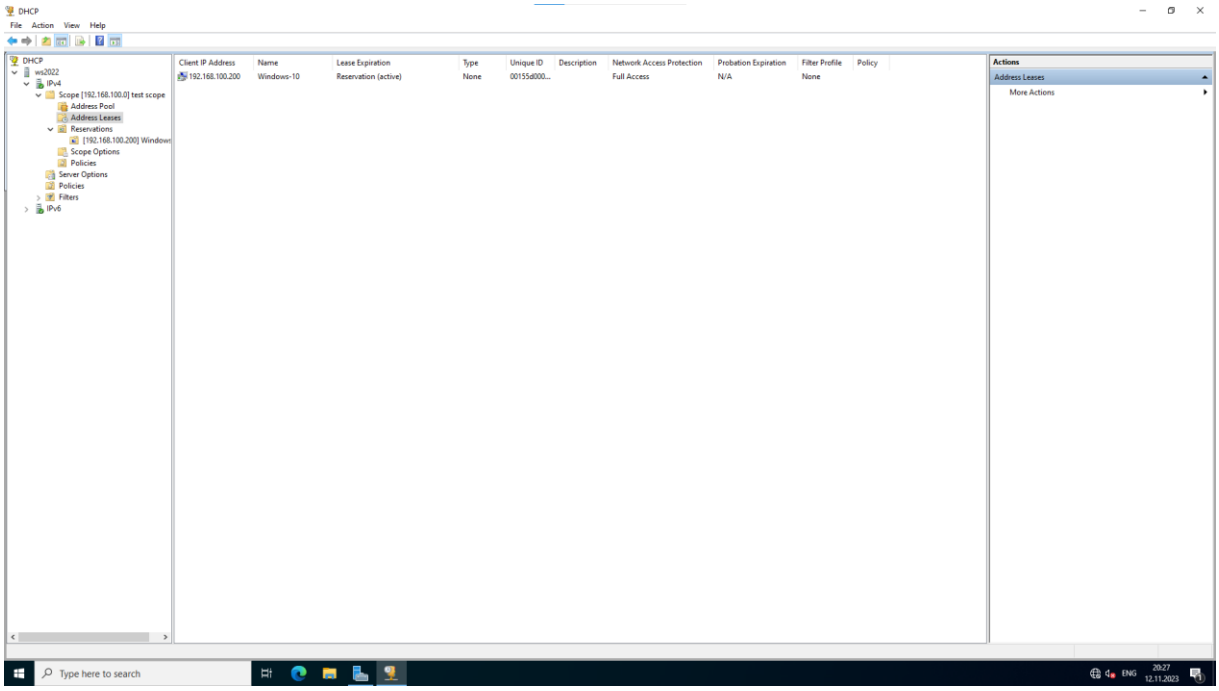


Рисунок 3.18 – Орендована адреса клієнтською машиною

На рисунку 3.19 зображено задані параметри DHCP сервером для клієнтської машини.

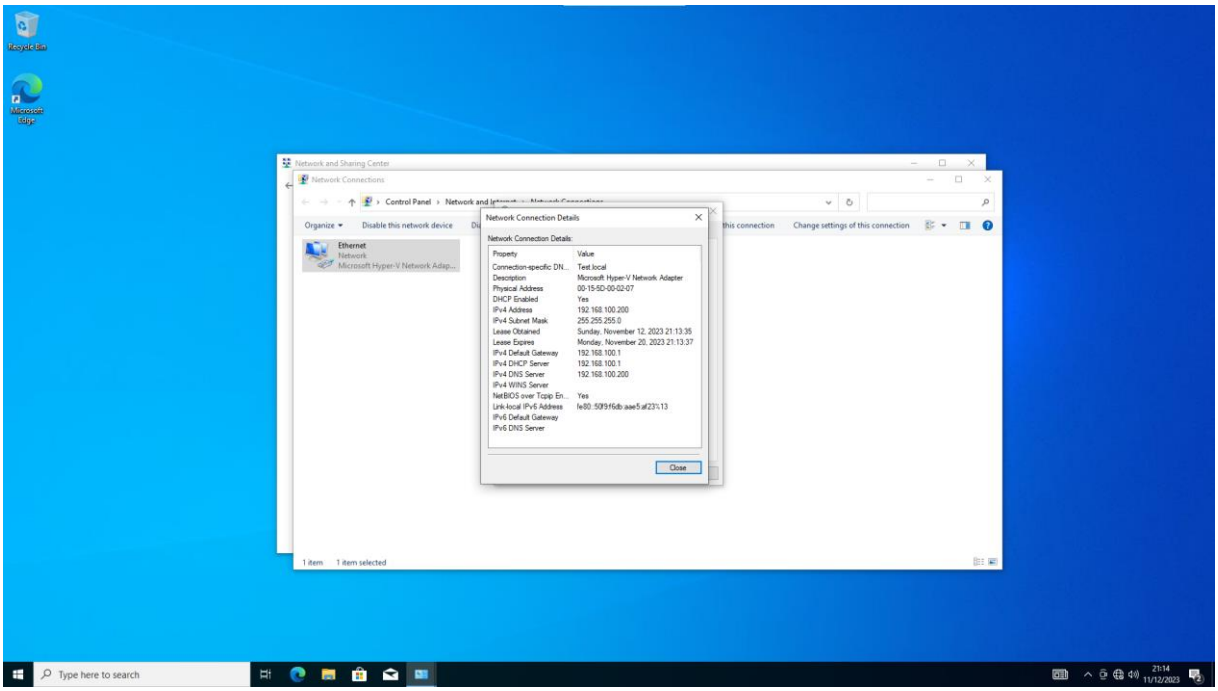


Рисунок 3.19 – Задані параметри DHCP сервером

3.3.2 Розгортання та налаштування AD

AD у Windows Server 2022 — це служба каталогів, яка надає централізовану базу даних для керування та організації облікових записів користувачів, комп’ютерів та інших ресурсів у мережі. AD — це ієрархічна база даних із доменами на верхньому рівні, за якими йдуть організаційні підрозділи (OU), а потім такі об’єкти, як користувачі, комп’ютери та групи [27, 28, 29].

AD надає ряд переваг для організацій будь-якого розміру, зокрема [27, 28, 29]:

1. Централізоване керування: AD забезпечує єдине місце для керування всіма мережевими ресурсами, полегшуючи відстеження користувачів, комп’ютерів і дозволів [27, 28, 29].
2. Безпека: AD допомагає захистити мережеві ресурси, надаючи послуги автентифікації та авторизації. AD також можна використовувати для впровадження політик безпеки, таких як вимоги до пароля та блокування облікового запису [27, 28, 29].
3. Масштабованість: AD можна масштабувати для підтримки мереж будь-якого розміру, від кількох десятків до сотень тисяч користувачів [27, 28, 29].
4. Надійність: AD дуже надійний і доступний завдяки таким функціям, як реплікація та відмовостійкість [27, 28, 29].

AD є важливим компонентом багатьох мереж Windows і використовується організаціями будь-якого розміру для керування своїми мережевими ресурсами [27,28,29].

На рисунку 3.20 зображено вибраний тип установки "Role-based or feature-based installation” [27, 28, 29].

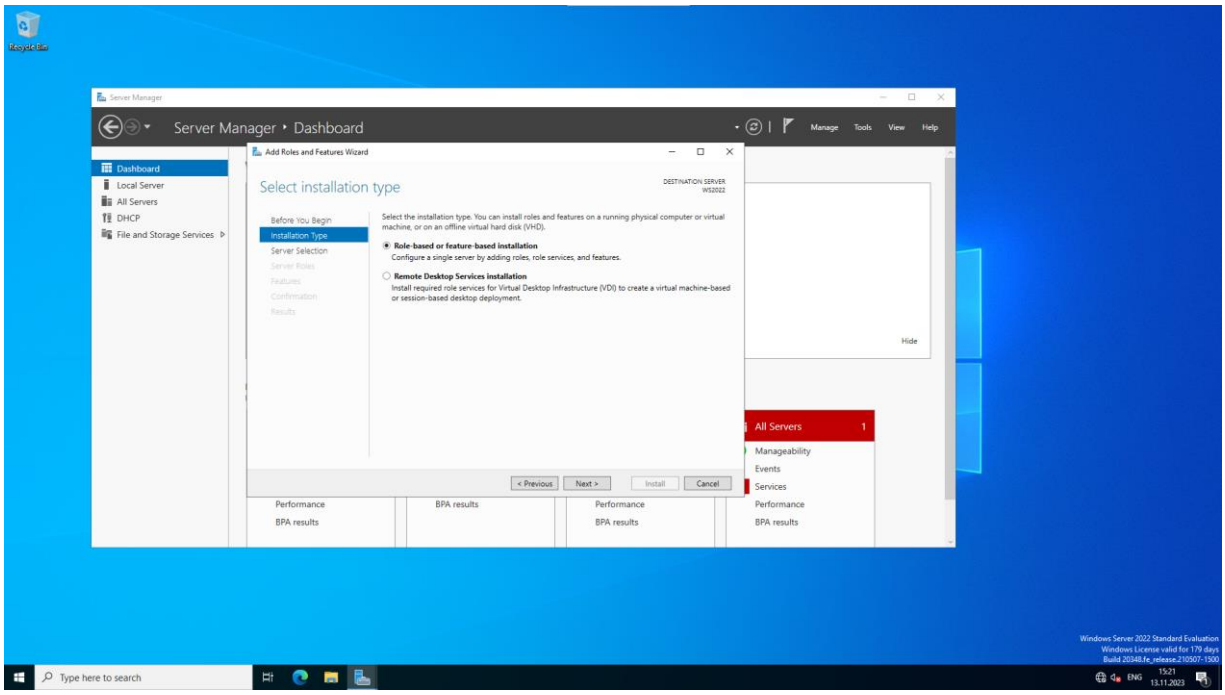


Рисунок 3.20 – Вибраний тип установки "Role-based or feature-based installation”

На рисунку 3.21 зображено сервер, на який буде проводитися установка ролі [27, 28, 29].

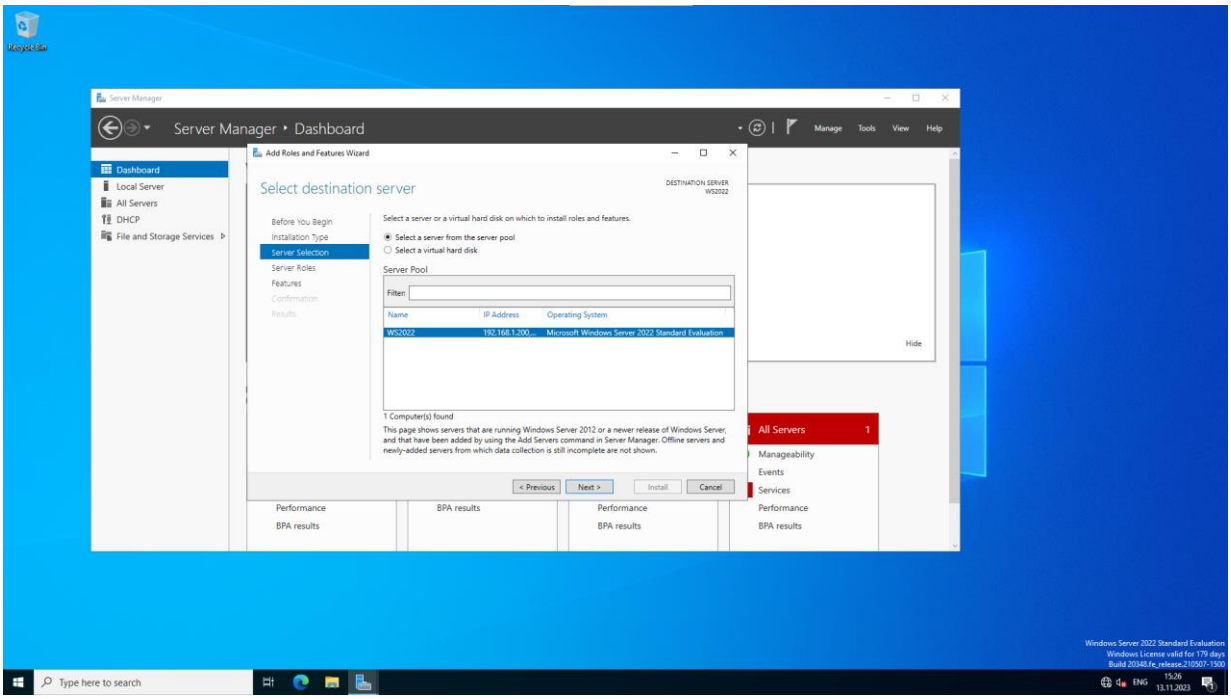


Рисунок 3.21 – Вибраний сервер на який буде проводитися установка ролі

На рисунку 3.22 зображено вибрану роль для сервера [27,28,29].

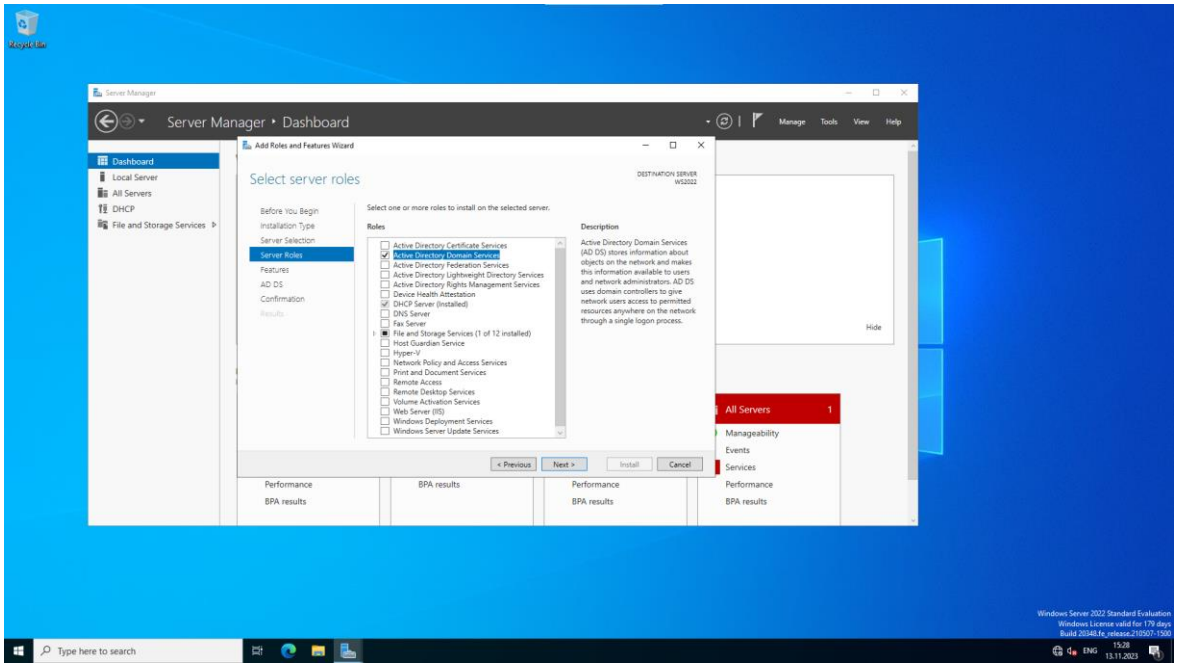


Рисунок 3.22 – Вибрана роль для сервера

На рисунку 3.23 зображено обраного компонента [27, 28, 29].

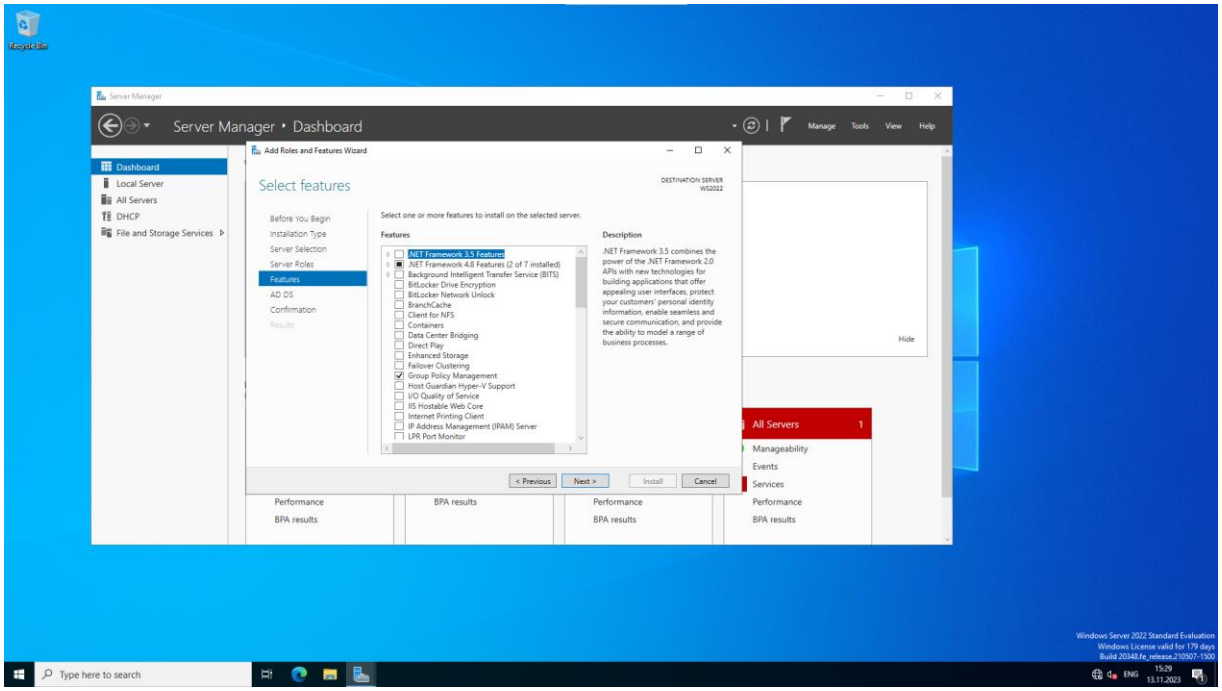


Рисунок 3.23 – Обраний компонент

На рисунку 3.24 зображено додаткову інформацію про домен “Active Directory Domain Services” [27, 28, 29].

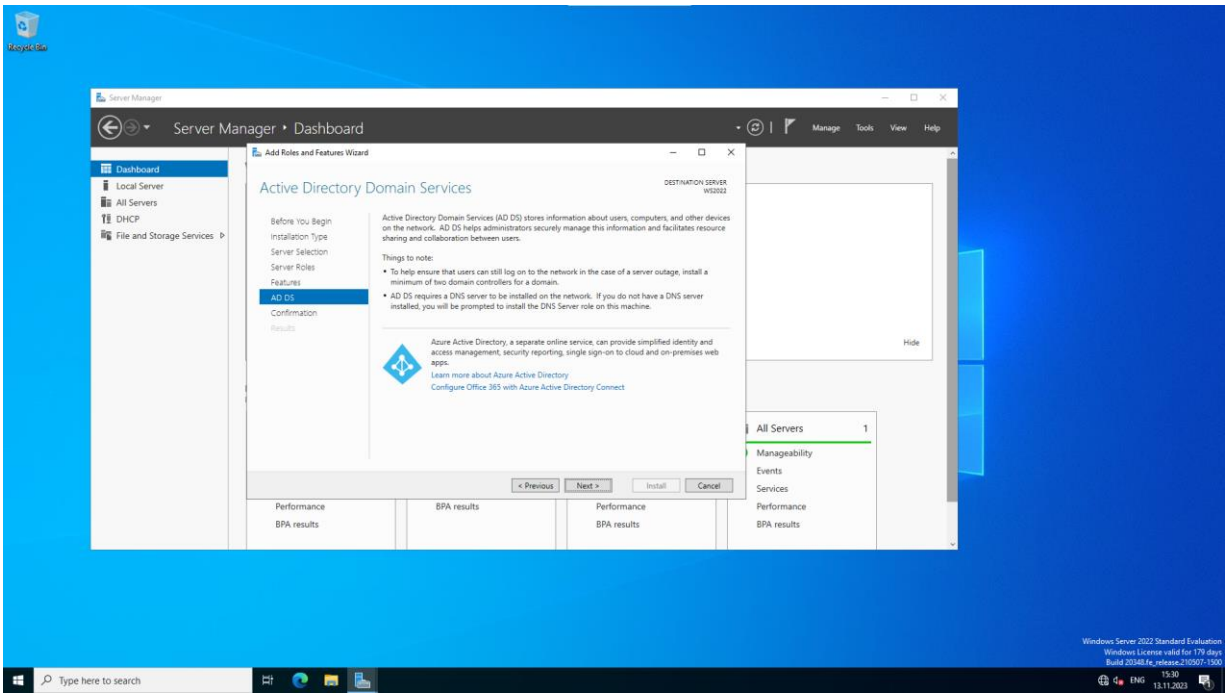


Рисунок 3.24 – Додаткова інформація про “Active Directory Domain Services”

На рисунку 3.25 зображено підтвердження встановлення компонентів [27, 28, 29].

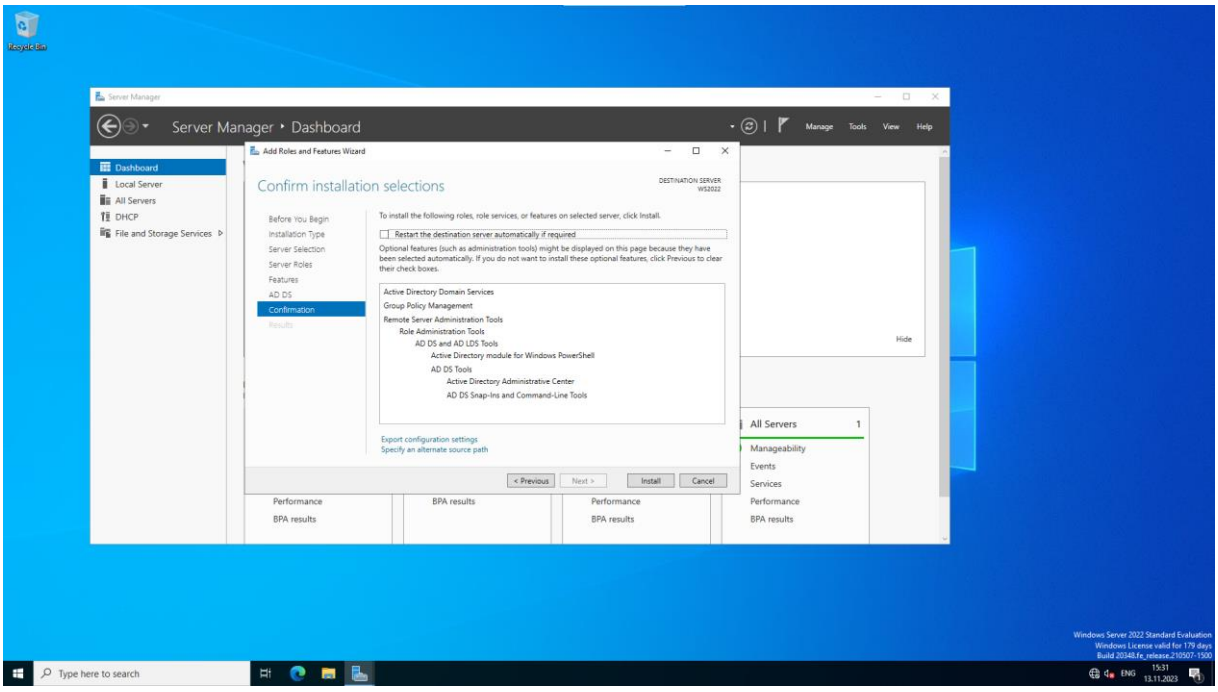


Рисунок 3.25 – Підтвердження встановлення компонентів

На рисунку 3.26 зображено процес установки обраних ролей і необхідних компонентів [27, 28, 29].

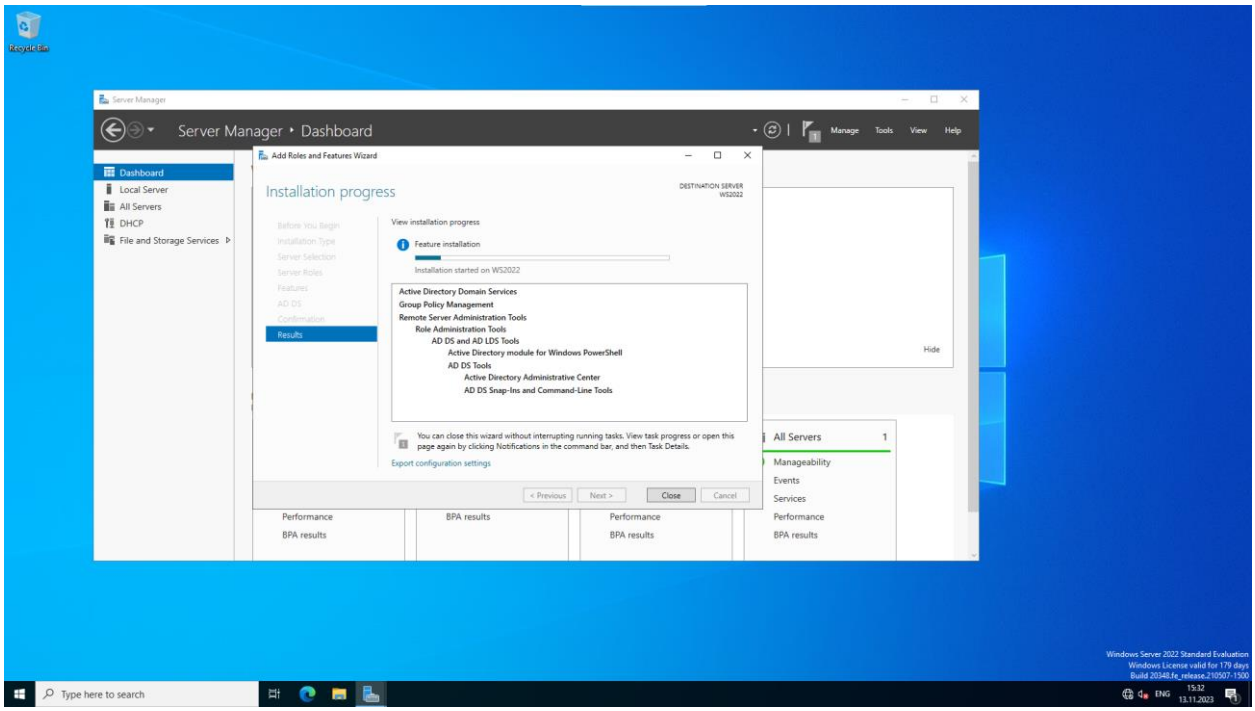


Рисунок 3.26 – Процес установки обраних ролей і необхідних компонентів

На рисунку 3.27 зображено створення нового лісу та вказання ім'я [27, 28, 29].

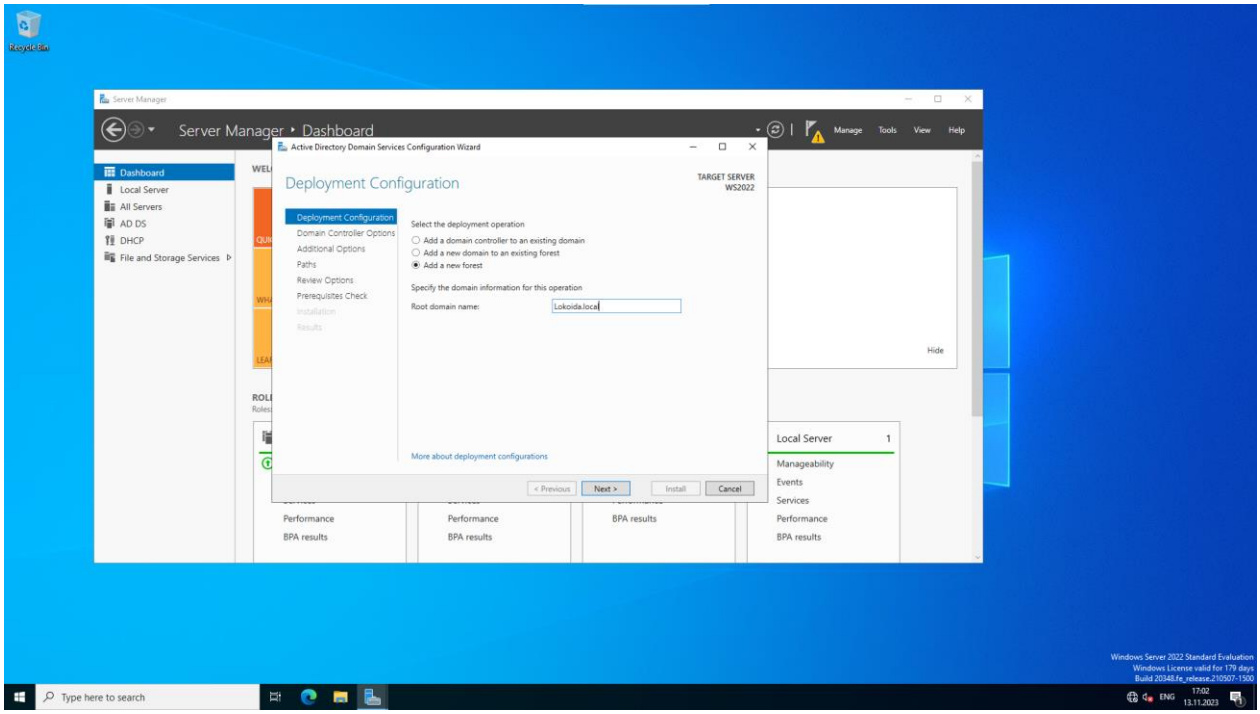


Рисунок 3.27 – Створення нового лісу та вказування ім'я для домену

На рисунку 3.28 зображено задані налаштування для домену контролера [27, 28, 29].

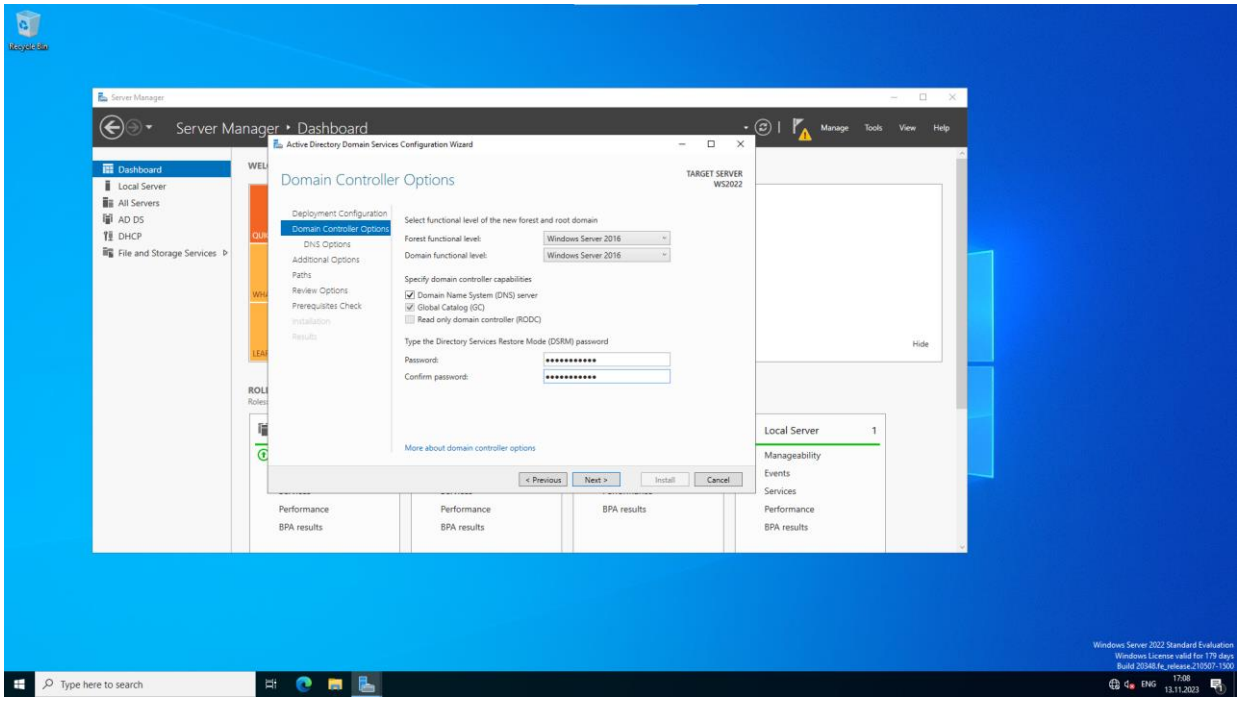


Рисунок 3.28 – Задані налаштування для домену контролера

На рисунку 3.29 зображено попередження про делегування DNS-сервера [27, 28, 29].

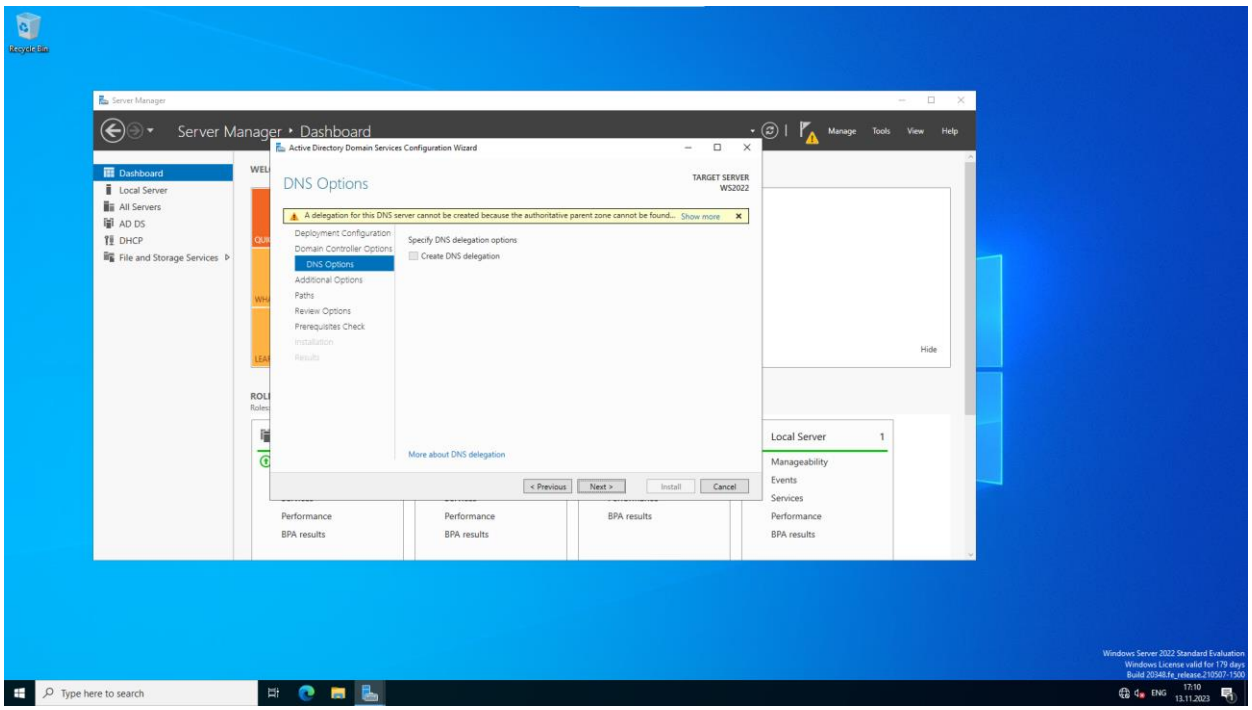


Рисунок 3.29 – Попередження про делегування DNS-сервера

На рисунку 3.30 зображено задане ім'я домену NetBIOS [27, 28, 29].

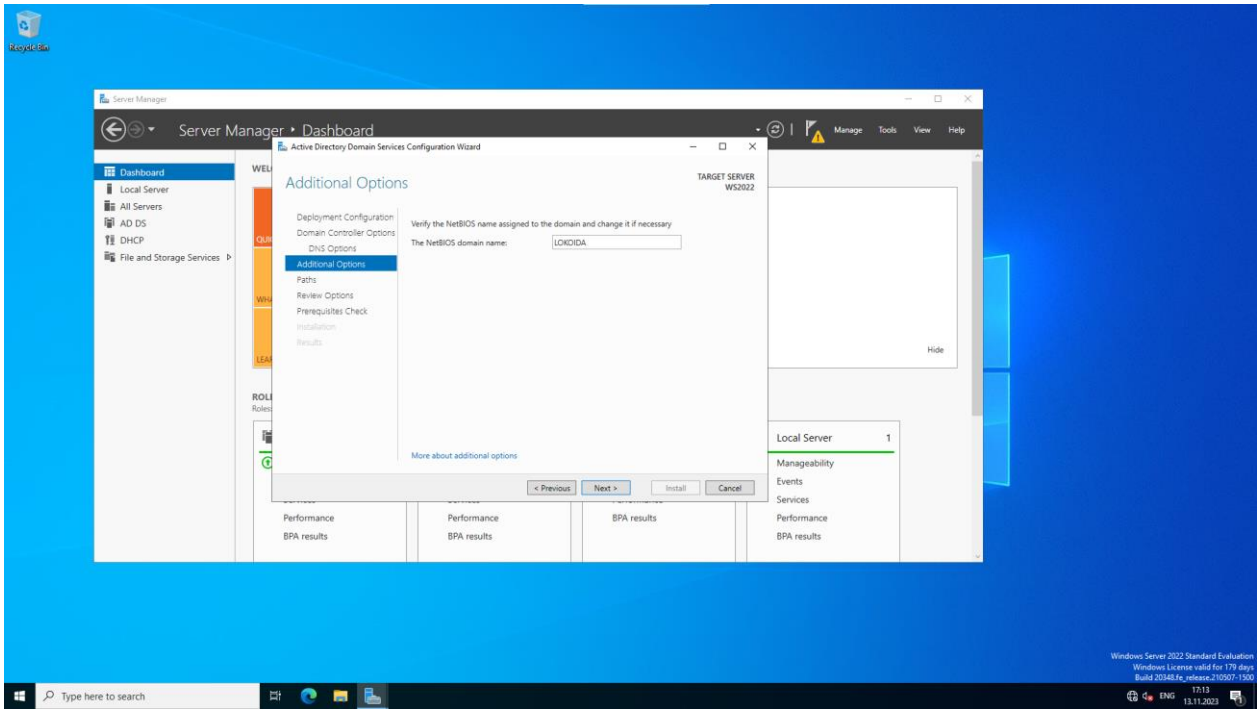


Рисунок 3.30 – Задане ім'я домену NetBIOS

На рисунку 3.31 зображено задані шляхи до каталогів бази даних, AD DS, файлів журналу та папки SYSVOL [27, 28, 29] .

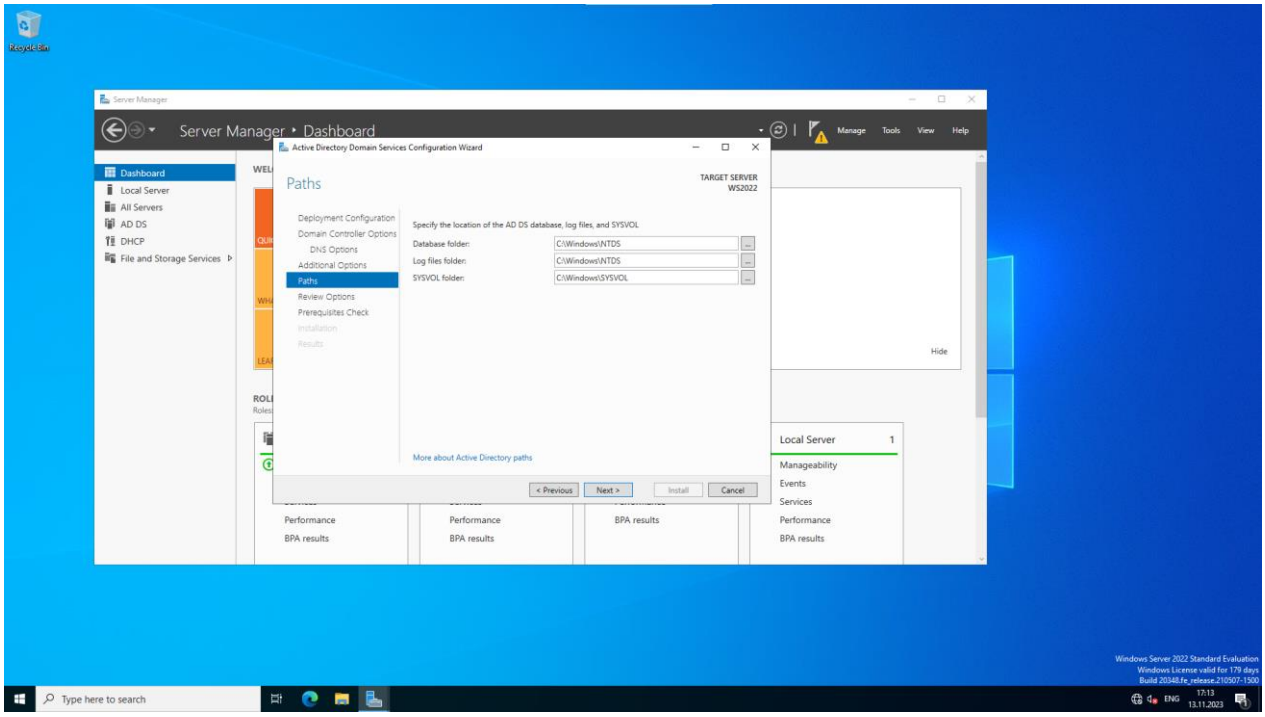


Рисунок 3.31 – Задані шляхи до каталогів бази даних, AD DS, файлів журналу та папки SYSVOL

На рисунку 3.32 зображено інформацію щодо підсумку розгортання AD [27, 28, 29].

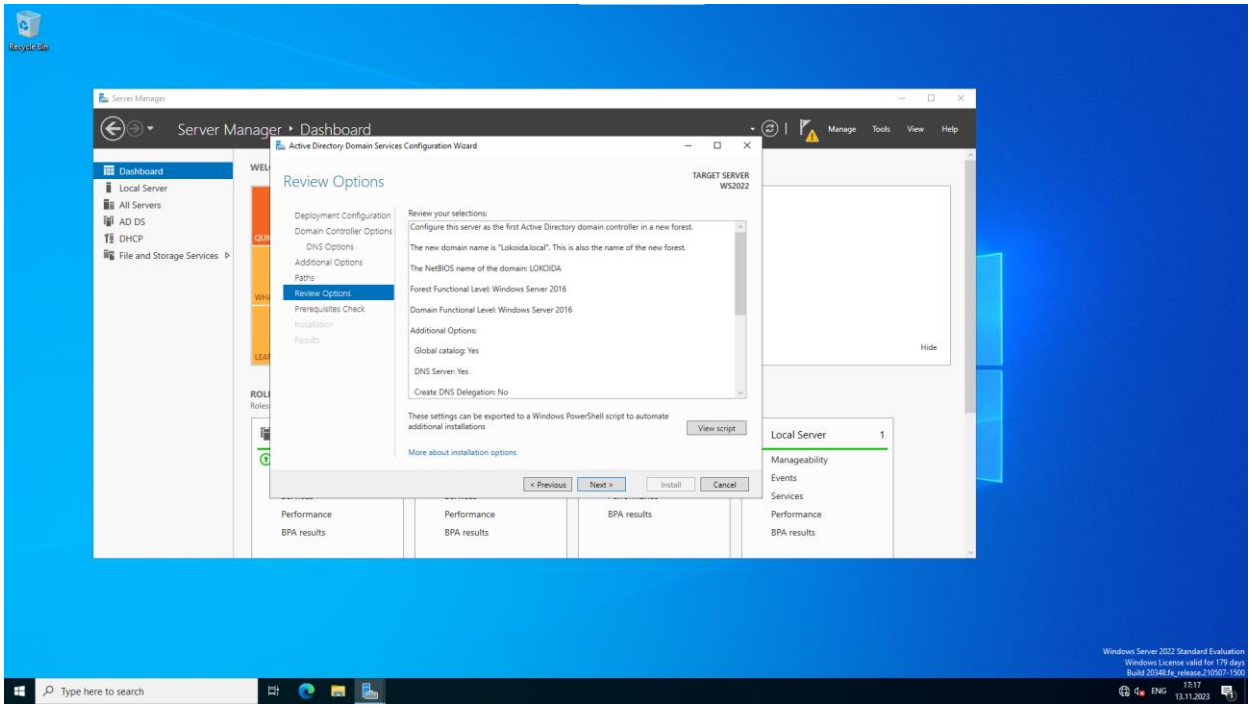


Рисунок 3.32 – Інформація щодо підсумку розгортання AD

На рисунку 3.33 зображено перевірку попередніх вимог [27, 28, 29].

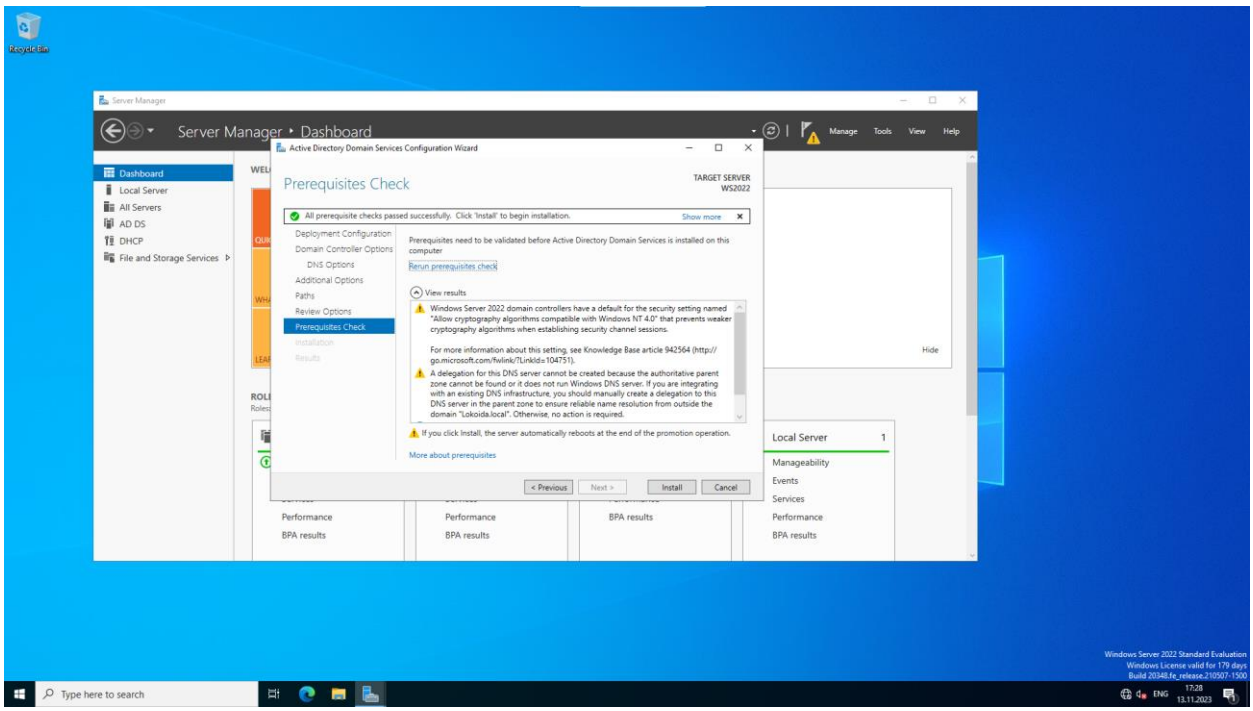


Рисунок 3.33 – Перевірка попередніх вимог

На рисунку 3.34 зображено процес підвищення ролі сервера до рівня контролера домену [27, 28, 29].

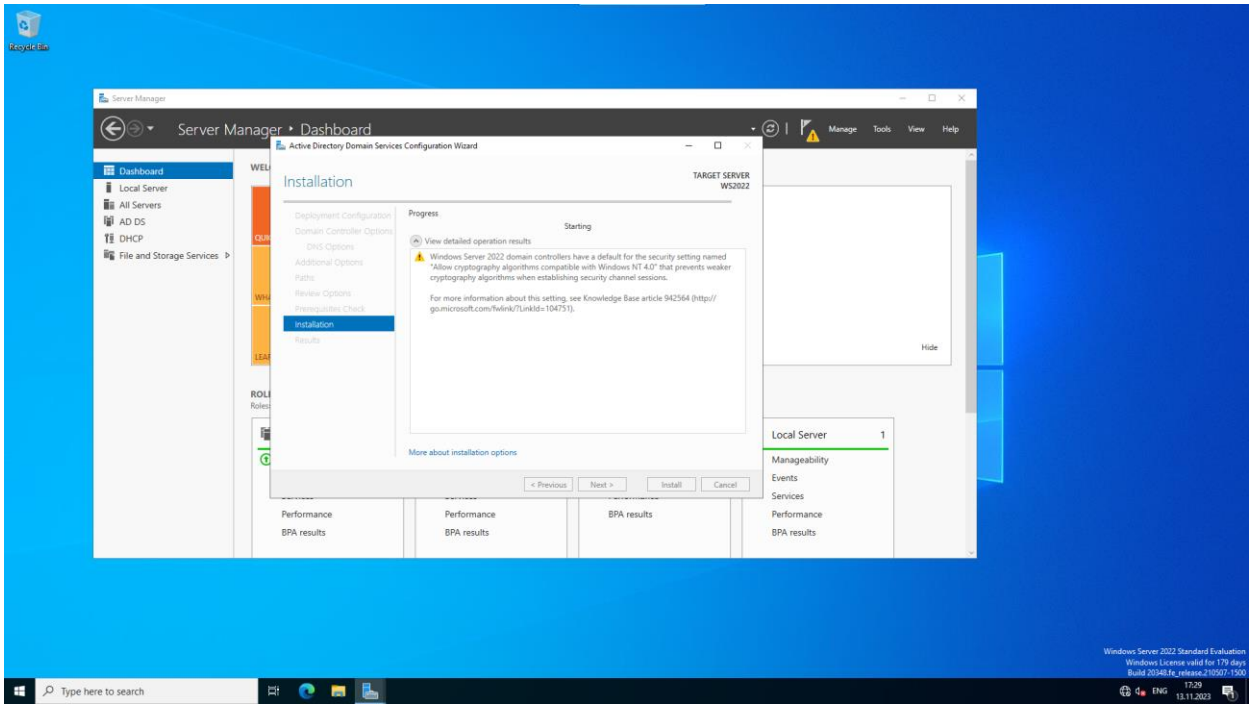


Рисунок 3.34 – Процес підвищення ролі сервера до рівня контролера домену

На рисунку 3.35 зображено інструмент “Active Directory Administrative Center” [27, 28, 29].

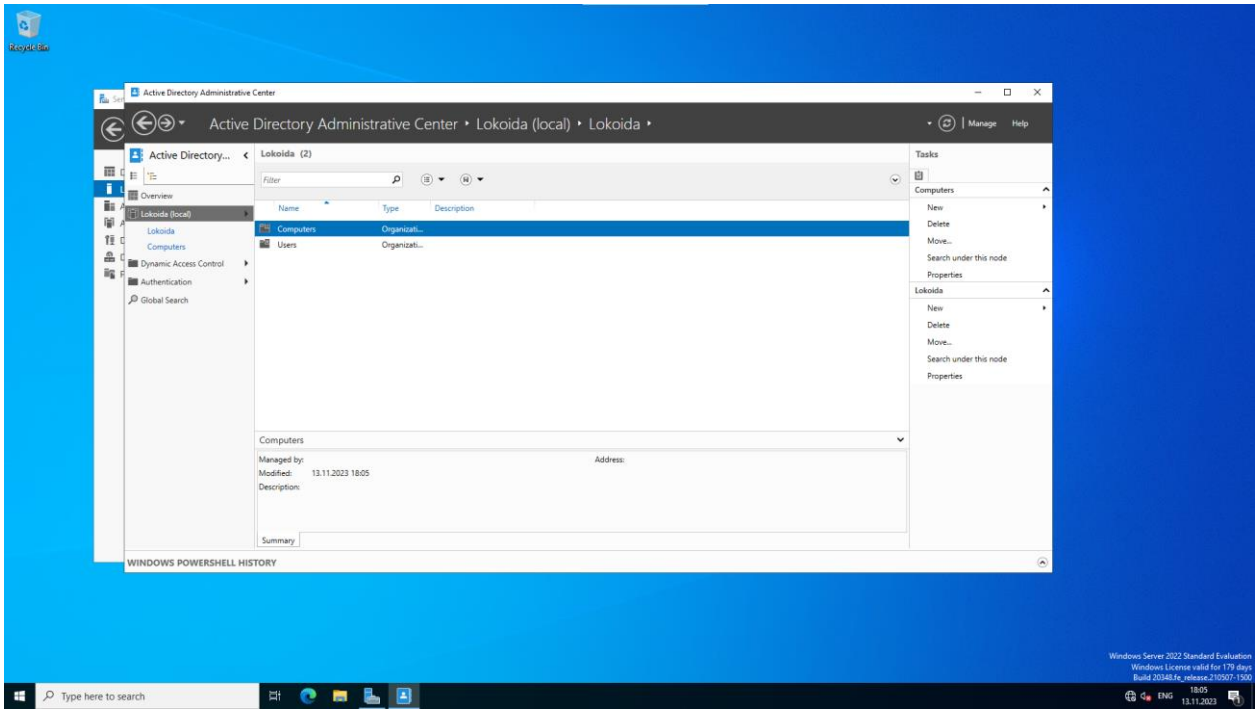


Рисунок 3.35 – Інструмент “Active Directory Administrative Center”

На рисунку 3.36 зображені задані параметри для додавання віртуальної машини до новоствореного домену [27, 28, 29].

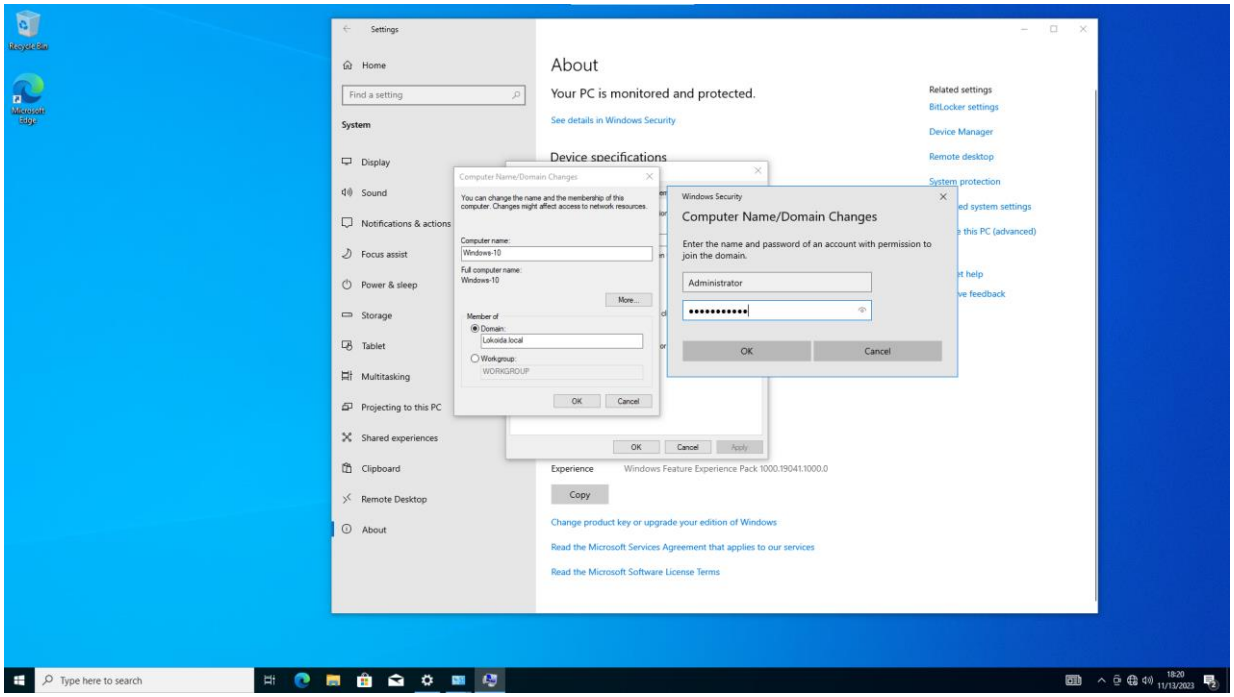


Рисунок 3.36 – Задані параметри для додавання віртуальної машини до новоствореного домену

На рисунку 3.37 зображено успішне додавання віртуальної машини до нового домену [27, 28, 29].

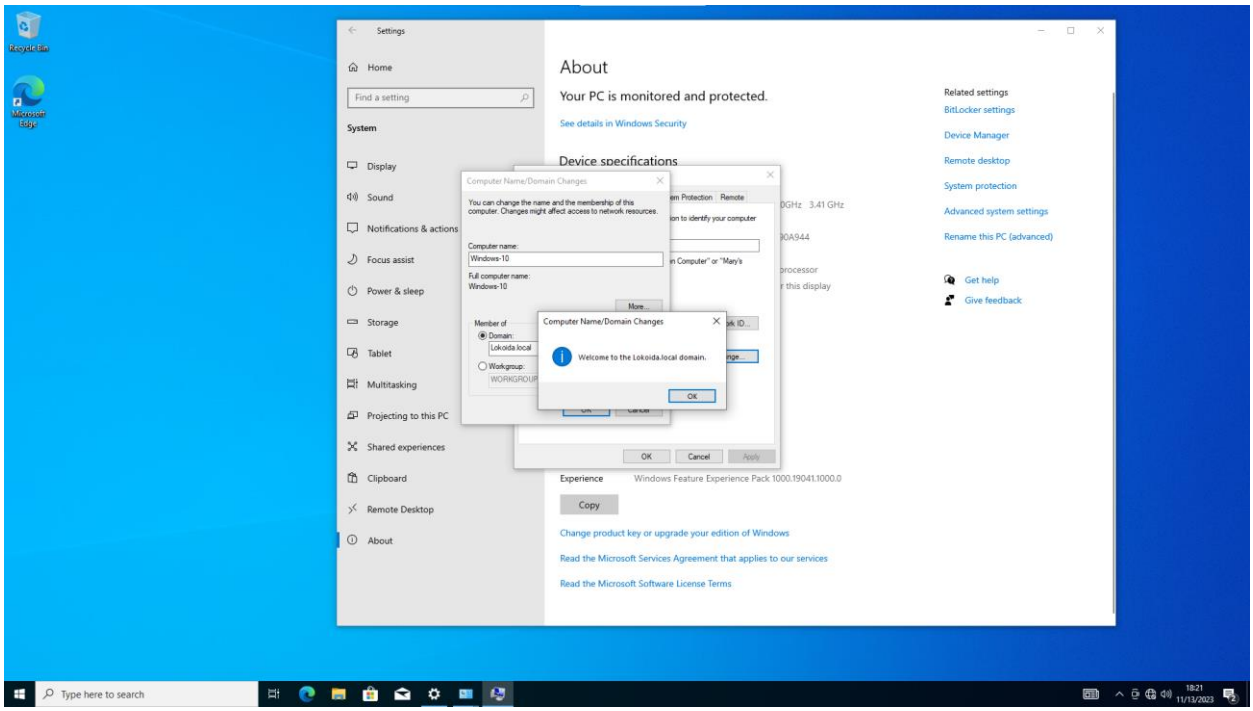


Рисунок 3.37– Успішне додавання віртуальної машини до нового домену

На рисунку 3.38 зображено задані особисті дані та ім'я входу для нового користувача [27, 28, 29].

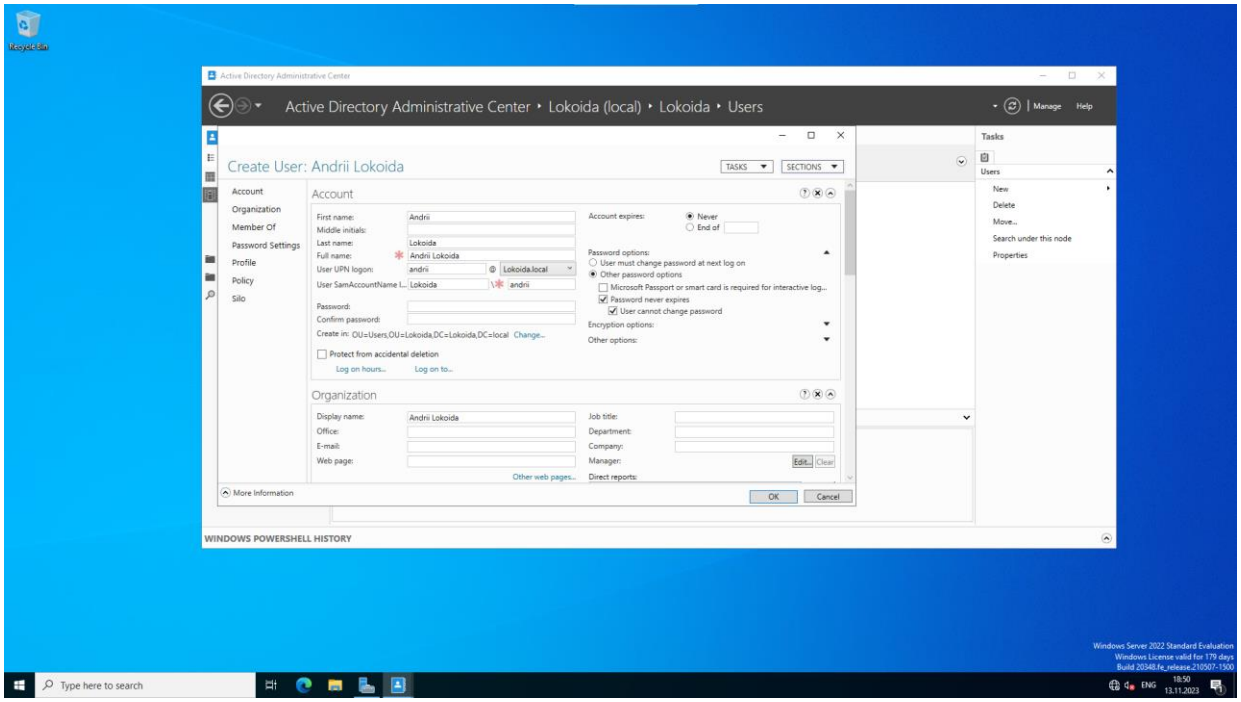


Рисунок 3.38 – Задані особисті дані та ім'я входу для нового користувача

На рисунку 3.39 зображено закінчення створення нового користувача підключеного до контролера домену [27, 28, 29].

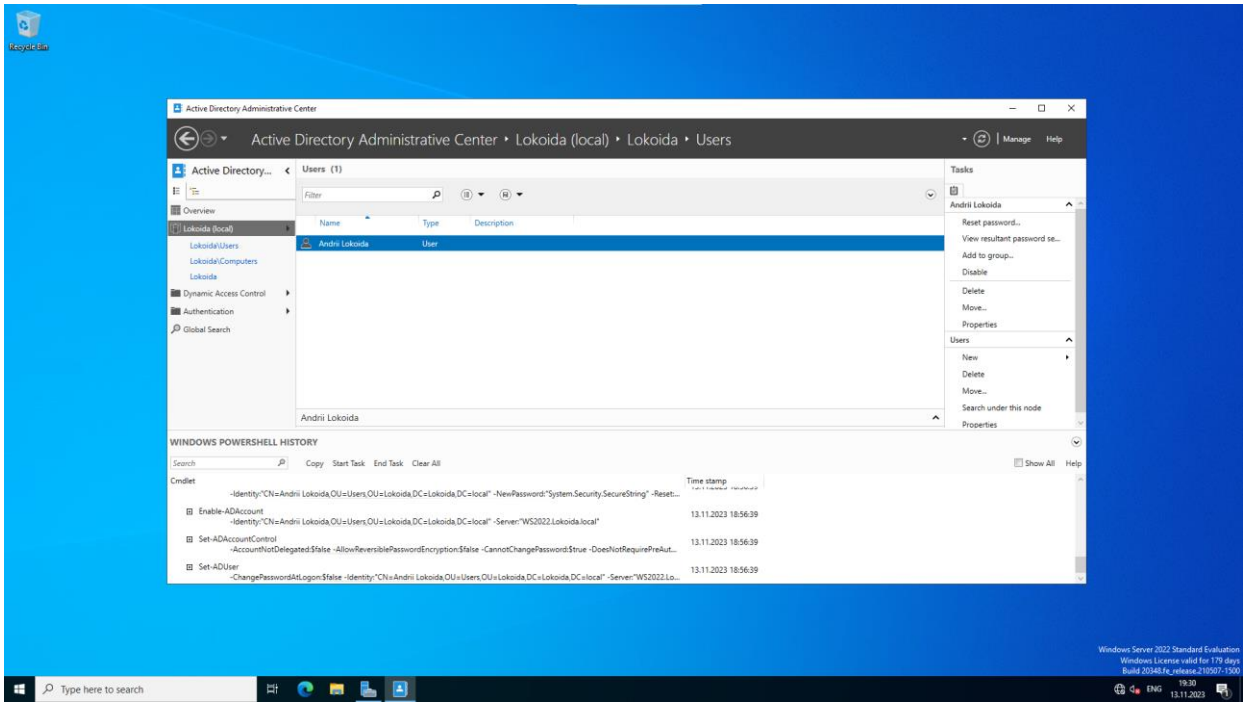


Рисунок 3.39 – Закінчення створення нового користувача підключеного до контролера домену

3.3.3 Розгортання та налаштування DNS-серверу

DNS-сервер у Windows Server 2022 є критично важливим компонентом будь-якої корпоративної мережі, оскільки він забезпечує дозвіл імен у мережі. DNS-сервер відповідає за перетворення доменних імен, таких як www.example.com, на IP-адреси, які використовуються для доступу до комп'ютерів та ресурсів у мережі [27, 28, 29] .

У корпоративній мережі DNS-сервер зазвичай використовується для таких цілей [27, 28, 29] :

1. Дозвіл імен для комп'ютерів та пристроїв у мережі. Це дозволяє користувачам та програмам підключатися до інших комп'ютерів та пристроїв у мережі, використовуючи їхні імена, а не IP-адреси [27, 28, 29].
2. Дозвіл імен для служб та ресурсів у мережі. Це дозволяє користувачам та програмам підключатися до служб та ресурсів у мережі, використовуючи їхні імена, а не IP-адреси [27, 28, 29].
3. Надійність та відмовостійкість мережі. DNS-сервер забезпечує відмовостійкість мережі, надаючи резервні сервери Domain Name System, які можуть використовуватися у разі відмови основного сервера Domain Name System.

DNS-сервер у Windows Server 2022 підтримує такі функції:

- Класичний DNS – це традиційний спосіб роботи DNS-сервера. У цьому режимі сервер зберігає базу даних, яка зіставляє доменні імена з IP-адресами.
- Динамічний DNS - це режим, у якому клієнти можуть оновлювати свої записи DNS. Це спрощує керування DNS-сервером, адже адміністратору не потрібно вручну оновлювати записи для кожного клієнта.
- DNS-запис імен комп'ютерів - це функція, яка дозволяє створювати записи DNS для комп'ютерів у локальній мережі. Це дозволяє користувачам знаходити комп'ютери на ім'я, а не за IP-адресою.

- DNS-запис імен ресурсів – це функція, яка дозволяє створювати записи DNS для ресурсів у мережі, таких як веб-сайти, сервери додатків тощо.
- DNS-запис імен зон – це функція, яка дозволяє створювати записи DNS для зон у мережі. Зона - це частина мережі, для якої використовується один сервер DNS.

На рисунку 3.40 зображено вибраний тип установки "Role-based or feature-based installation”.

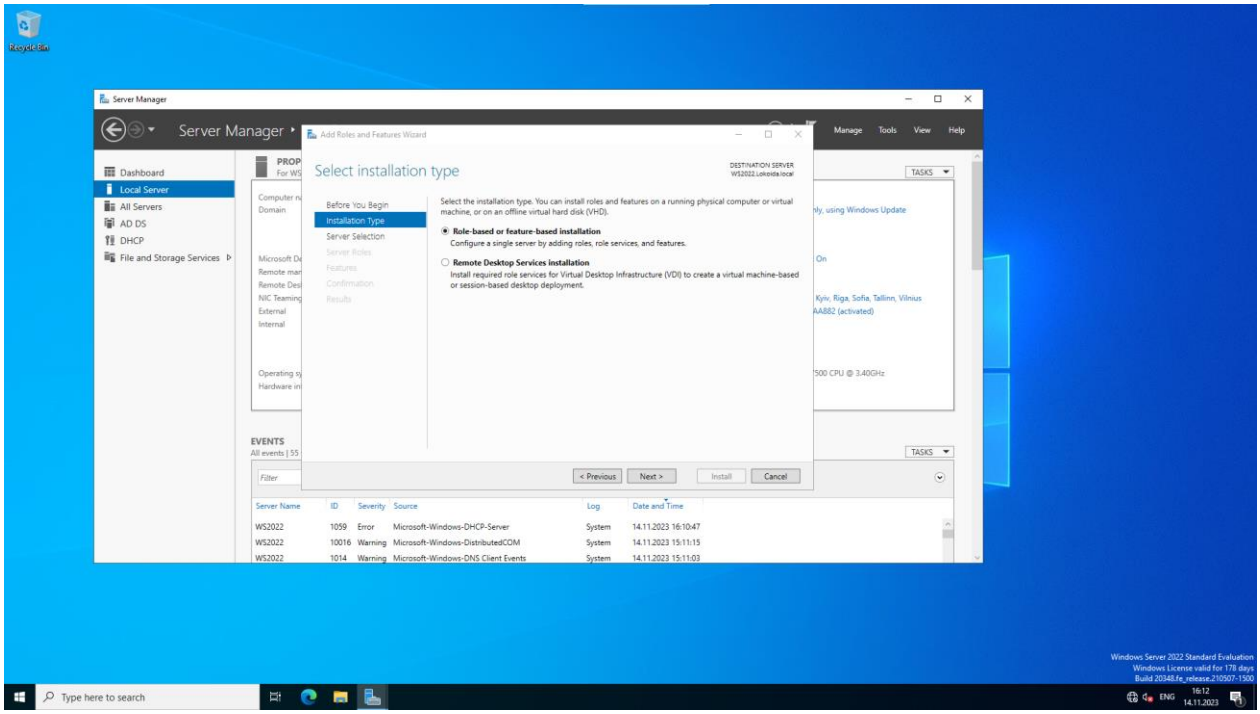


Рисунок 3.40 – Вибраний тип установки "Role-based or feature-based installation”

На рисунку 3.41 зображено сервер, на який буде проводитися установка ролей.

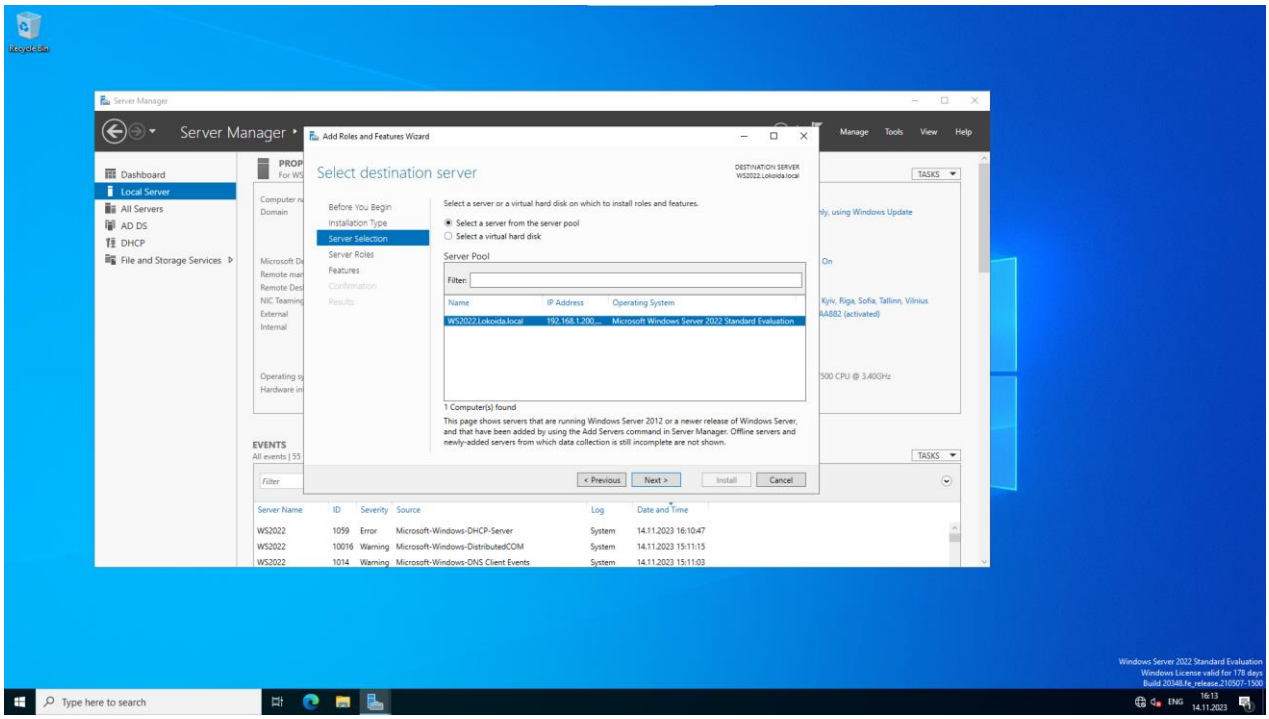


Рисунок 3.41 – Вибраний сервер на який буде проводитися установка ролей

На рисунку 3.42 зображено вибрану роль для сервера.

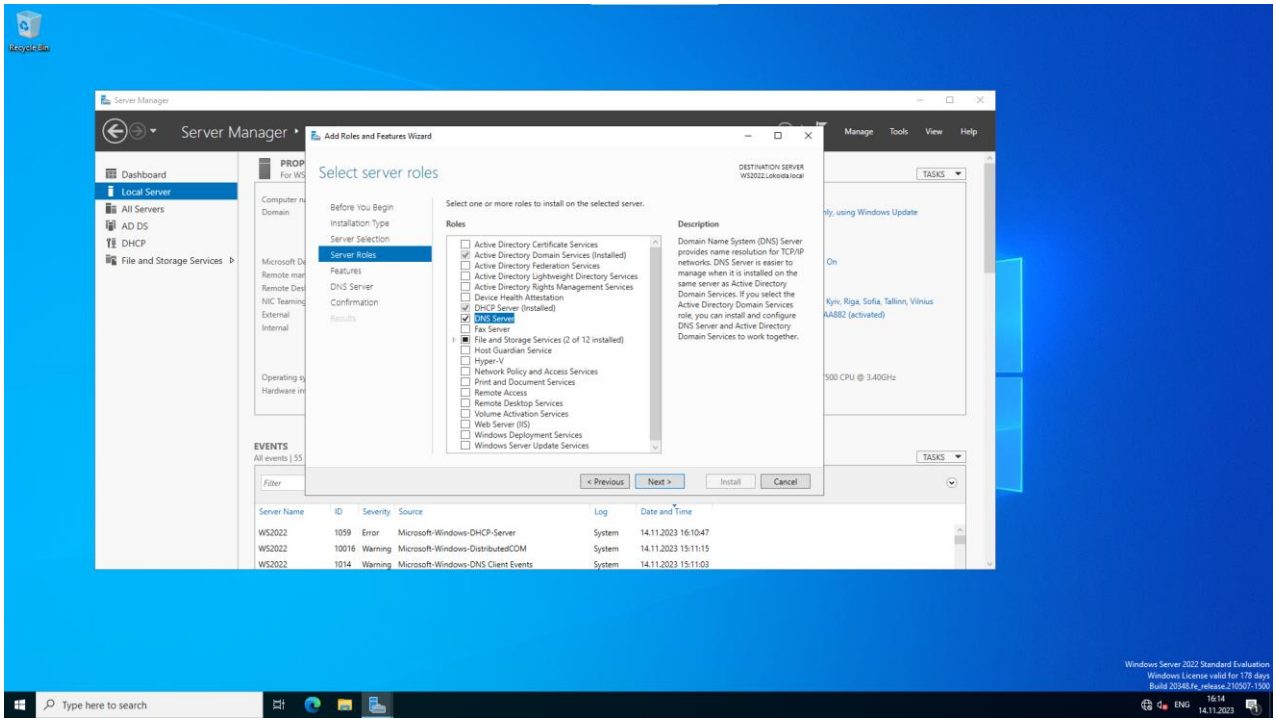


Рисунок 3.42 – Вибрана роль для сервера

На рисунку 3.43 зображено обраного компонента.

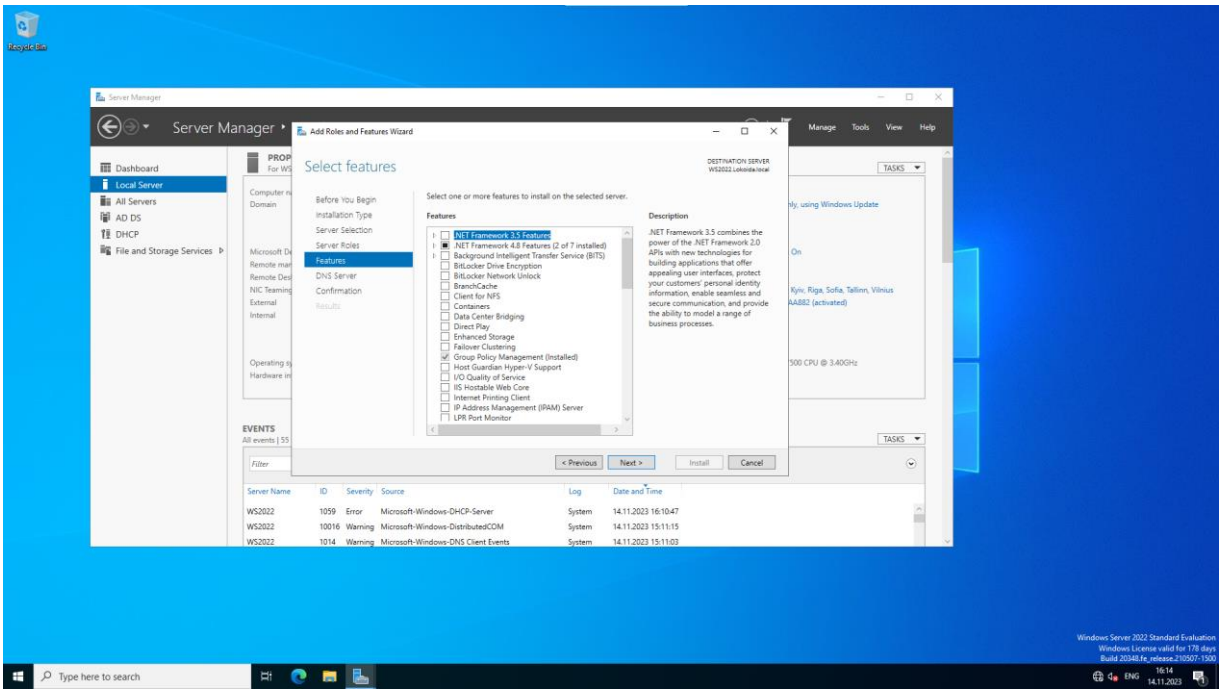


Рисунок 3.43 – Обраний компонент

На рисунку 3.44 зображено попередження DNS-сервера.

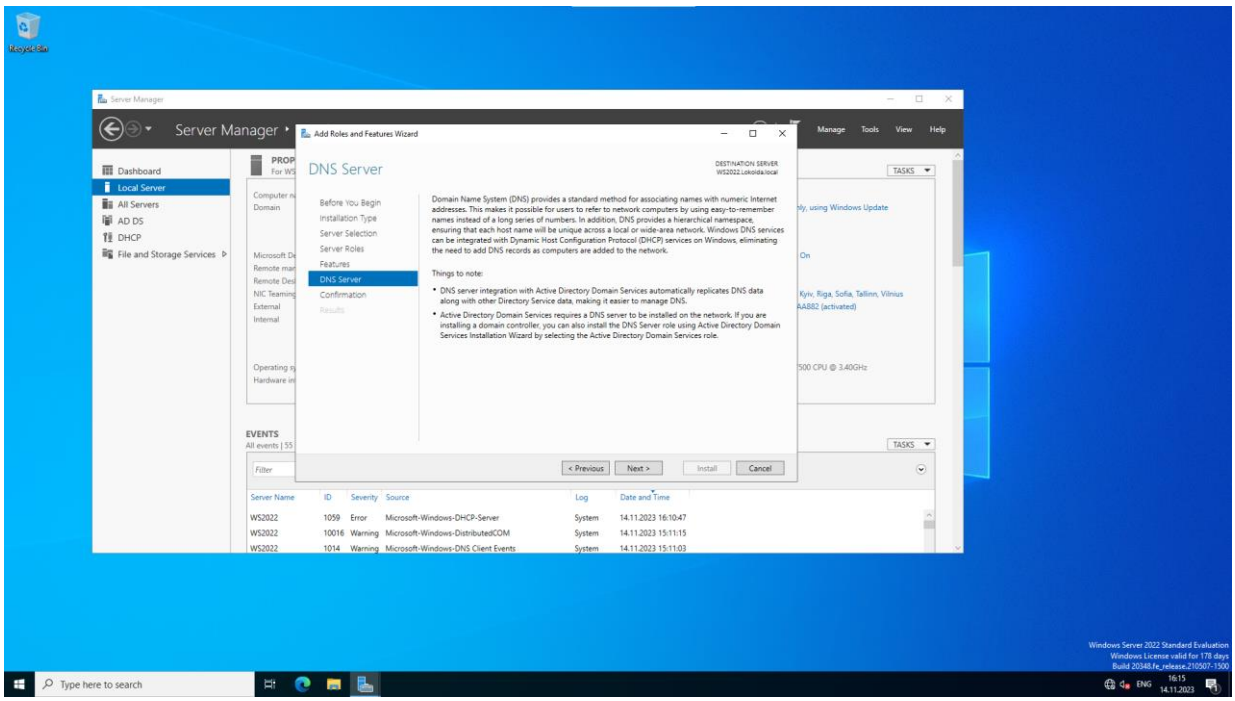


Рисунок 3.44 – Попередження DNS-сервера

На рисунку 3.45 зображено підсумок обраної ролі і компонентів.

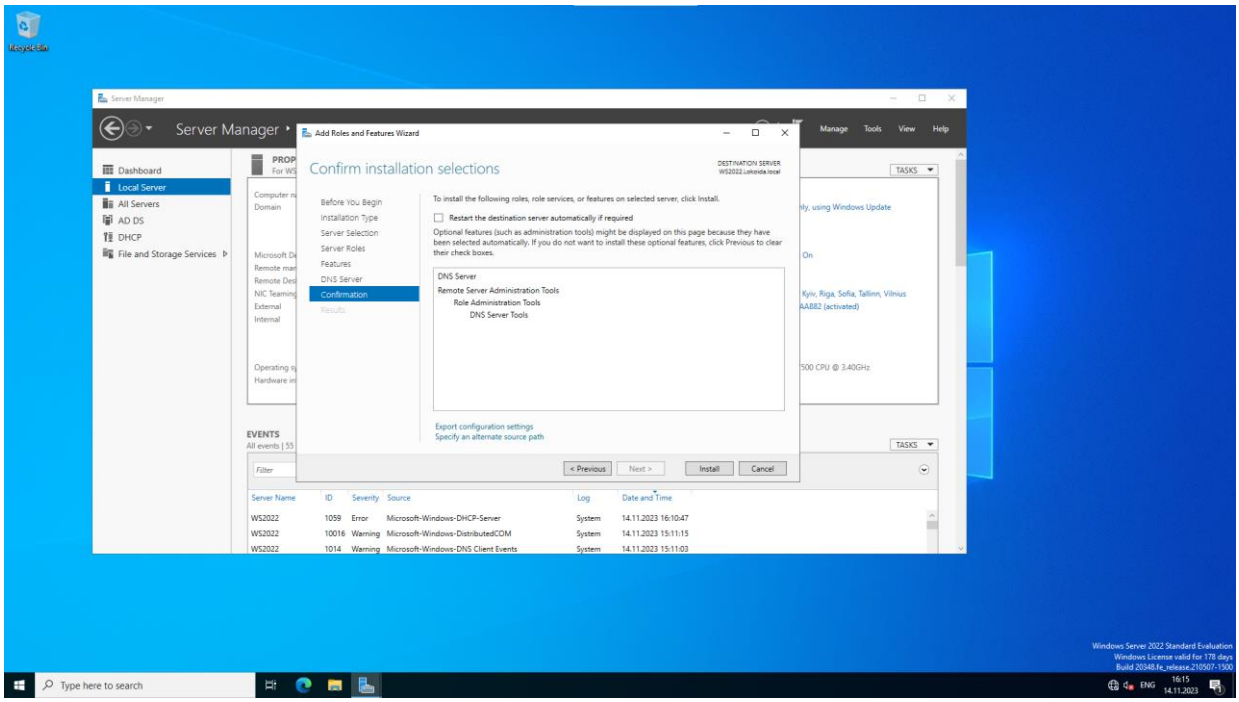


Рисунок 3.45 – Підсумок обраної ролі і компонентів

На рисунку 3.46 зображено процес встановлення обраної ролі і необхідних компонентів.

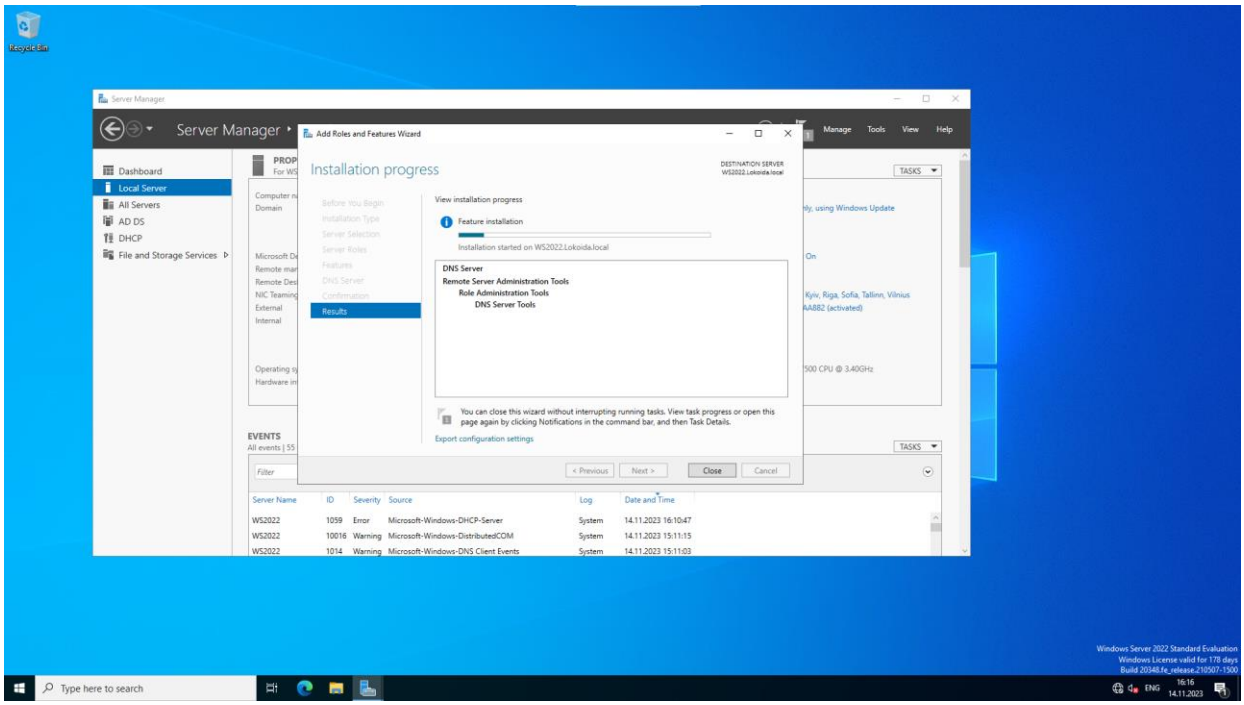


Рисунок 3.46 – Процес встановлення обраної ролі і необхідних компонентів

На рисунку 3.47 зображено закінчення встановлення обраної ролі і необхідних компонентів.

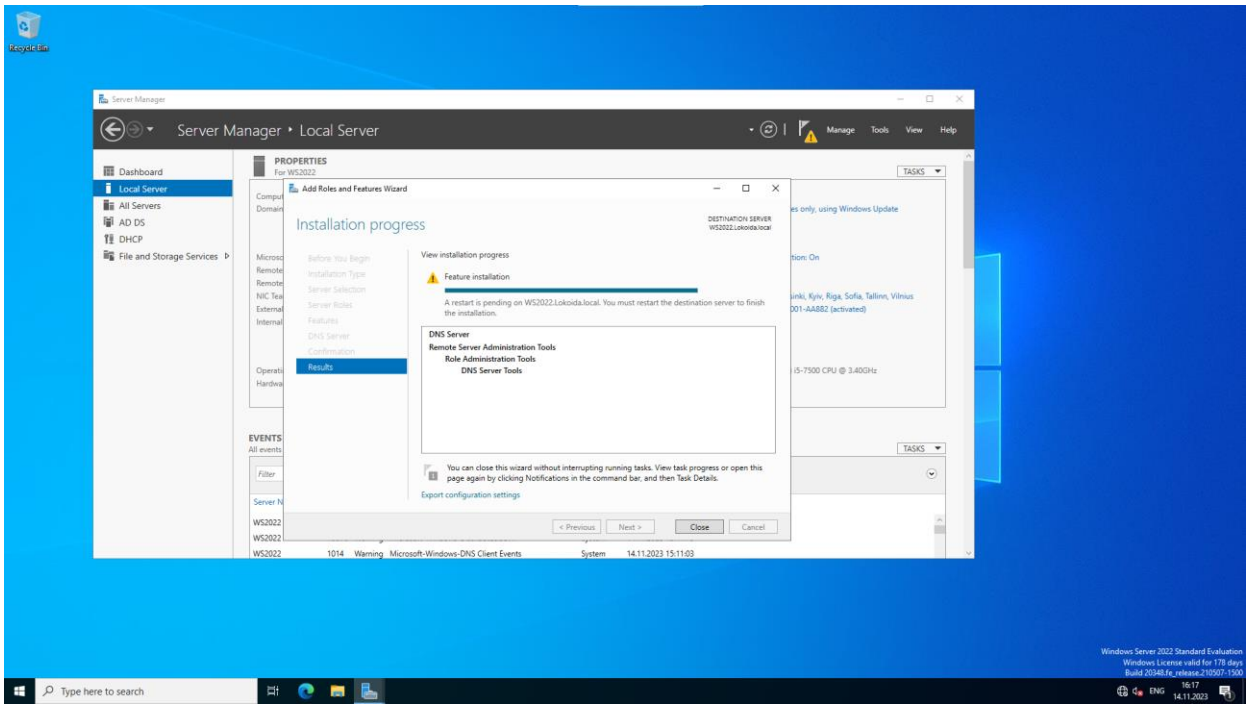


Рисунок 3.47 – Закінчення встановлення обраної ролі і необхідних компонентів

На рисунку 3.48 зображено майстер створення нової зони.

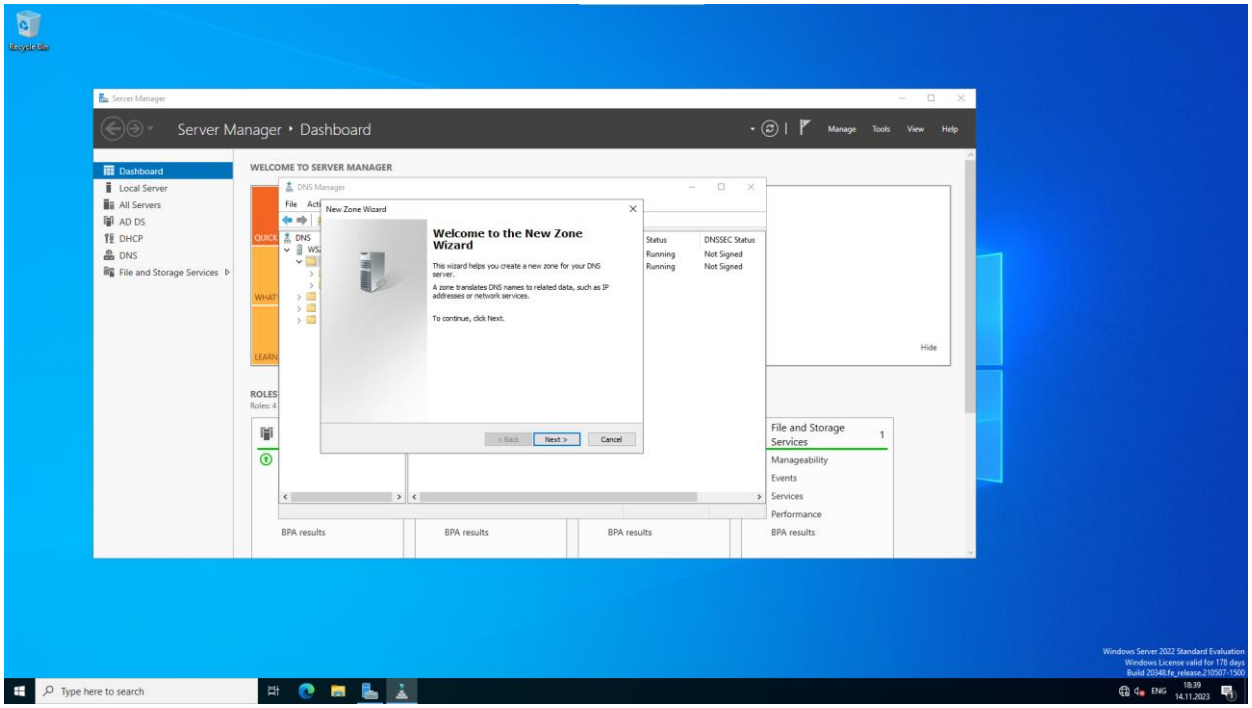


Рисунок 3.48 – Майстер створення нової зони

На рисунку 3.49 зображено тип обраної зони і збереження її в домені контролера.

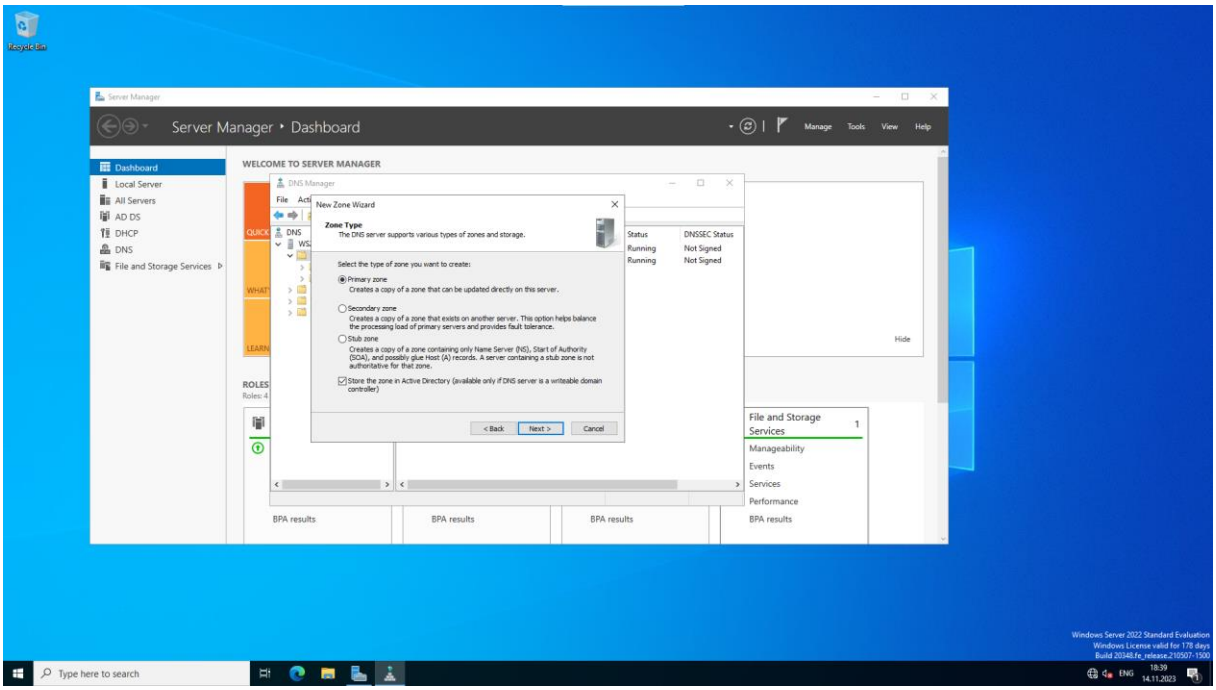


Рисунок 3.49 – Тип обраної зони

На рисунку 3.50 зображено вибрану область реплікації домену контролера.

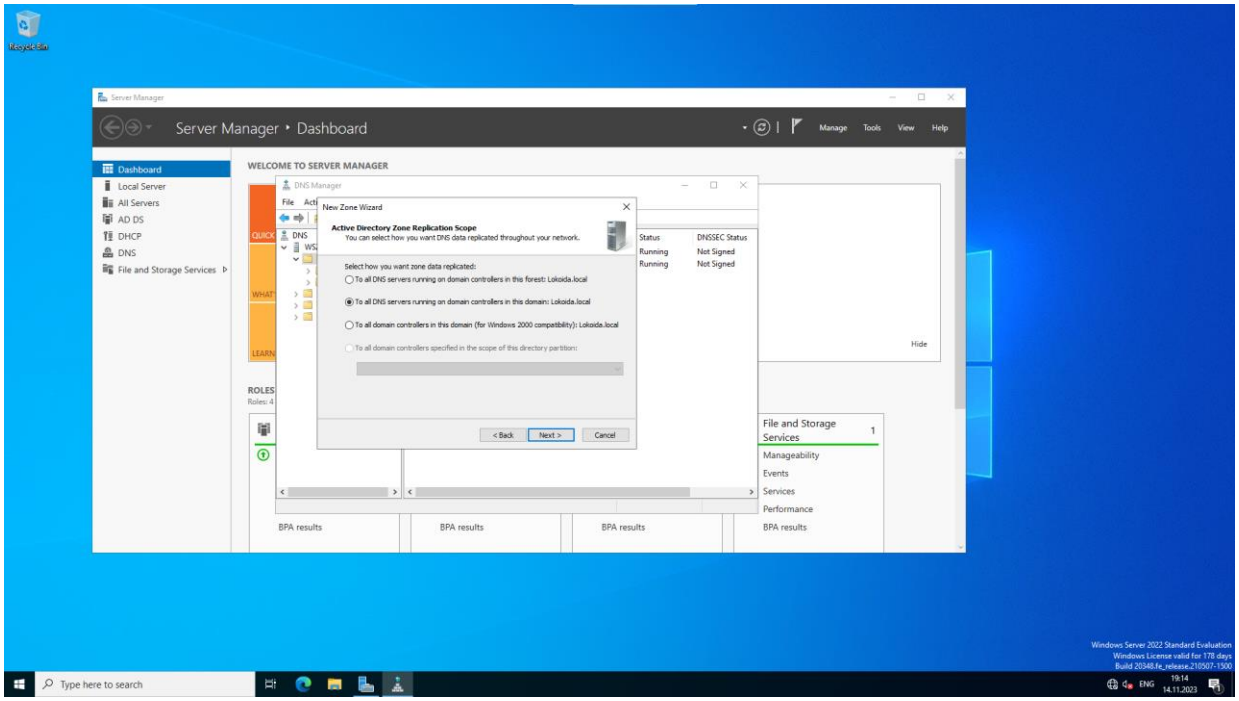


Рисунок 3.50 – Область реплікації домену контролера

На рисунку 3.51 зображено задану назву для нової зони.

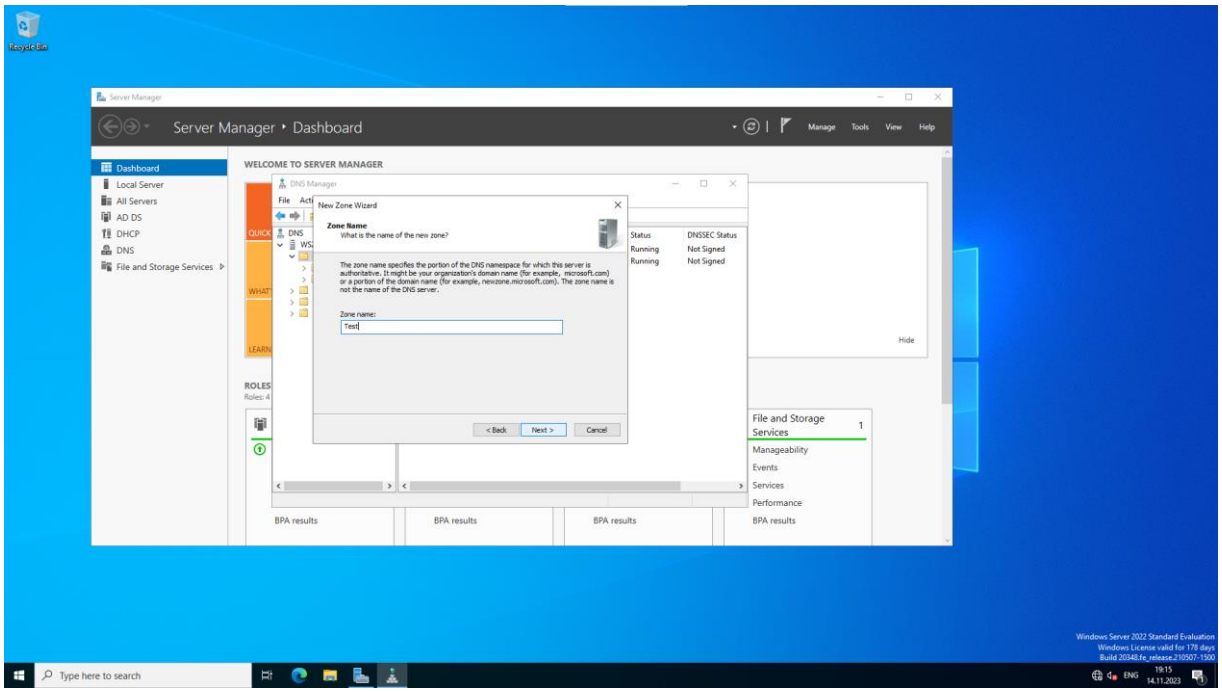


Рисунок 3.51 – Задана назва для нової зони

На рисунку 3.52 зображено вказаний тип динамічного оновлення зони.

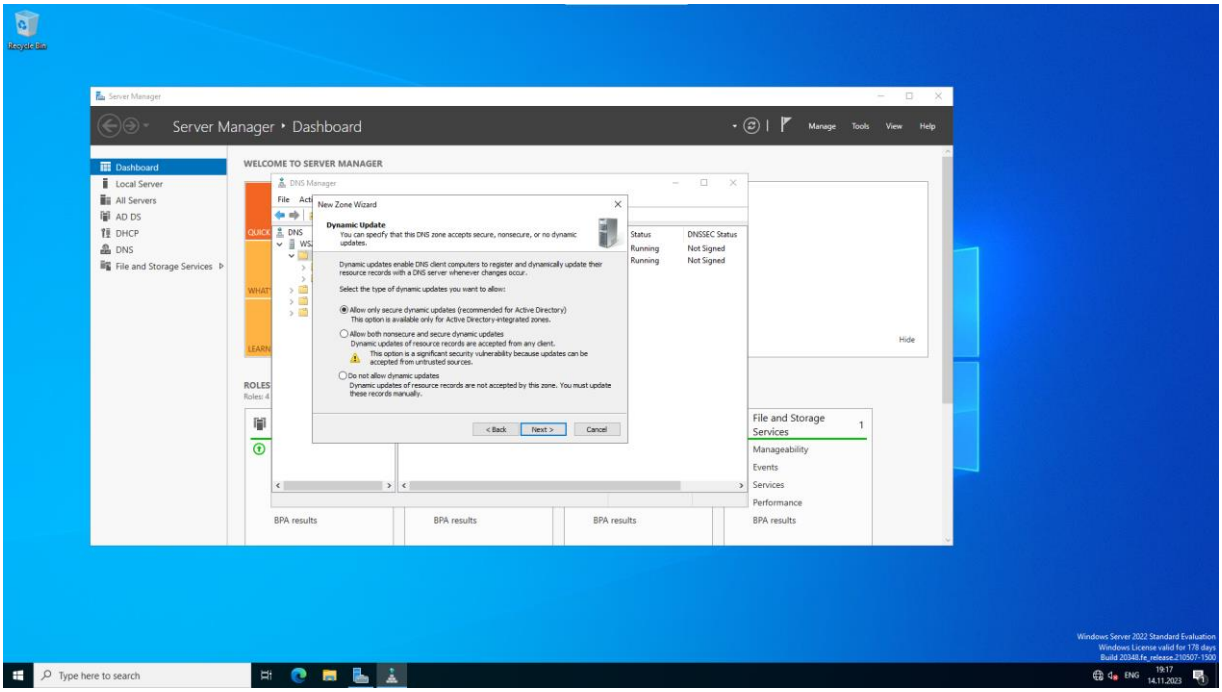


Рисунок 3.52 – Тип динамічного оновлення зони

На рисунку 3.53 зображено завершення налаштування прямої зони.

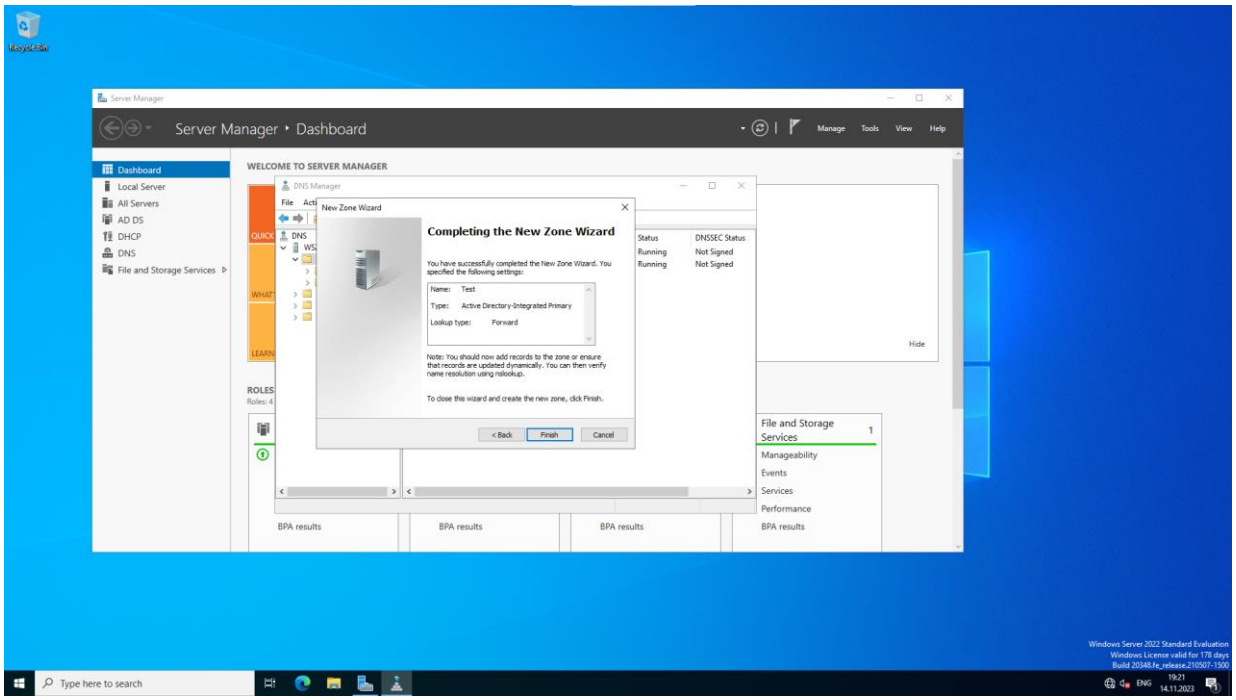


Рисунок 3.53 – Завершення налаштування прямої зони

На рисунку 3.54 зображено майстер створення нової зони.

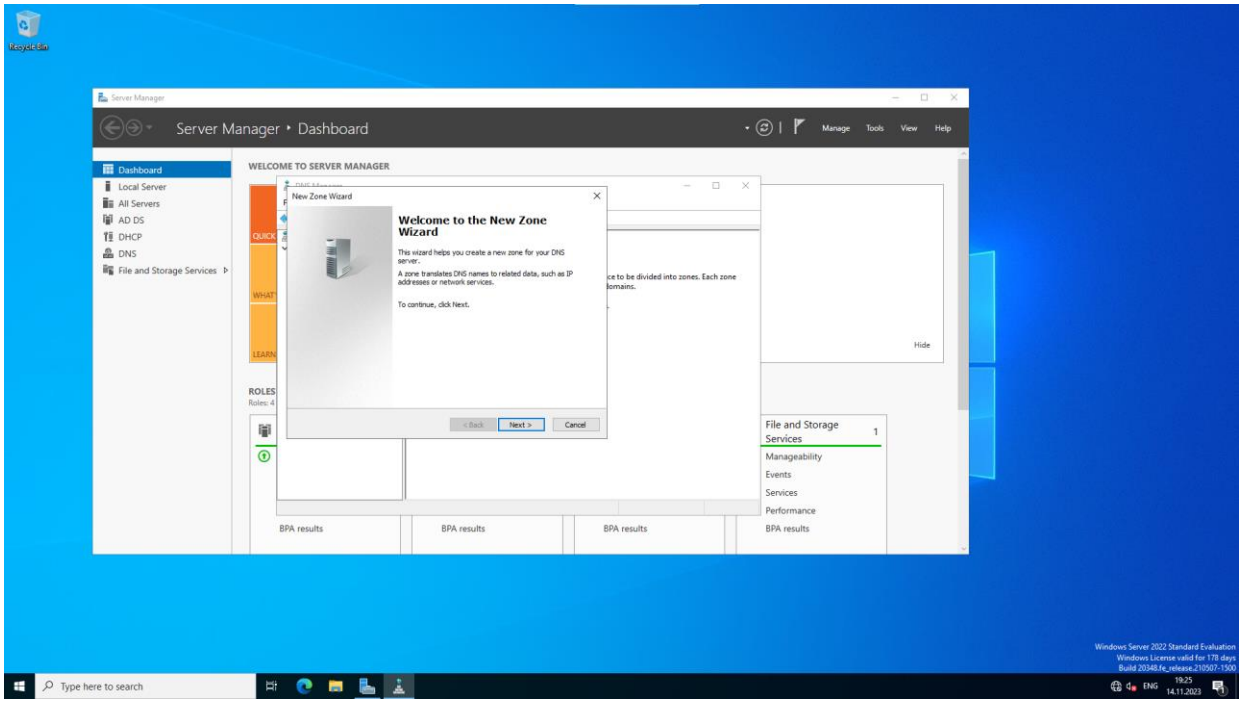


Рисунок 3.54 – Майстер створення нової зони

На рисунку 3.55 зображено тип обраної зони і збереження її в домені контролера.

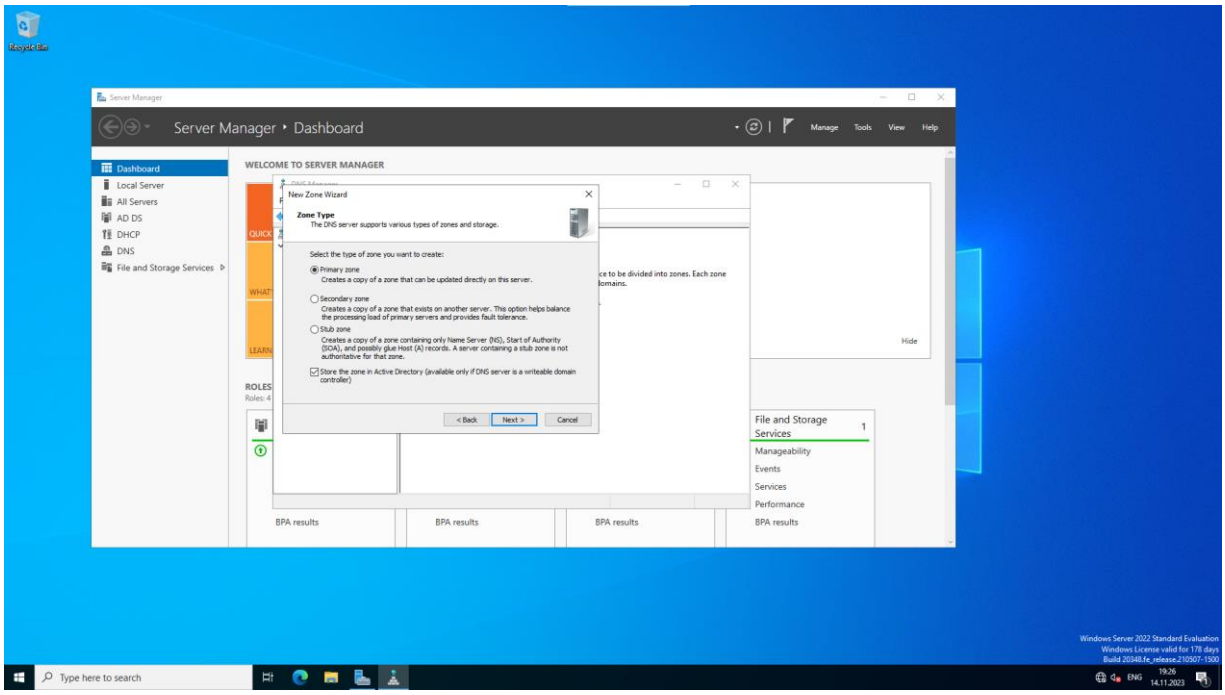


Рисунок 3.55 – Тип обраної зони і збереження її в домені контролера

На рисунку 3.56 зображено вибрану область реплікації домену контролера.

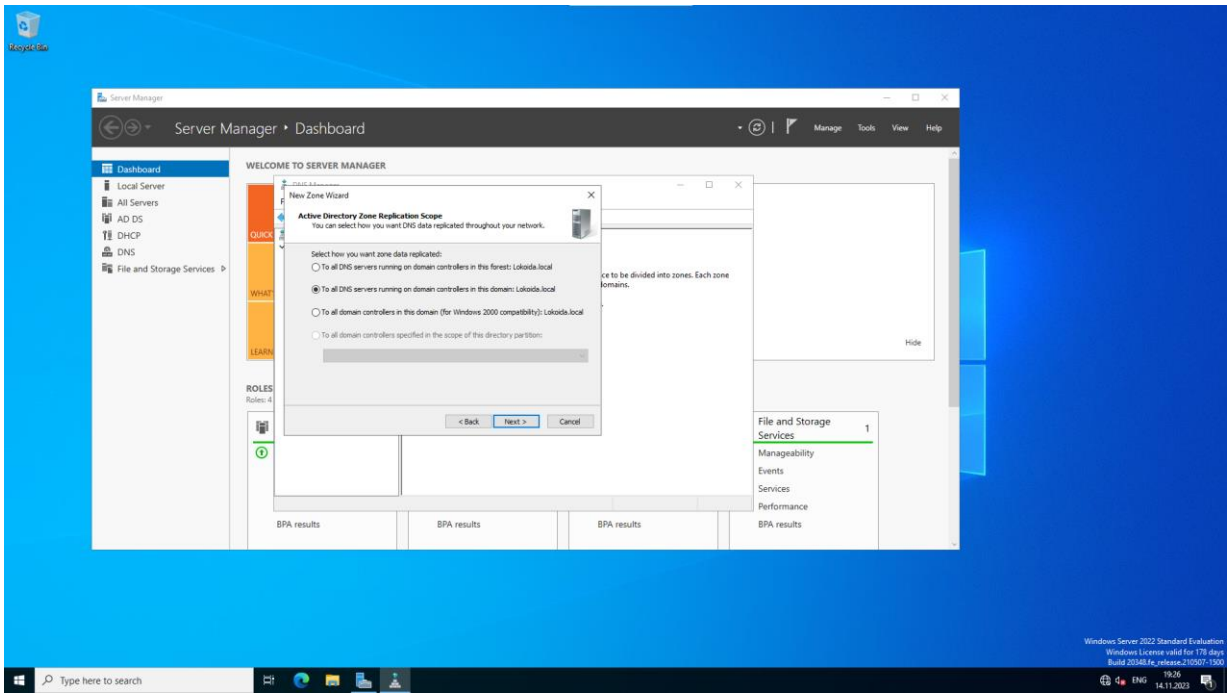


Рисунок 3.56 – Вибрану область реплікації домену контролера

На рисунку 3.57 зображено обране призначення для адрес IPv4.

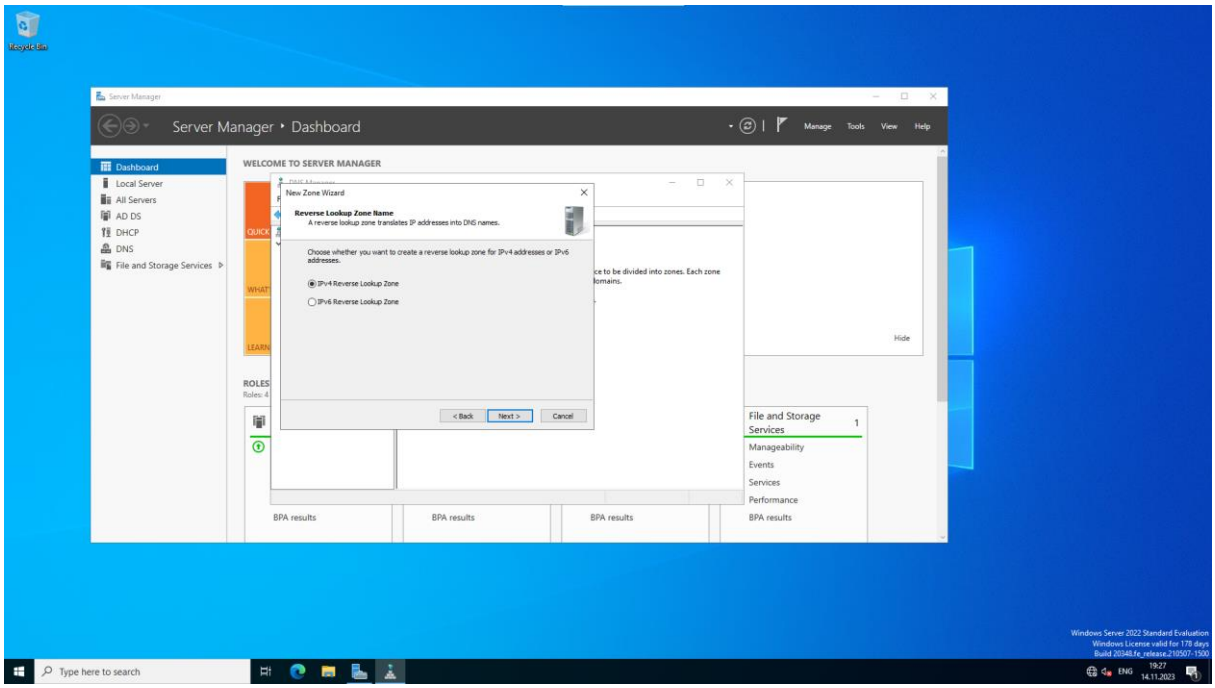


Рисунок 3.57 – Призначення для адрес IPv4

На рисунку 3.58 зображено вказаний ідентифікатор мережі.

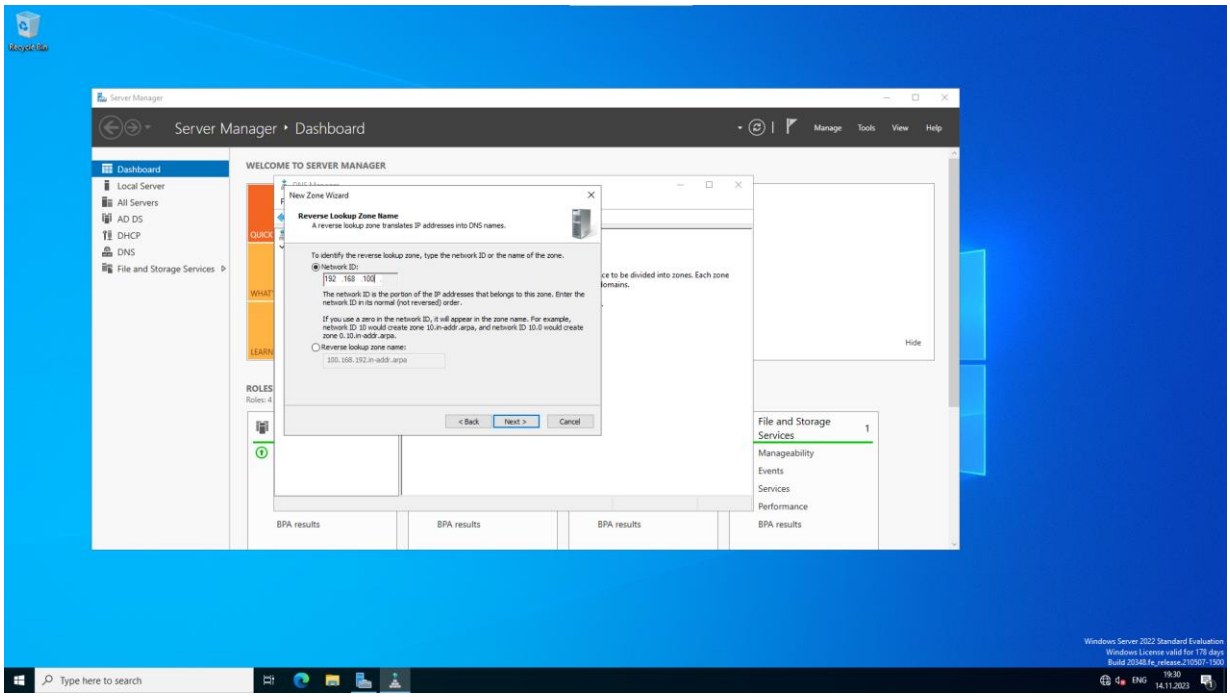


Рисунок 3.58 – Вказаний ідентифікатор мережі

На рисунку 3.59 зображено вказаний тип динамічного оновлення зони.

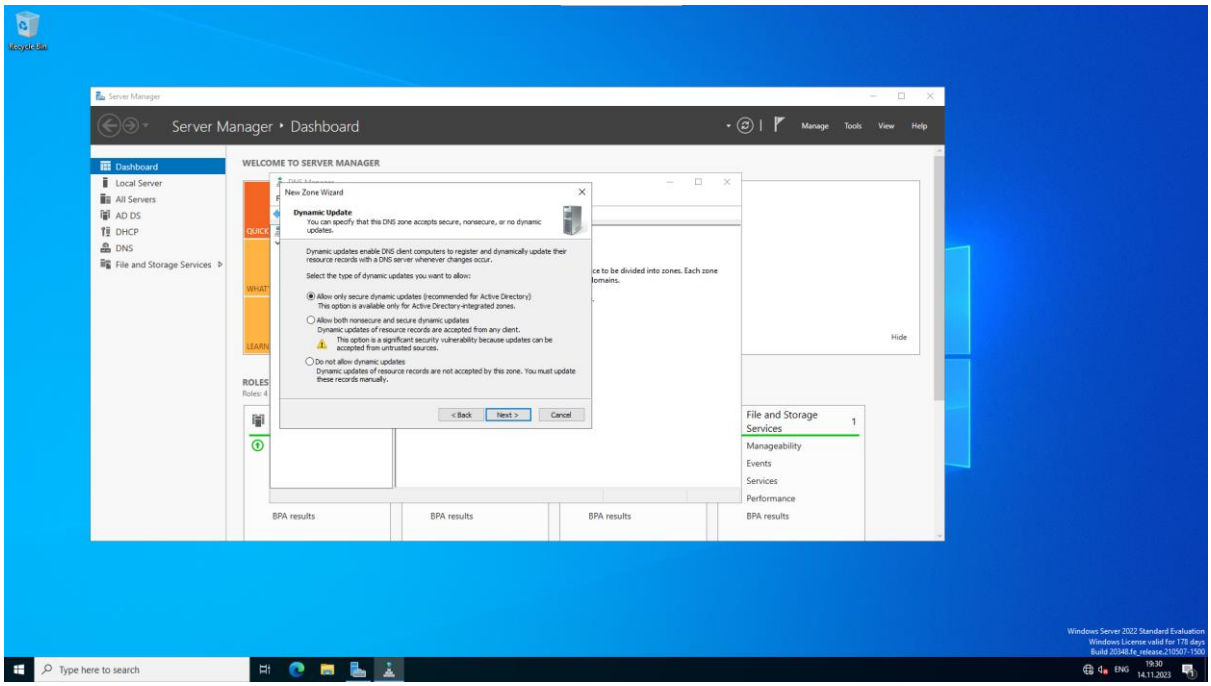


Рисунок 3.59 – Тип динамічного оновлення зони

На рисунку 3.60 зображено завершення налаштування зворотної зони.

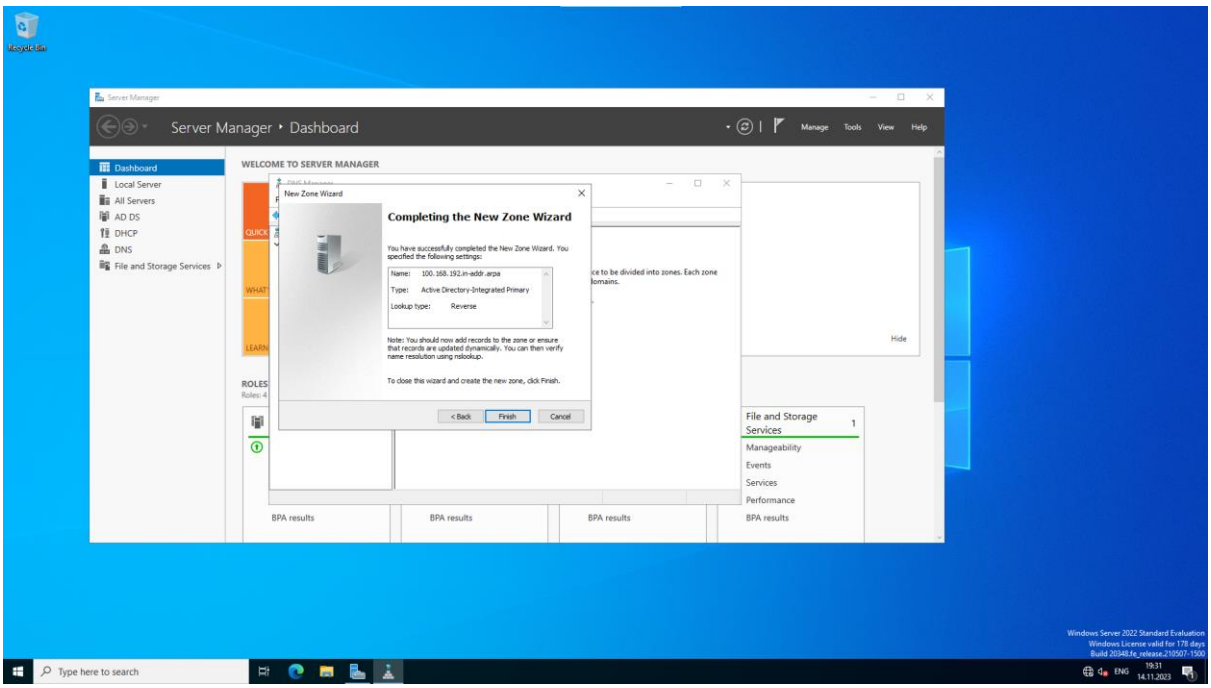


Рисунок 3.60 – Завершення налаштування зворотної зони

На рисунку 3.61 зображена створена зона зворотнього перегляду.

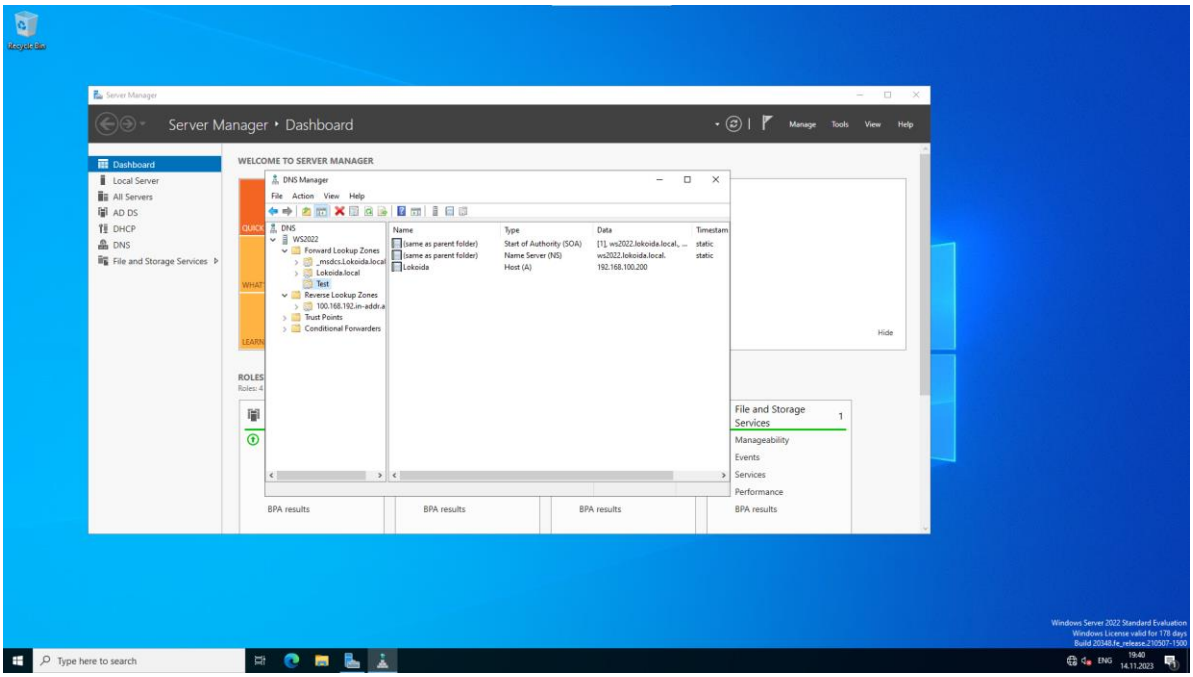


Рисунок 3.61 – Зона зворотнього перегляду

На рисунку 3.62 зображено перевірку роботи прямої та зворотньої зони.

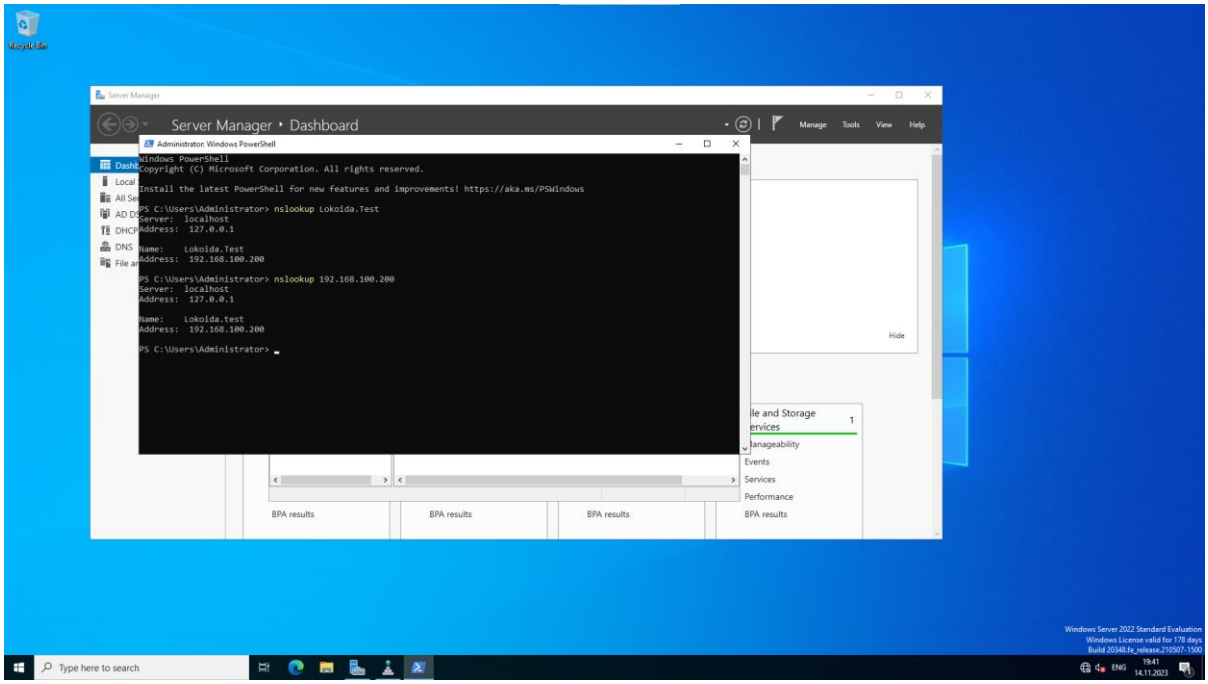


Рисунок 3.62 – Перевірка роботи прямої та зворотньої зони

3.3.4 Розгортання та налаштування RRAS

RRAS – це служба, яка дозволяє Windows Server 2022 виконувати функції маршрутизатора та віддаленого доступу. Вона може використовуватися для централізованого управління корпоративною мережею, надаючи такі можливості:

1. Централізоване керування маршрутизацією: RRAS дозволяє адміністраторам централізовано керувати маршрутизацією в корпоративній мережі. Це може бути корисним для забезпечення узгодженості маршрутизації та для спрощення управління маршрутизаторами.

2. Централізоване керування віддаленим доступом: RRAS дозволяє адміністраторам централізовано керувати віддаленим доступом до корпоративної мережі. Це може бути корисним для забезпечення безпеки та для спрощення керування віддаленими користувачами.

RRAS дозволяє адміністраторам централізовано керувати маршрутизацією в корпоративній мережі за допомогою таких функцій:

- Планування маршрутизації: RRAS надає інструменти для планування маршрутизації, які допомагають адміністраторам визначити оптимальну конфігурацію маршрутизації для корпоративної мережі.
- Конфігурація маршрутизації: RRAS дозволяє адміністраторам централізовано конфігурувати маршрутизацію корпоративної мережі.
- Моніторинг маршрутизації: RRAS надає інструменти моніторингу маршрутизації, які допомагають адміністраторам відстежувати стан маршрутизації в корпоративній мережі.

RRAS дозволяє адміністраторам централізовано керувати віддаленим доступом до корпоративної мережі за допомогою таких функцій:

- Конфігурація віддаленого доступу: RRAS дозволяє адміністраторам централізовано конфігурувати віддалений доступ до корпоративної мережі.
- Моніторинг віддаленого доступу: RRAS надає інструменти для моніторингу віддаленого доступу, які допомагають адміністраторам відстежувати стан віддаленого доступу в корпоративній мережі.

На рисунку 3.63 зображено вибраний тип установки "Role-based or feature-based installation”.

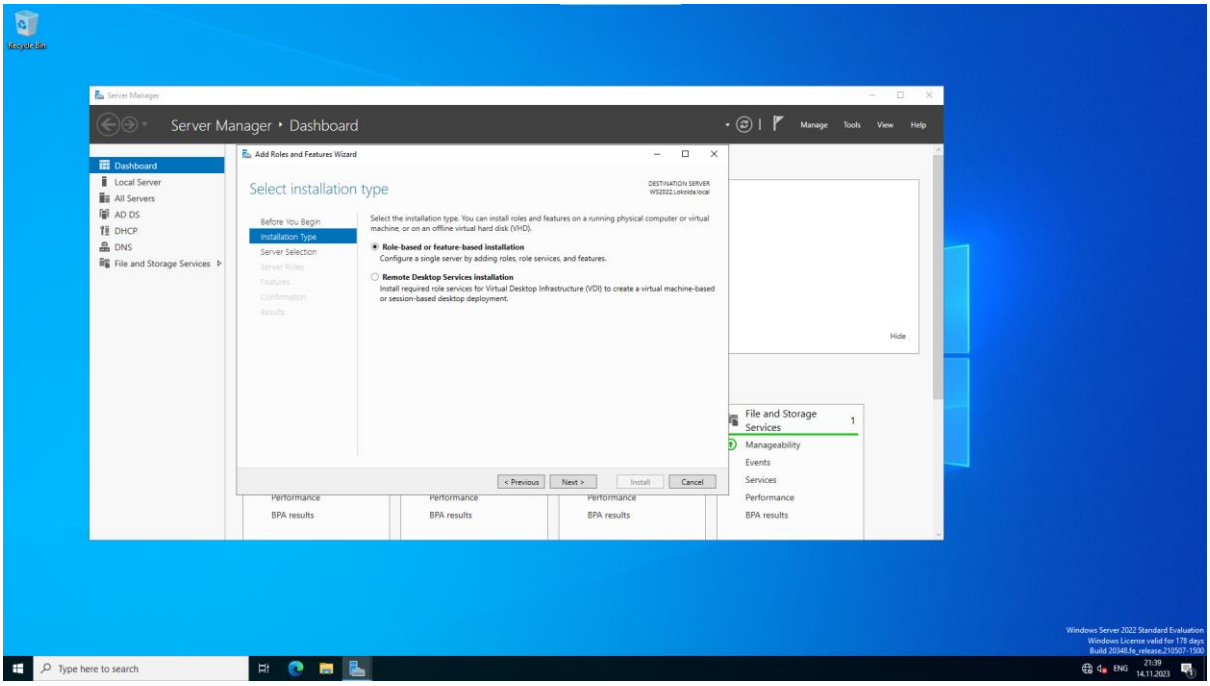


Рисунок 3.63 – Вибраний тип установки

На рисунку 3.64 зображено сервер, на який буде проводитися установка ролі.

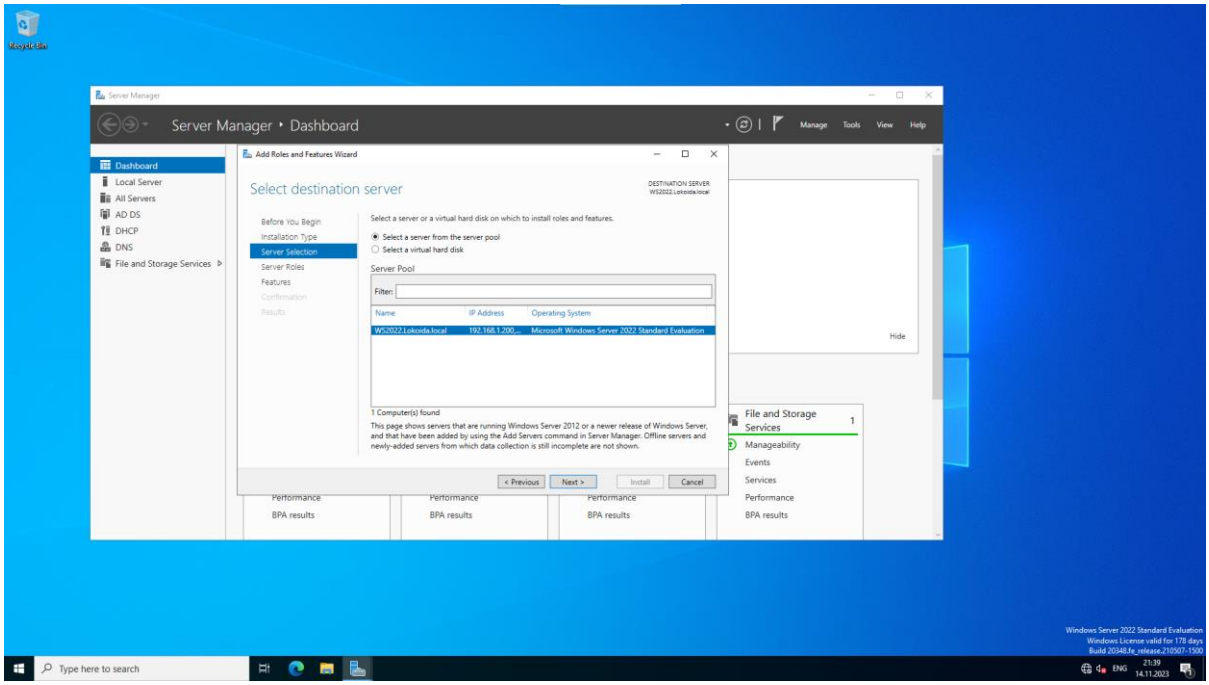


Рисунок 3.64 – Вибраний сервер на який буде проводитися установка ролі

На рисунку 3.65 зображено вибрану роль для сервера.

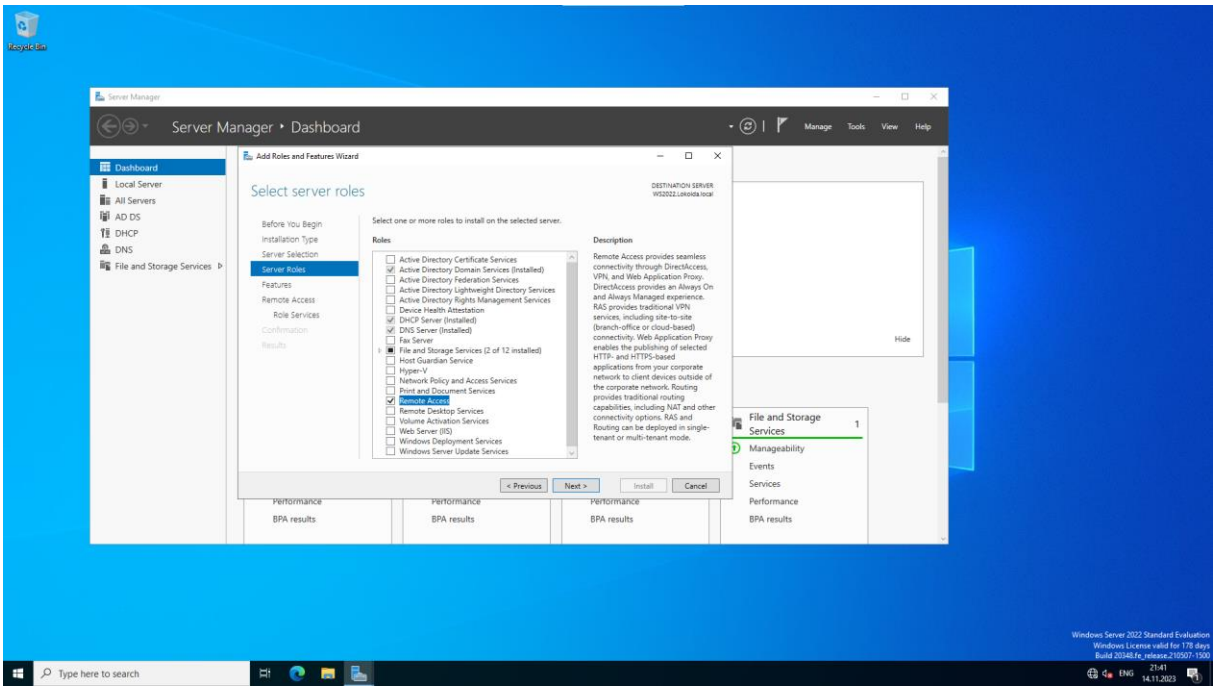


Рисунок 3.65 – Вибрана роль для сервера

На рисунку 3.66 зображено вибір необхідного компонента.

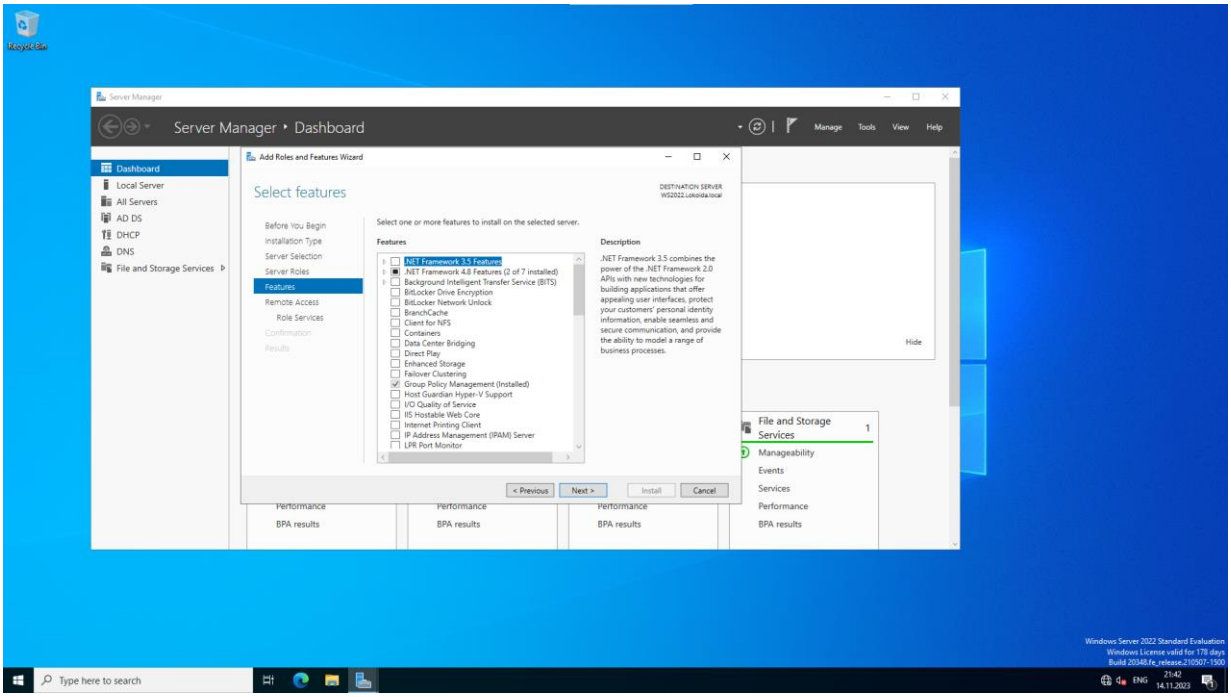


Рисунок 3.66 – Вибір необхідного компонента

На рисунку 3.67 зображено опис ролі віддаленого доступу.

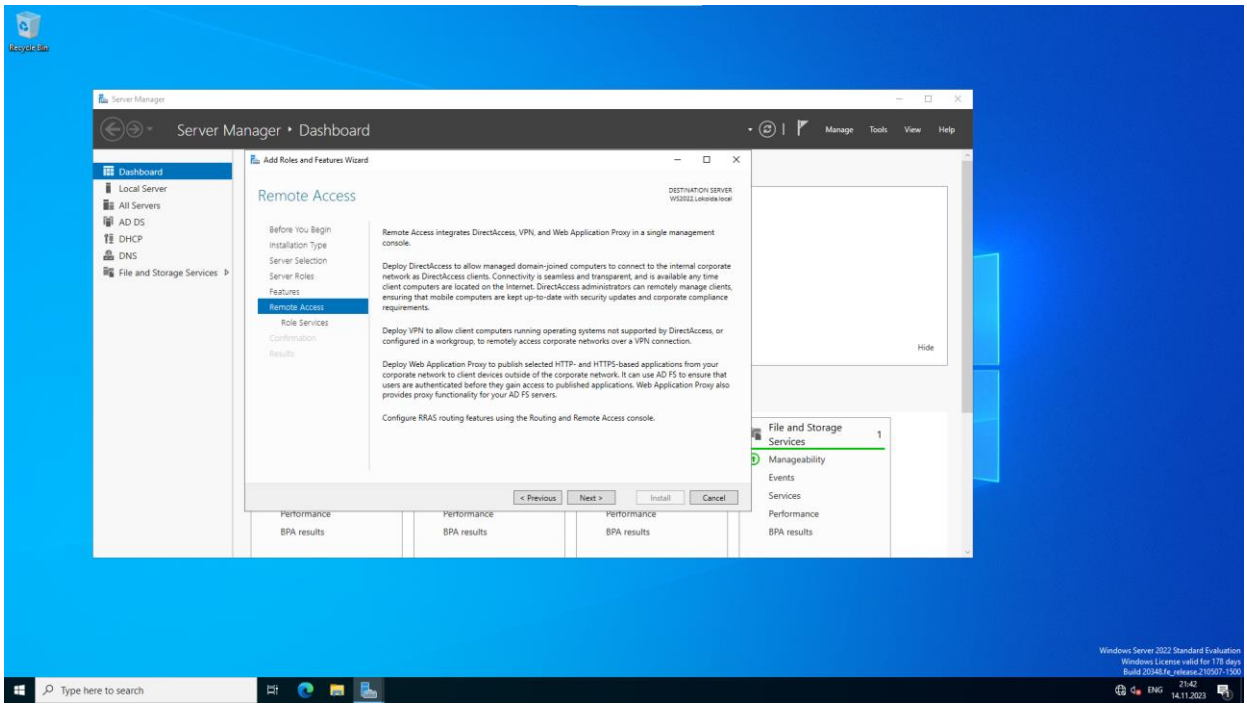


Рисунок 3.67 – Опис ролі віддаленого доступу

На рисунку 3.68 зображено вибрані "служби ролей" ролі віддаленого доступу.

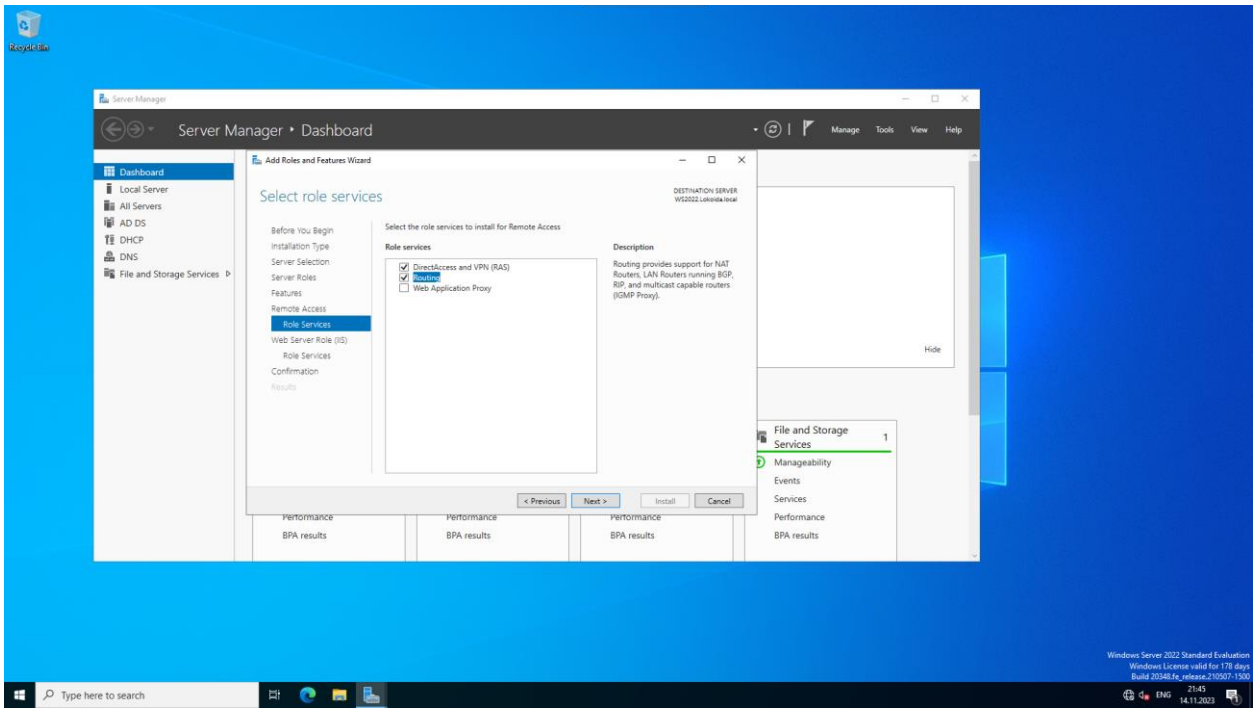


Рисунок 3.68 – Вибрані "служби ролей" ролі віддаленого доступу

На рисунку 3.69 зображено опис ролі веб серверу.

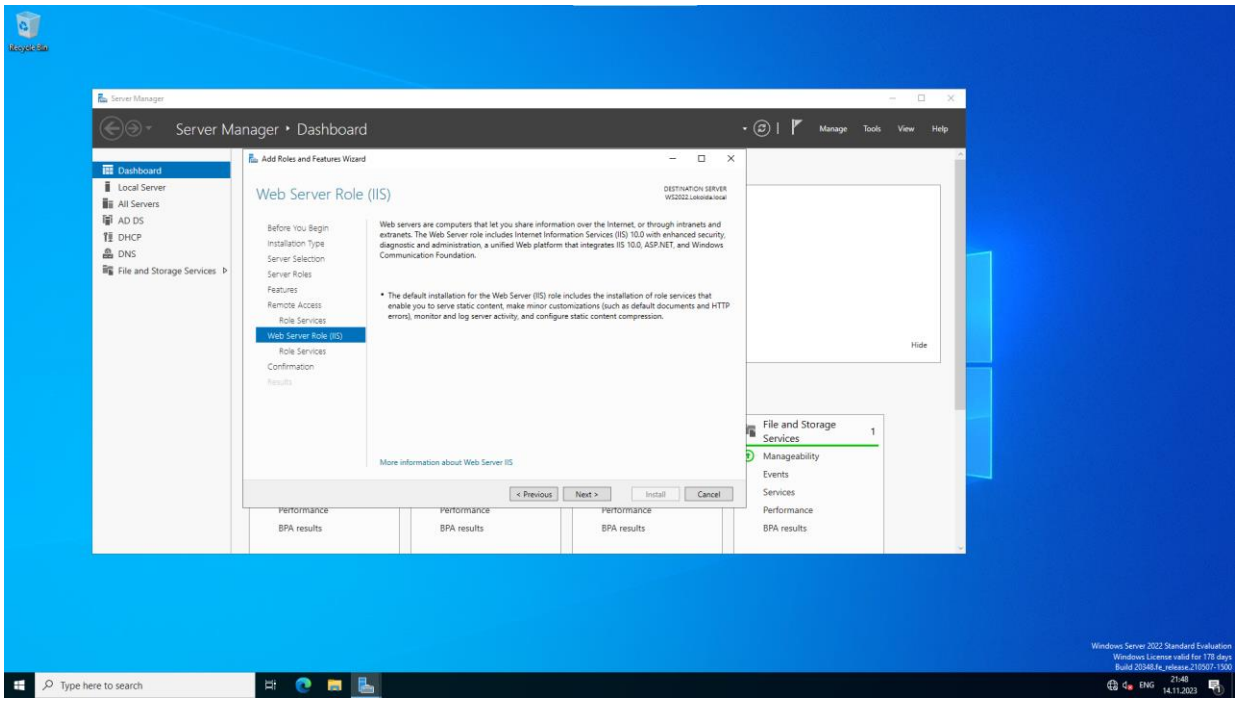


Рисунок 3.69 – Опис ролі веб серверу

На рисунку 3.70 зображено вибрані "служби ролей" ролі веб серверу.

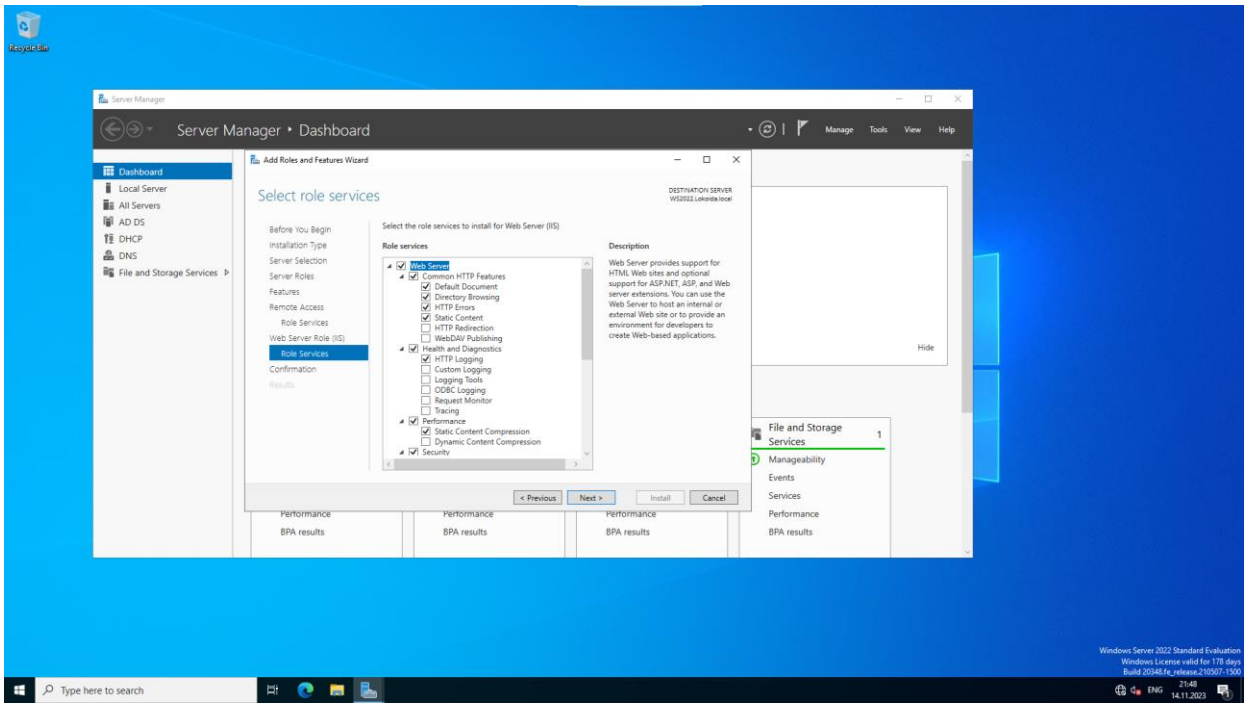


Рисунок 3.70 – Вибрані "служби ролей" ролі веб серверу

На рисунку 3.71 зображено остаточне підтвердження вибраних ролей і компонетів.

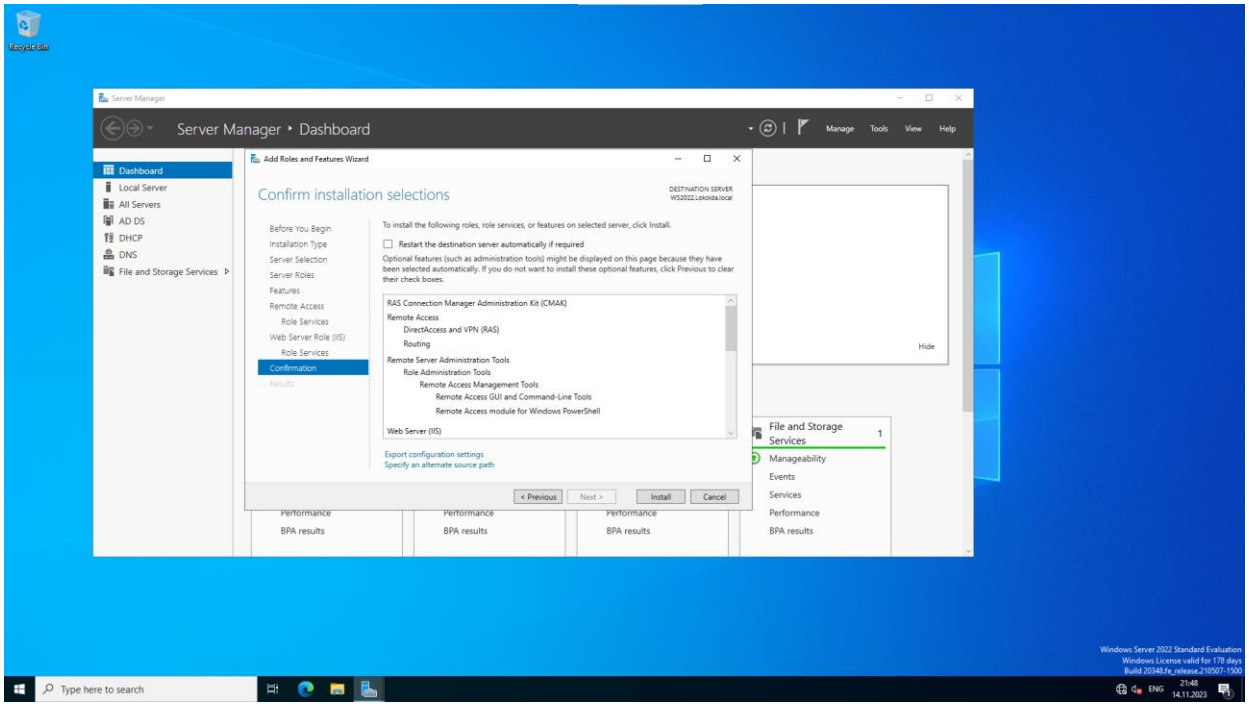


Рисунок 3.71 – Остаточне підтвердження вибраних ролей і компонетів

На рисунку 3.72 зображено процес установки обраних ролей і необхідних компонентів.

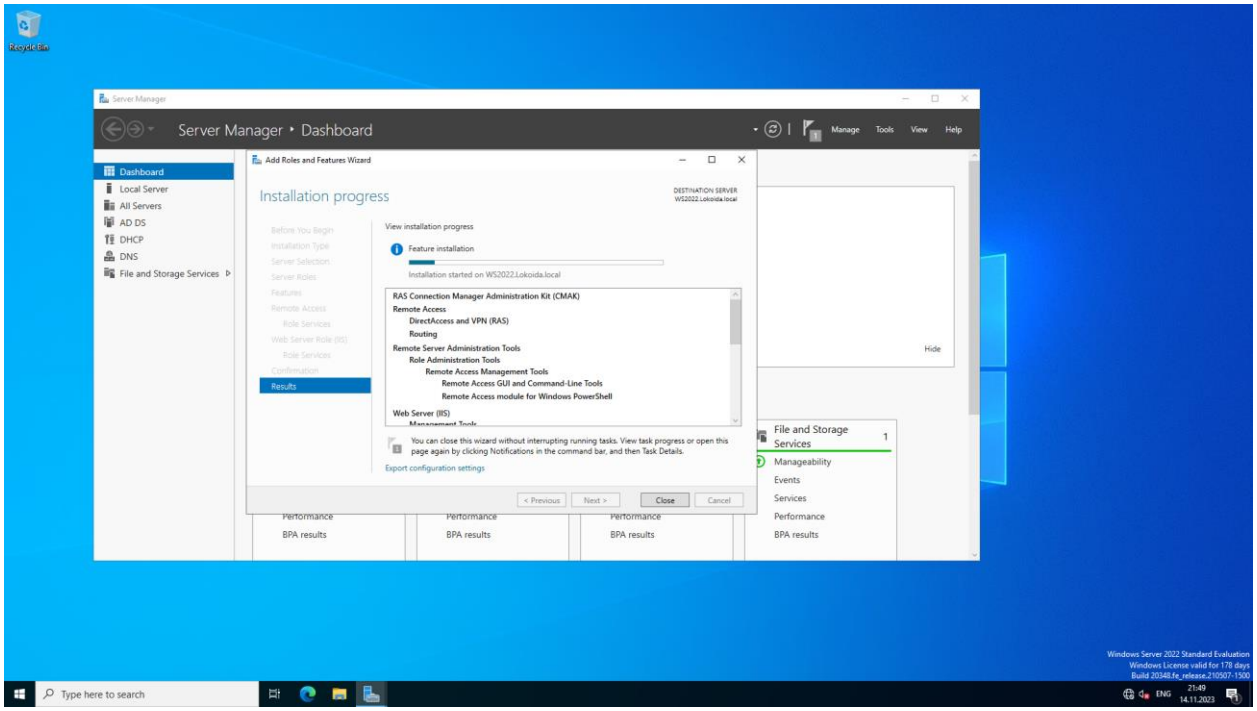


Рисунок 3.72 – Процес установки обраних ролей і необхідних компонентів

На рисунку 3.73 зображено закінчення процесу установки необхідних ролей і необхідних компонентів.

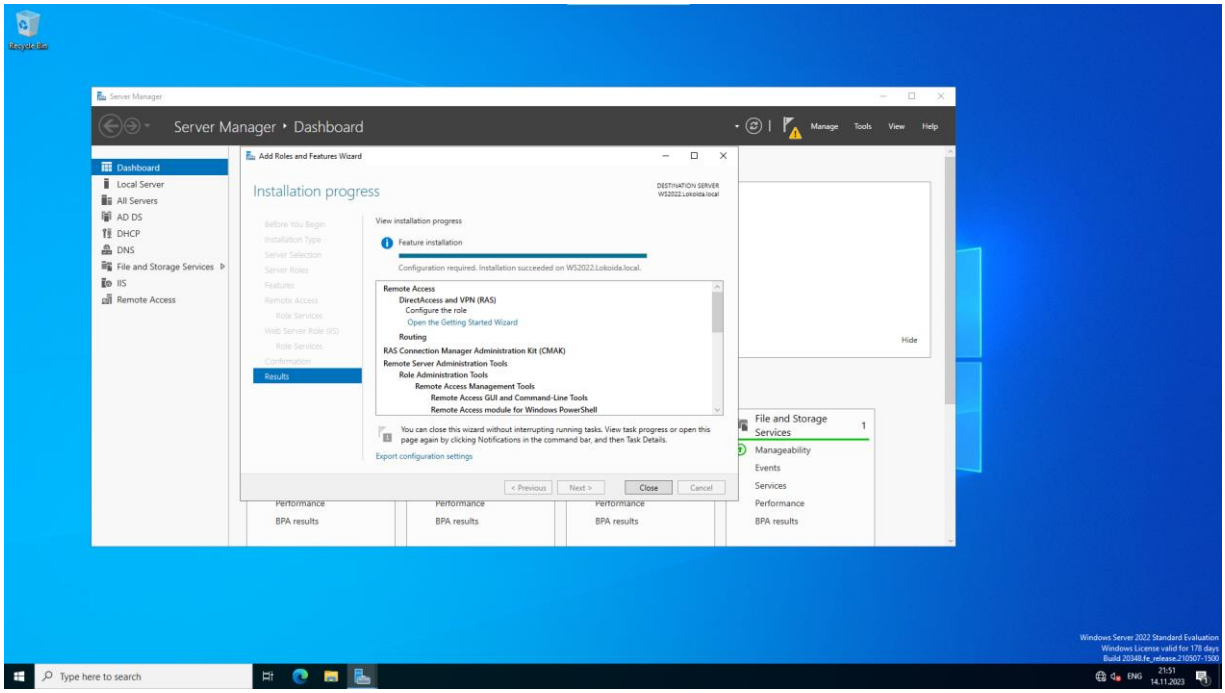


Рисунок 3.73 – Закінчення процесу установки необхідних ролей і необхідних компонентів

На рисунку 3.74 зображено майстер додавання обладнання.

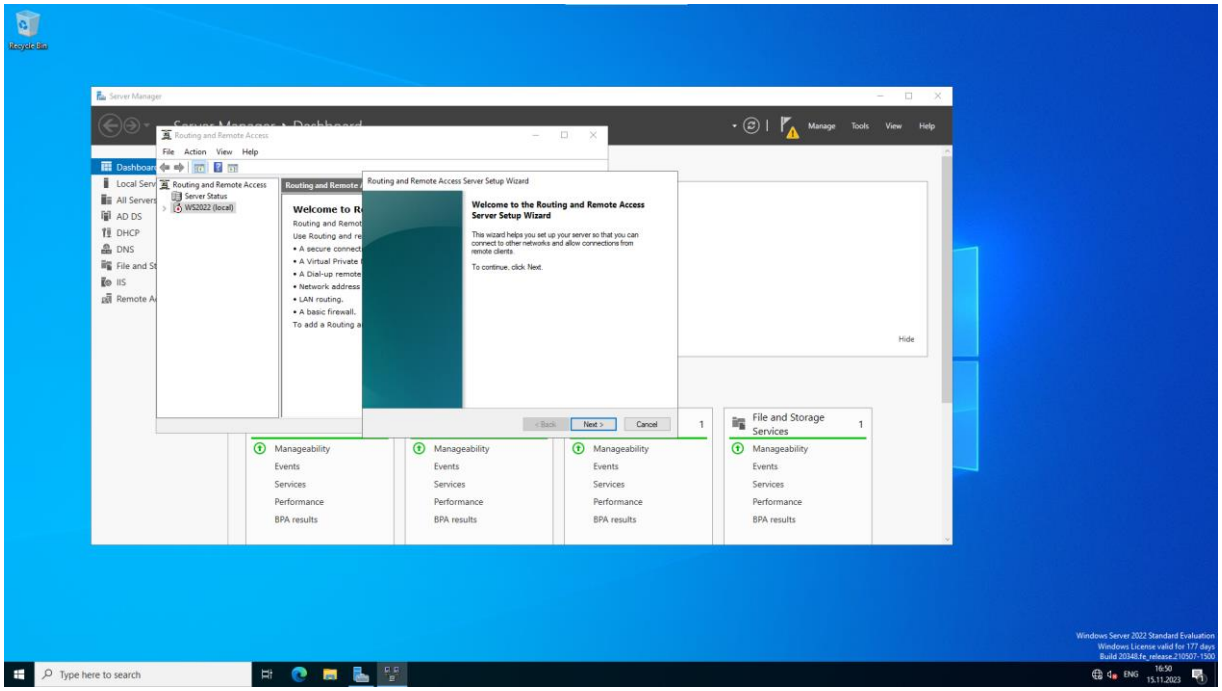


Рисунок 3.74 – Майстер додавання обладнання

На рисунку 3.75 зображено обраний пункт "Конфігурація користувача".

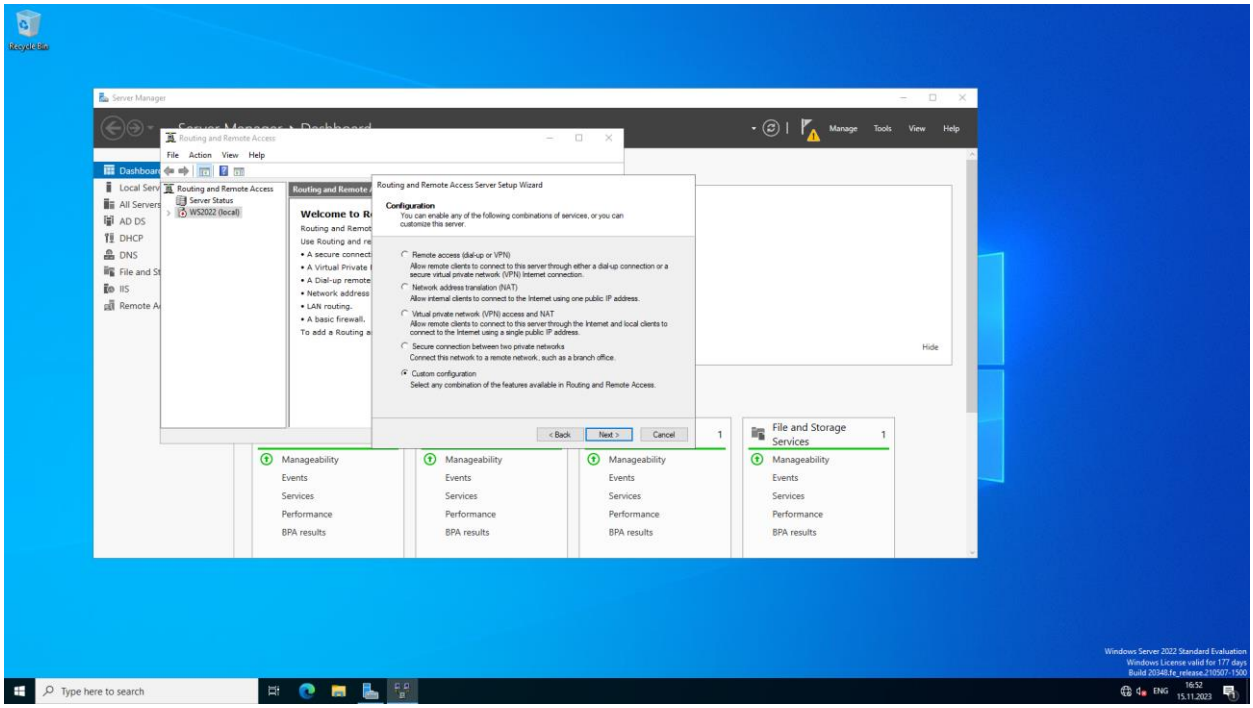


Рисунок 3.75 – Обраний пункт "Конфігурація користувача"

На рисунку 3.76 зображено обрані три сервіси.

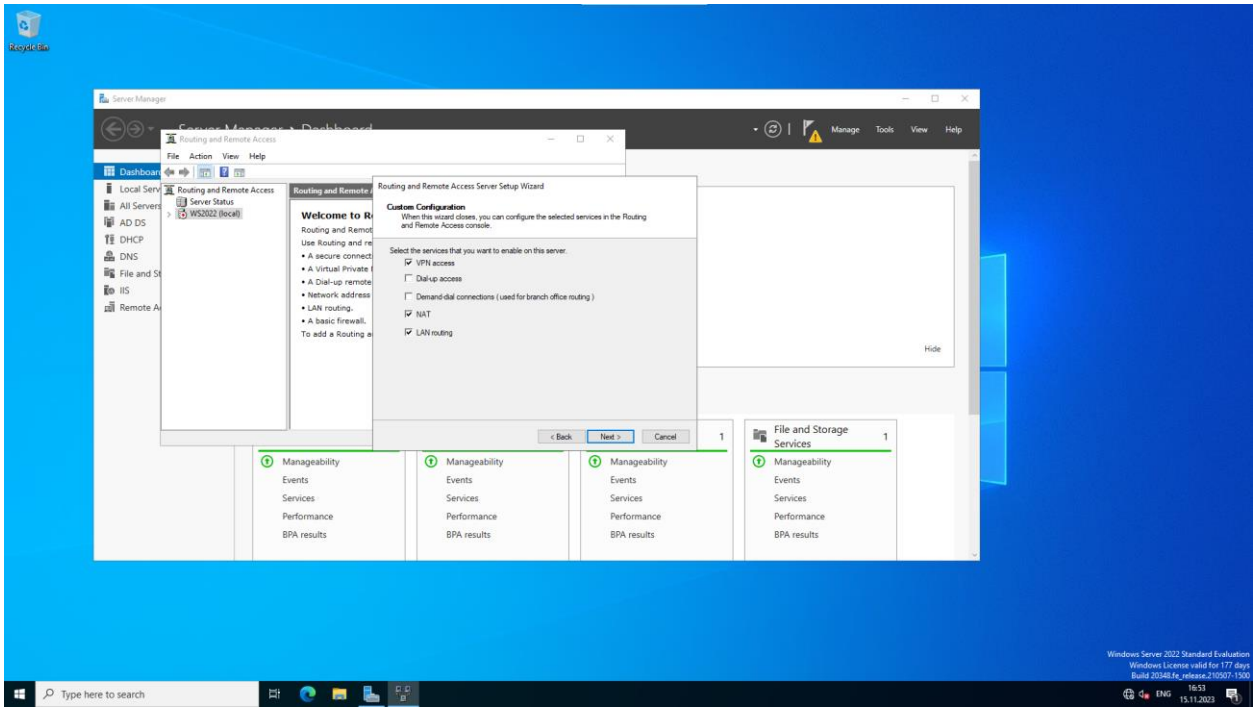


Рисунок 3.76 – Обрані три сервіси

На рисунку 3.76 зображено завершення роботи майстра налаштування.

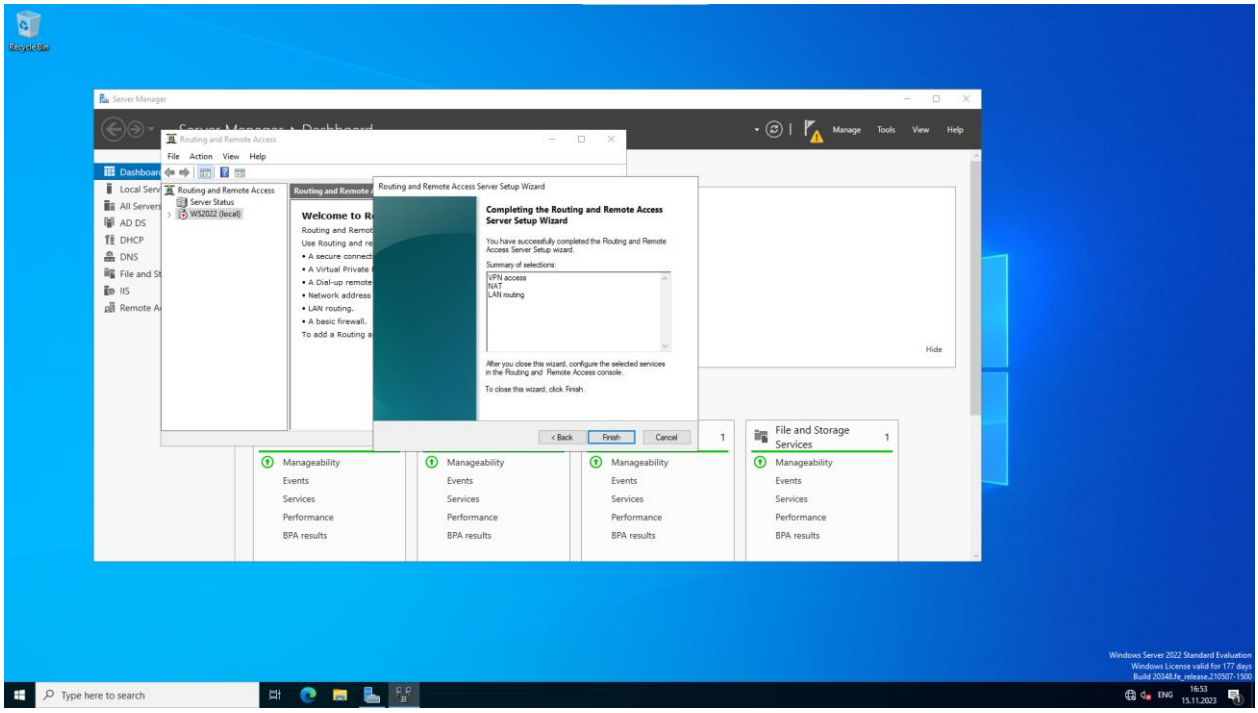


Рисунок 3.77 – Завершення роботи майстра налаштування

На рисунку 3.78 зображено обраного необхідного інтерфейса.

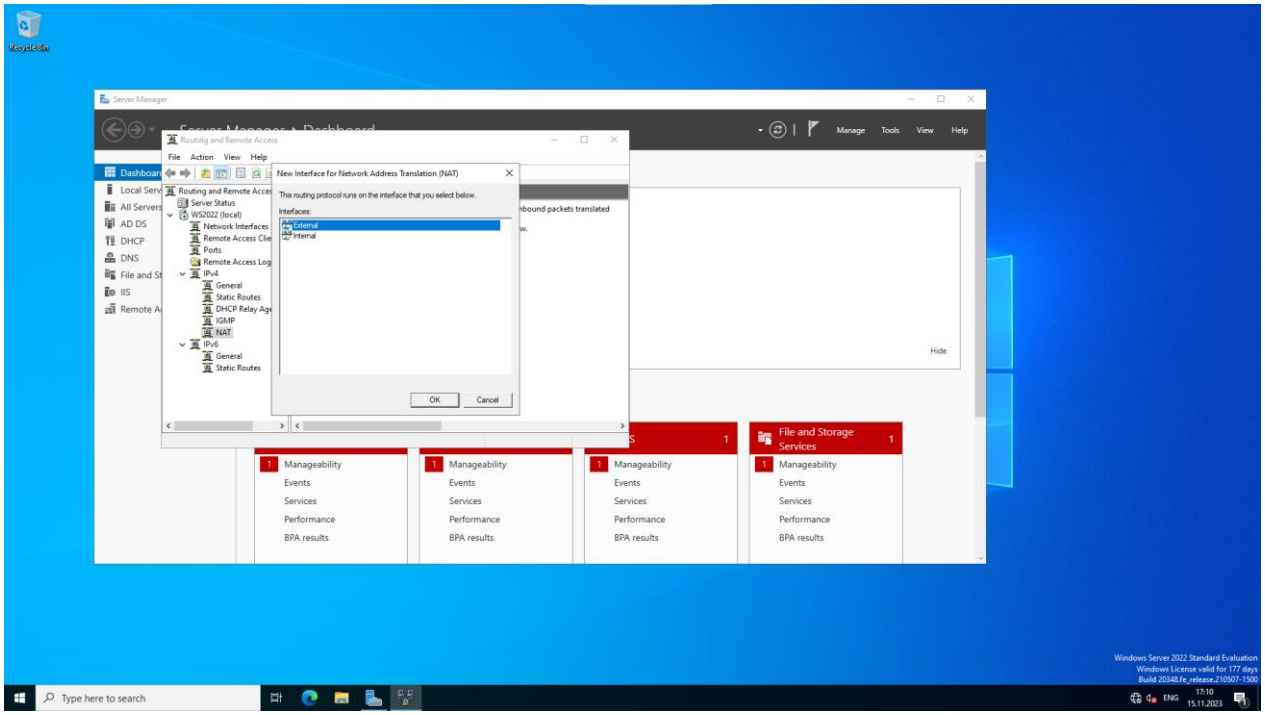


Рисунок 3.78 – Обраний необхідний інтерфейс

На рисунку 3.79 зображено встановлений прапорець "Включити NAT на цьому інтерфейсі".

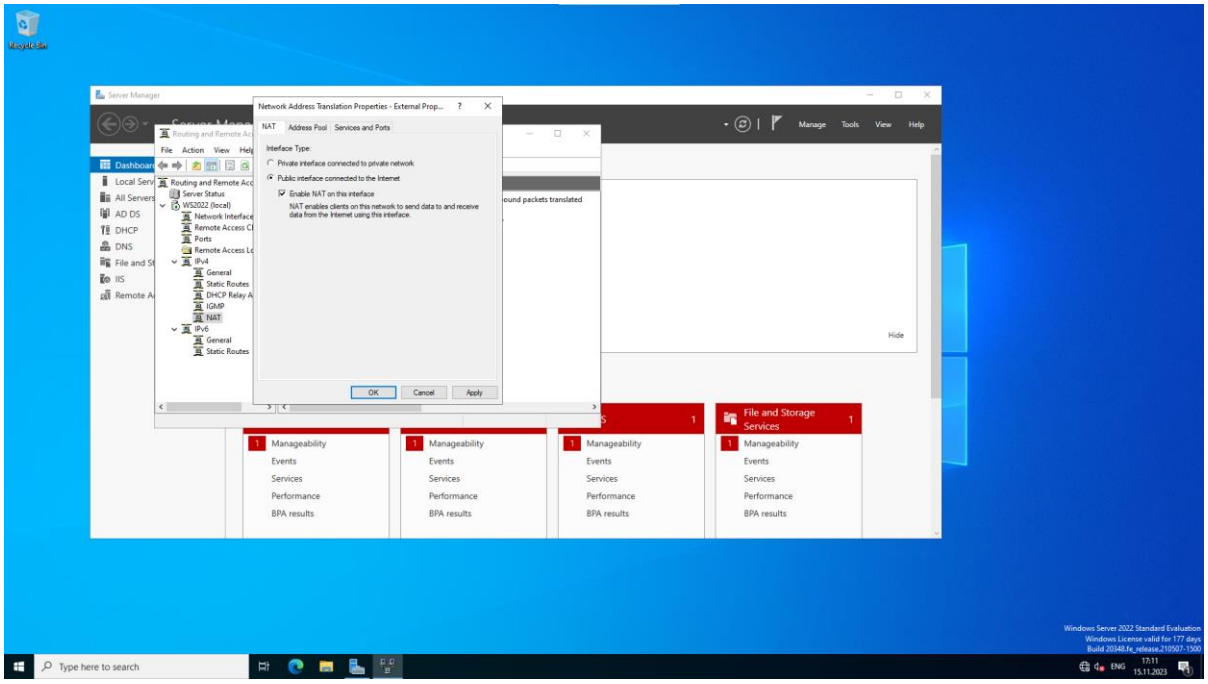


Рисунок 3.79 – Прапорець "Включити NAT на цьому інтерфейсі"

На рисунку 3.80 зображено вибраний необхідний інтерфейс.

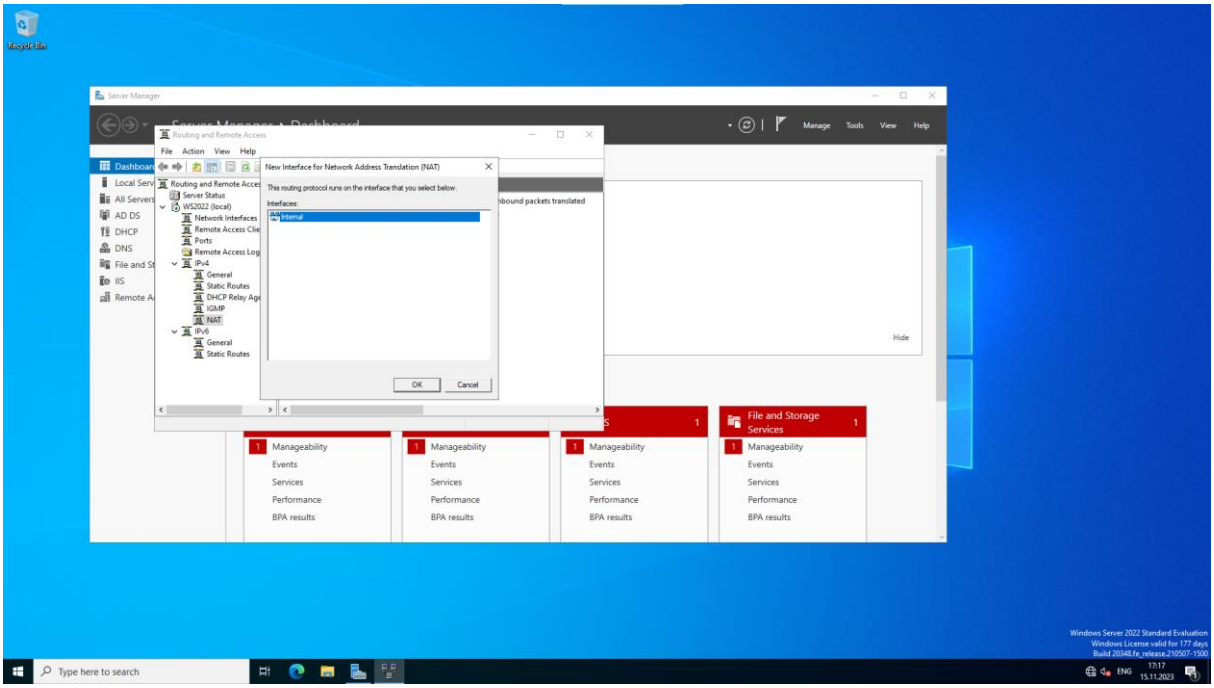


Рисунок 3.80 – Вибраний необхідний інтерфейс

На рисунку 3.81 зображено підключення інтерфейсу до приватної мережі.

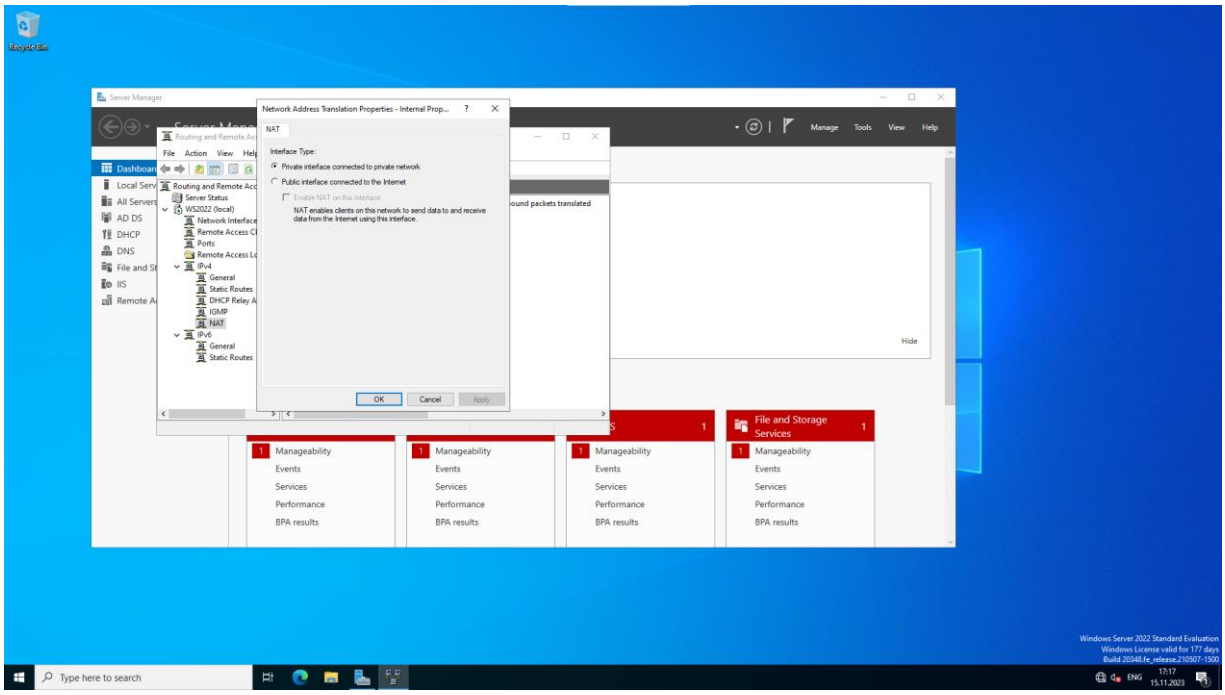


Рисунок 3.81 – Підключення інтерфейсу до приватної мережі

На рисунку 3.82 зображено необхідні додані інтерфейси для роботи NAT.

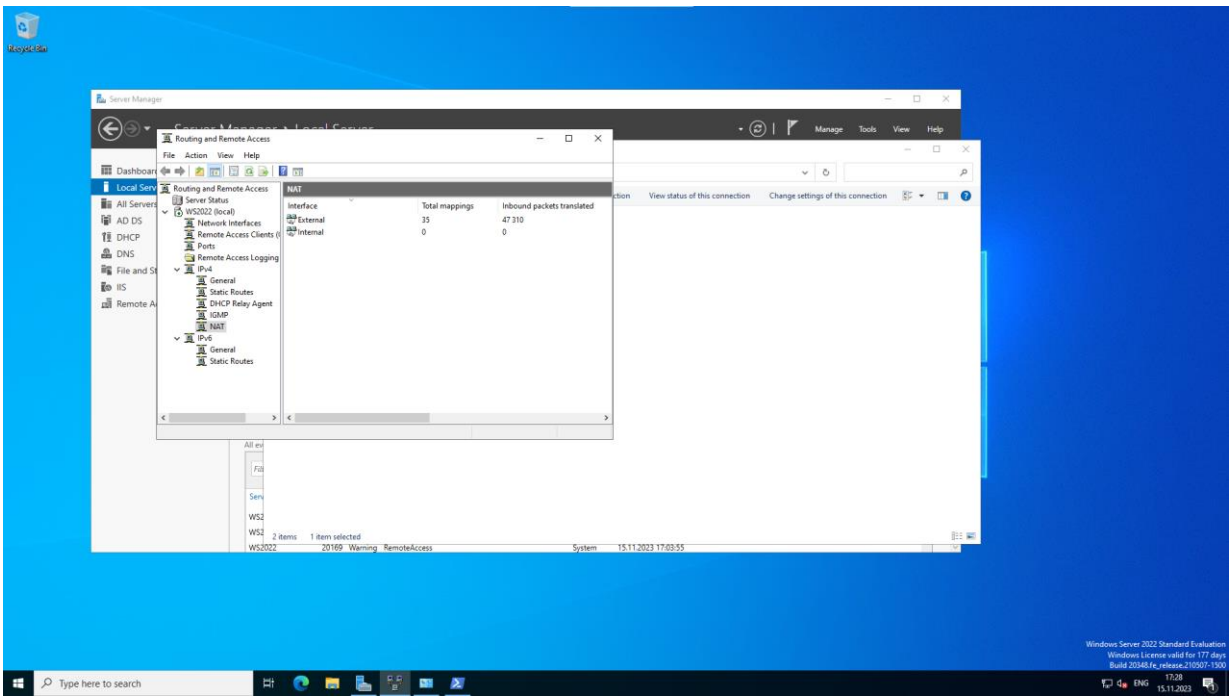


Рисунок 3.82 – Додані інтерфейси для роботи NAT

На рисунку 3.83 зображено перевірку роботи NAT через Poweshell.

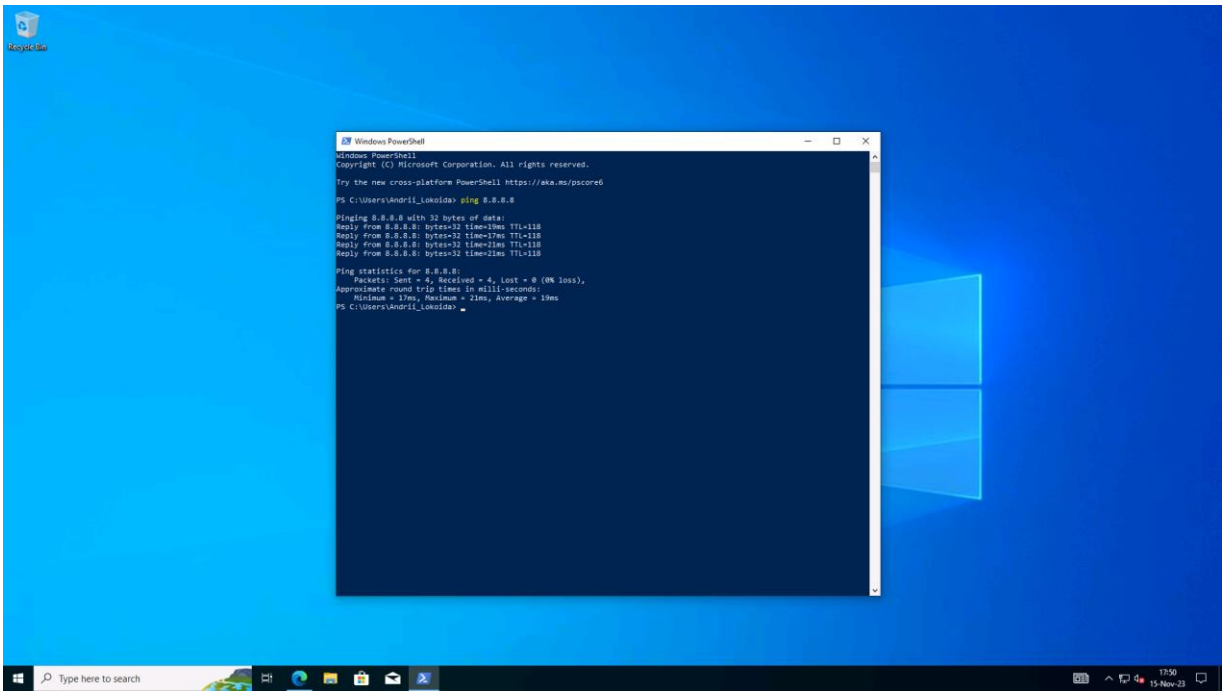


Рисунок 3.83 – Перевірка роботи NAT через Powershell

На рисунку 3.84 зображено перевірку роботи NAT через браузер.

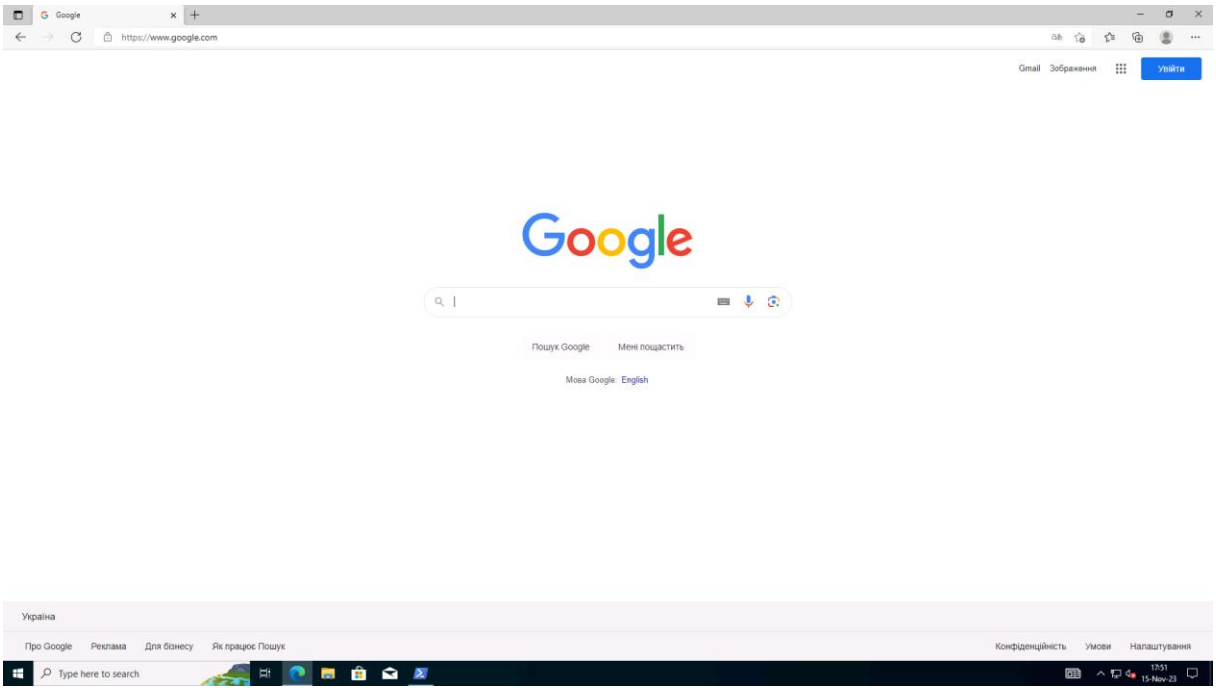


Рисунок 3.84 – Перевірка роботи NAT через браузер

На рисунку 3.85 зображено помічені важливі функції і число максимальних портів.

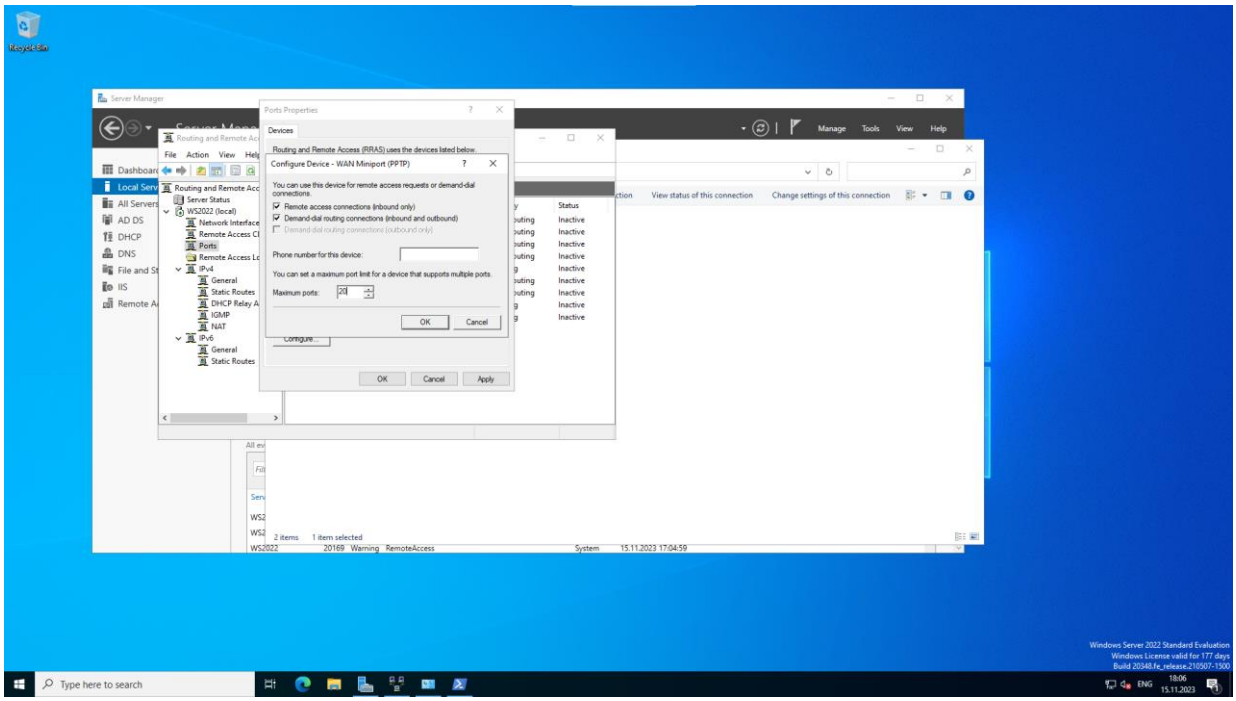


Рисунок 3.85 – Важливі функції і число максимальних портів

На рисунку 3.86 зображено заданий статичний пул IP-адресів.

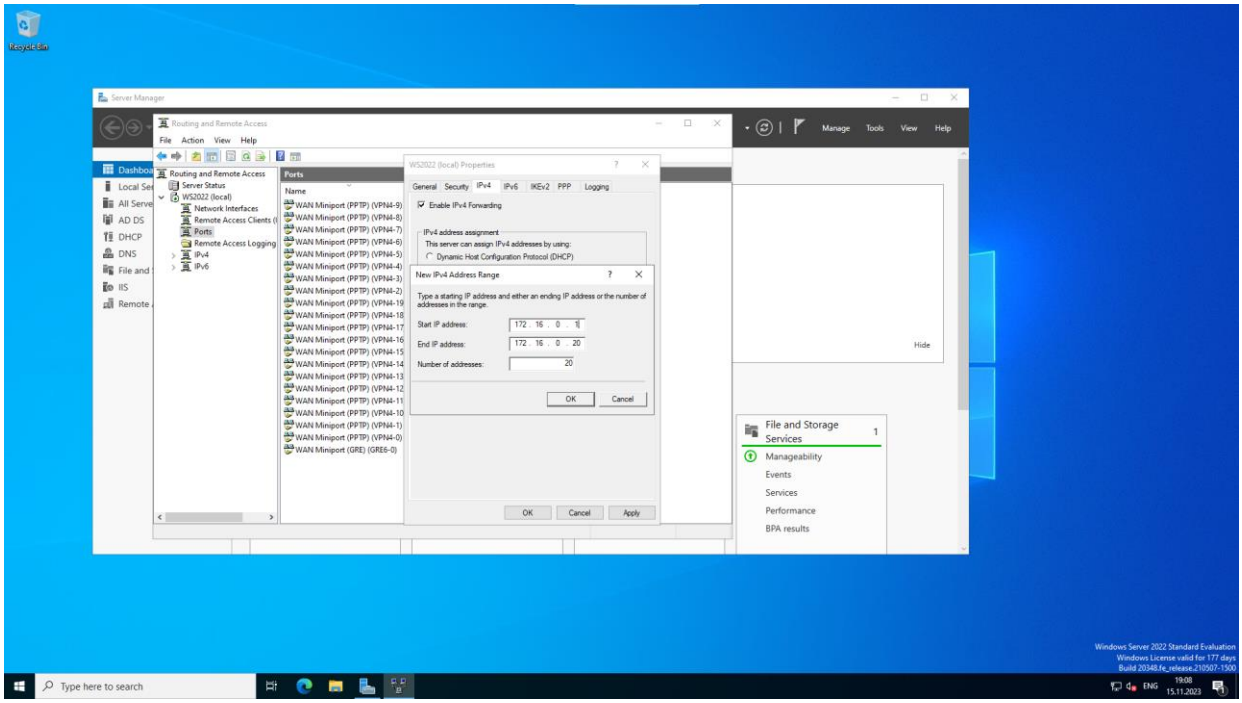


Рисунок 3.86 – Статичний пул IP-адресів

На рисунку 3.87 зображено помічений дозвіл для підключення нового користувача до VPN.

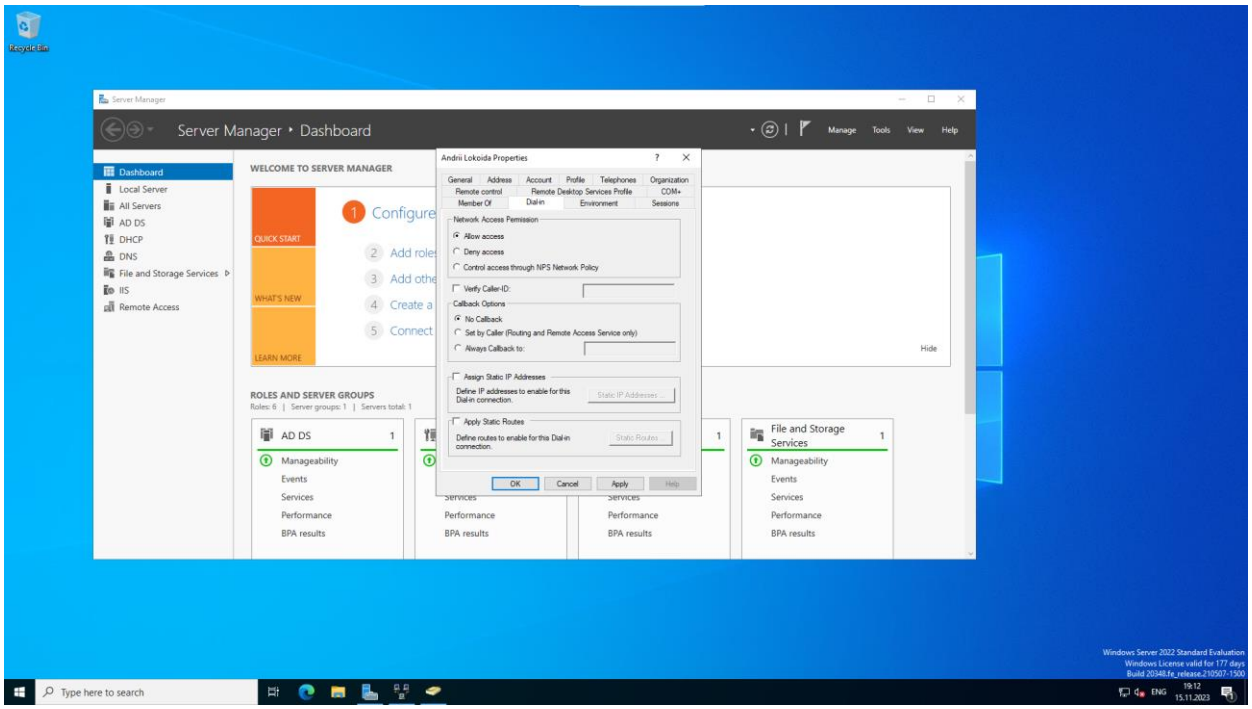


Рисунок 3.87 – Помічений дозвіл для підключення до VPN

На рисунку 3.88 зображено вибраний варіант “Підключення до робочого місця”.

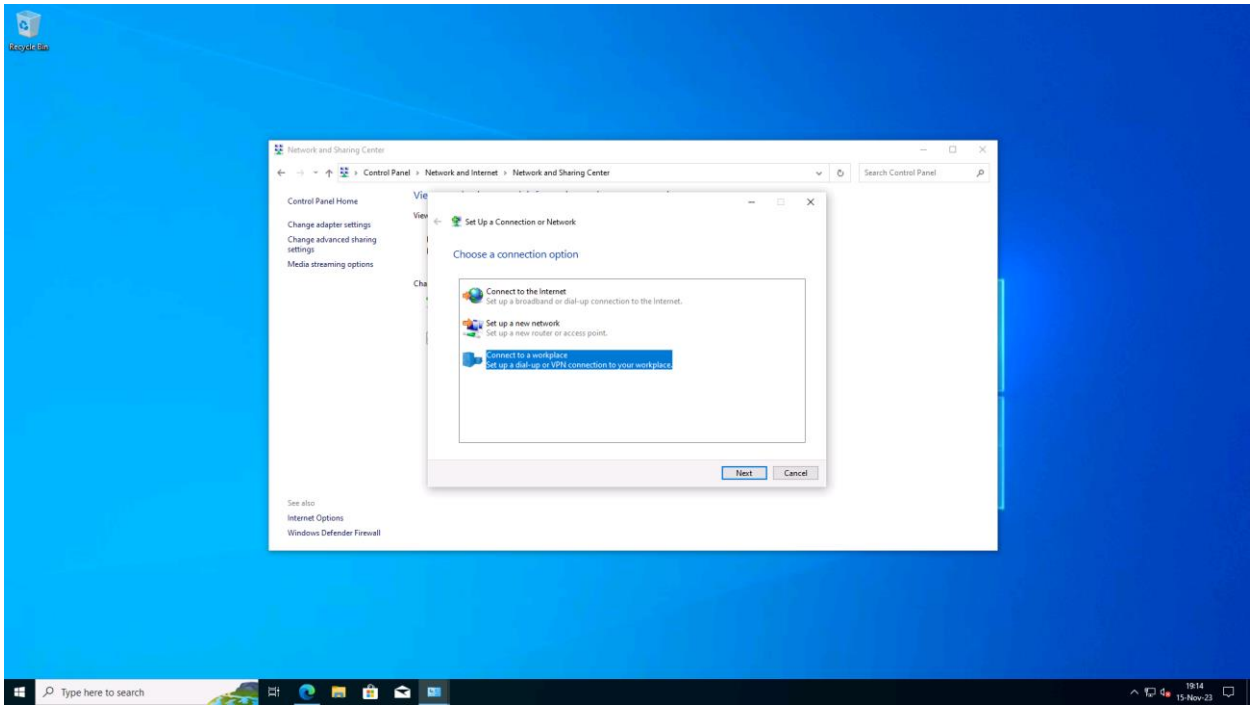


Рисунок 3.88 – Вибраний варіант “Підключення до робочого місця”

На рисунку 3.89 зображено вибраний варіант “Використовувати моє підключення до Інтернету (VPN)”.

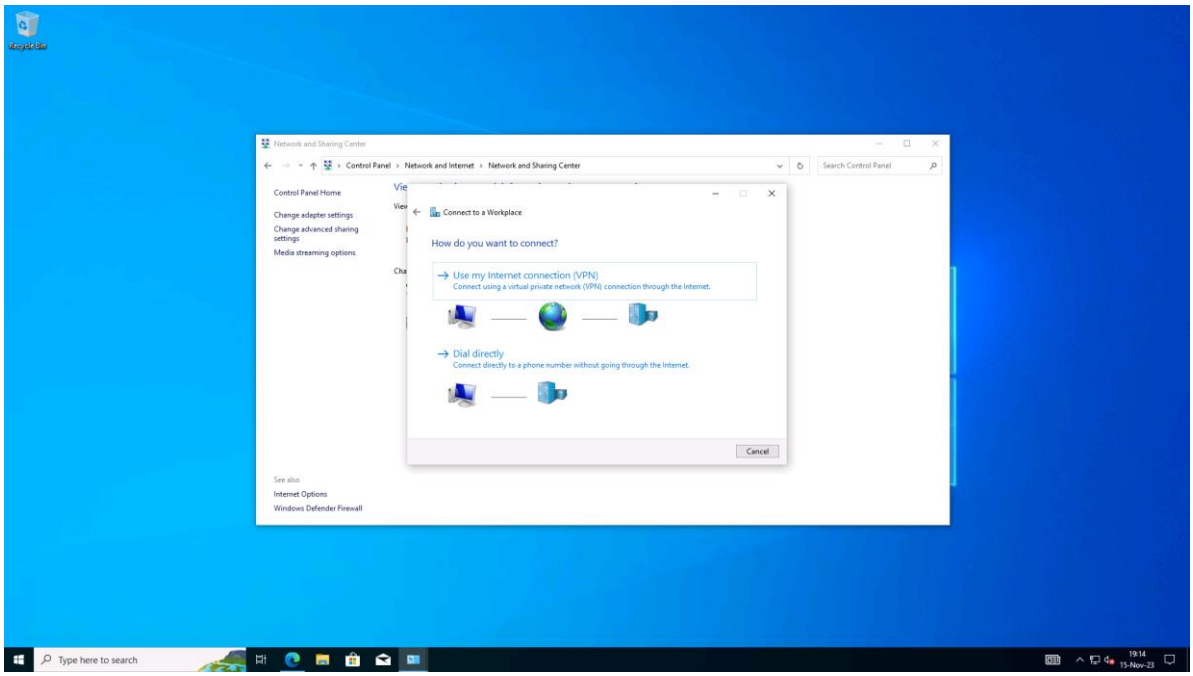


Рисунок 3.89 – вибраний варіант “ Використовувати моє підключення до Інтернету (VPN)”

На рисунку 3.90 зображено введені параметри для створення VPN з’єднання.

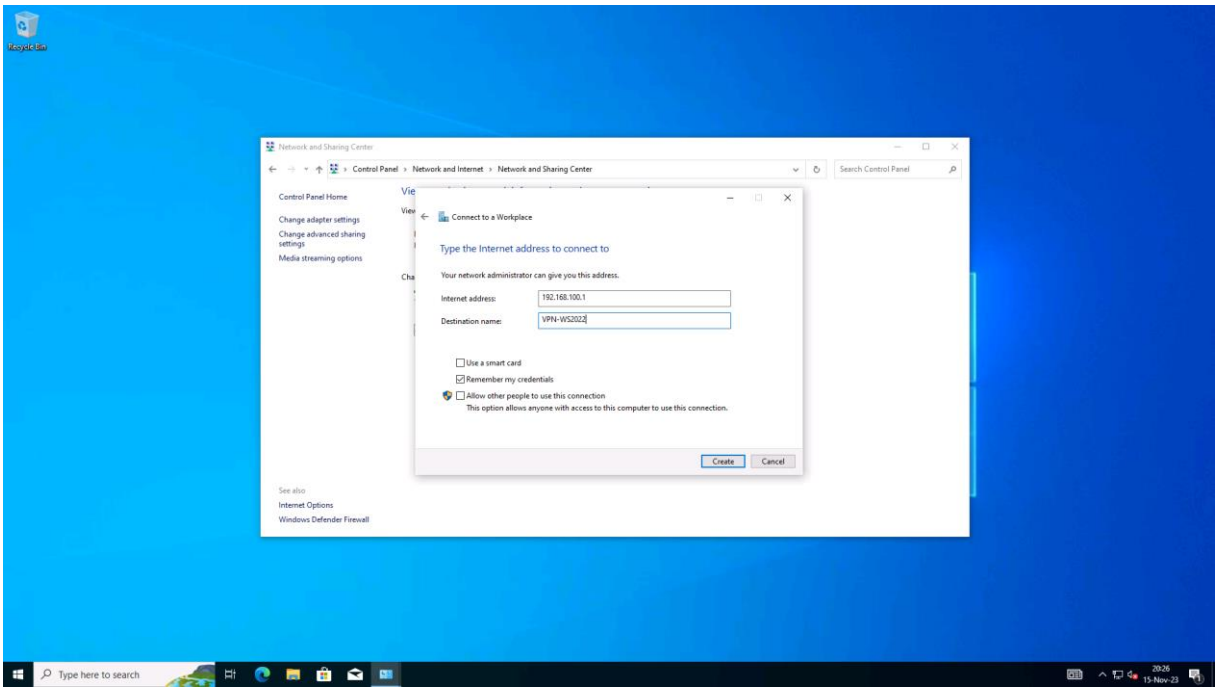


Рисунок 3.90 – Введені параметри для створення VPN з’єднання

На рисунку 3.91 зображено створене VPN з’єднання.

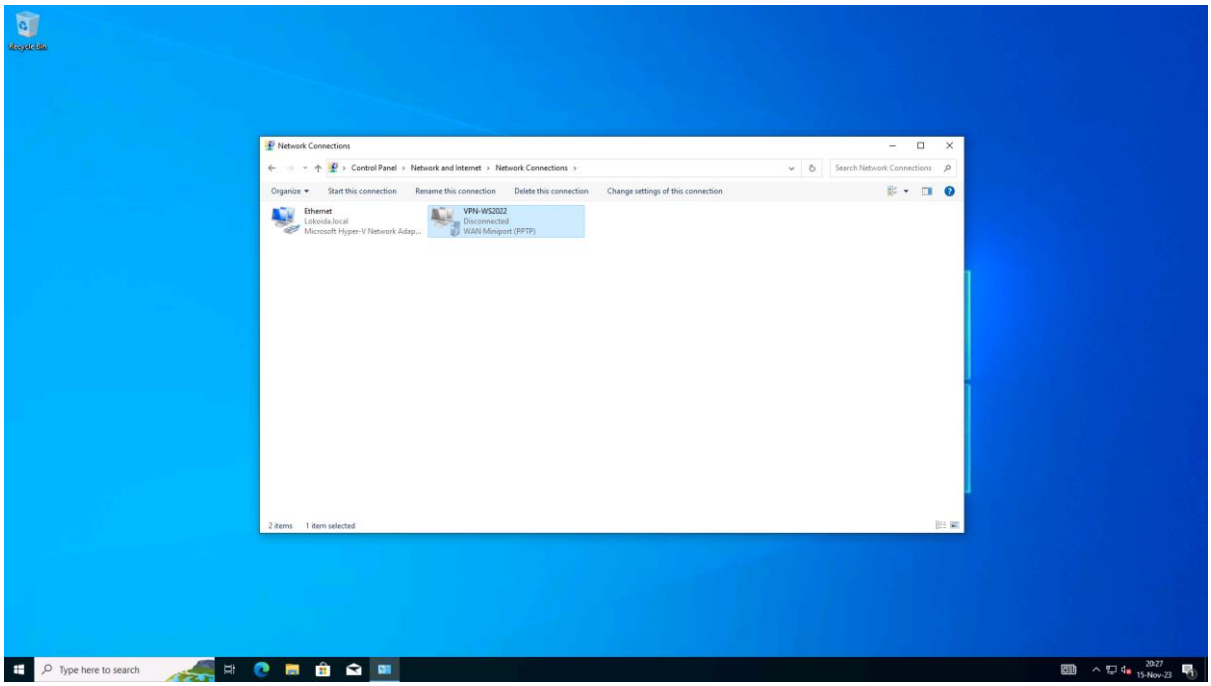


Рисунок 3.91 – Створене VPN з’єднання

На рисунку 3.92 зображено активоване VPN з’єднання.

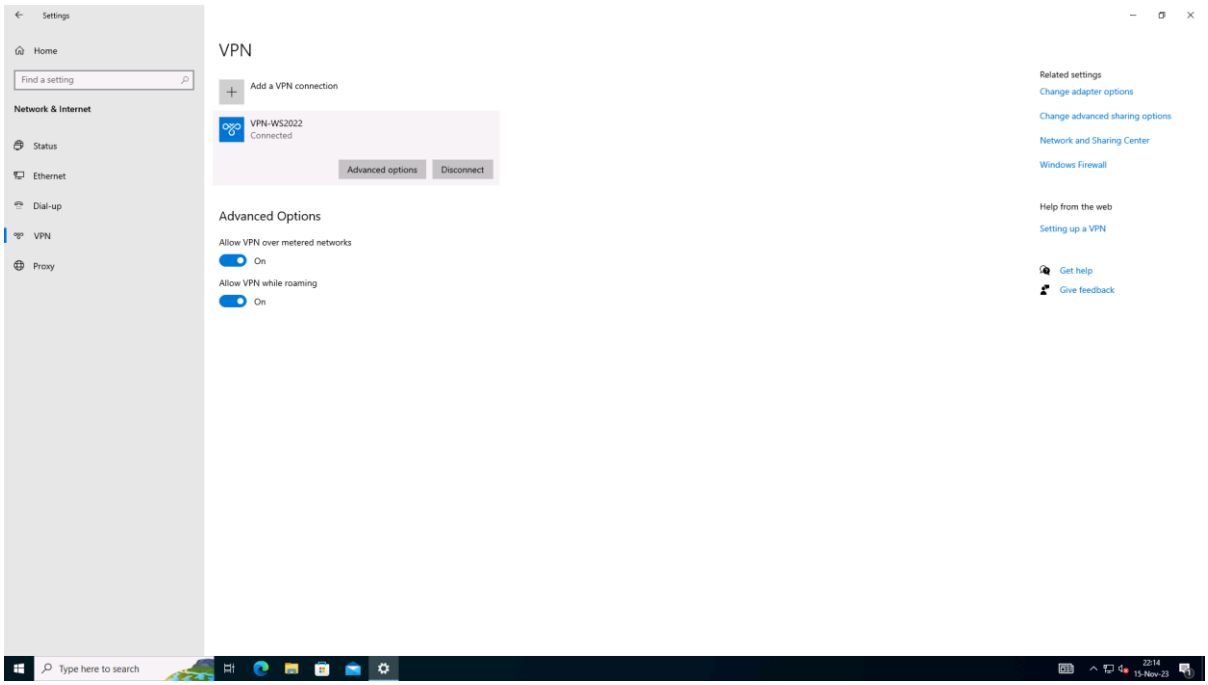


Рисунок 3.92 – Активоване VPN з’єднання

ВИСНОВКИ

Під час дослідження можливостей адміністрування корпоративної мережі на основі Windows Server 2022 було встановлено, що ця система надає широкий набір інструментів та можливостей для керування мережею.

В рамках дослідження можливостей адміністрування корпоративної мережі на основі Windows Server 2022 було вивчено такі аспекти:

1. Управління серверами

Windows Server 2022 надає широкий спектр можливостей для керування серверами, включаючи:

- Центр адміністрування Windows (Windows Admin Center) – єдина веб-консоль для керування всіма серверами в мережі.
- Windows PowerShell – потужна мова сценаріїв для автоматизації завдань адміністрування.

2. Управління мережею

Windows Server 2022 надає такі можливості для керування мережею:

- Active Directory - централізована служба каталогів для управління користувачами, групами та ресурсами у мережі.
- DNS - служба доменних імен для дозволу імен в IP-адреси.
- DHCP - служба динамічного розподілу IP-адрес.
- NAT-мережевий метод, який дозволяє приватній мережі використовувати обмежену кількість публічних IP-адрес для зв’язку з Інтернетом.
- VPN – віртуальні приватні мережі для безпечного підключення віддалених користувачів до мережі.

3. Управління безпекою

Windows Server 2022 надає широкий спектр можливостей для керування безпекою, включаючи

- Захист від шкідливих програм - вбудовані засоби захисту від шкідливих програм, включаючи антивірусний захист, брандмауер та пісочницю.
- Ідентифікація та аутентифікація - засоби для перевірки справжності користувачів та пристроїв.
- Управління доступом – механізми для контролю доступу до ресурсів мережі.
- Шифрування - засоби захисту даних від несанкціонованого доступу.

В результаті дослідження було встановлено, що Windows Server 2022 надає широкі можливості адміністрування корпоративної мережі будь-якого розміру. Ця операційна система дозволяє централізовано керувати серверами, мережею та безпекою, що спрощує та підвищує ефективність адміністрування. Вона забезпечує гнучкість і масштабованість, що дозволяє відповідати вимогам різних організацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Microsoft Windows Server 2022 Standard [Electronic resource]. – URL: https://itpro.ua/product/microsoft-windows-server-2022-standard/?tab=description (дата звернення: 06.11.2023).
2. Опис служб оновлення програмного забезпечення та служби Windows Server Update Services змін у вмісті за 2023 рік (KB894199) [Electronic resource]. – URL: https://support.microsoft.com/uk-ua/topic
3. Example of a Corporate Network Architecture. [Electronic resource]. – URL: https://www.researchgate.net/figure/Example-of-a-Corporate-Network-Architecture_fig1_353368550/ (дата звернення: 06.11.2023).
4. Planning for networking communications [Electronic resource]. – URL: https://www.ibm.com/docs/en/power5?topic=planning-networking-communications (дата звернення: 06.11.2023).
5. Windows Server documentation. [Electronic resource]. – URL: https://learn.microsoft.com/en-us/windows-server/ (дата звернення: 06.11.2023).
6. Windows Server 2022 Tutorials [Electronic resource]. – URL: https://www.vdtutorials.com/windows-server-2022-tutorials/ (дата звернення: 08.11.2023).
7. Thomas Lee. Windows Server Automation with PowerShell Cookbook: Powerful ways to automate and manage Windows administrative tasks/ Lee Thomas. – Packt Publishing, 2021. – 674 p.
8. Jordan Krause. Mastering Windows Server 2022 / Krause Jordan. – Packt Publishing, 2023. – 720 p.
9. Dishan Francis. Mastering Active Directory: Design, deploy, and protect Active Directory Domain Services for Windows Server 2022 / Francis Dishan. – Packt Publishing, 2021. – 778 p.

10. Bekim Dauti. Windows Server 2022 Administration Fundamentals: A beginner's guide to managing and administering Windows Server environments / Dauti Bekim. – Packt Publishing, 2022. – 398 p.
11. Adam Bertram. PowerShell for Sysadmins: Workflow Automation Made Easy / Bertram Adam. – No Starch Press, 2020. – 320 p.
12. Lee Holmes. PowerShell Cookbook: Your Complete Guide to Scripting the Ubiquitous Object-Based Shell / Holmes Lee. – O'Reilly Media, 2021. – 1000 p.
13. Катков Ю. І., Локойда А. О. ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК І ТЕРОРИСТИЧНИХ ЗАГРОЗ // Науково-практична конференція «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» Збірник тез. – К.: ДУІКТ, 2023. 27 жовтня 2023, С-180-182. https://duikt.edu.ua/uploads/p_2626_52007398.pdf
14. Операційні системи, їхні різновиди [Electronic resource]. – URL: https://ua5.org/opersys/2117-operaczijni-systemy-yihni-riznovydy.html (дата звернення: 08.11.2023).
15. ОС в тимчасових мережах [Electronic resource]. – URL: http://ni.biz.ua/3/3_16/3_168824_os-v-odnorangovih-setyah.html (дата звернення: 09.11.2023).
16. Datalogic Memor K Handheld Computer Посібник користувача [Electronic resource]. – URL: https://webcache.googleusercontent.com/search?q=cache:https://manualzz.com/doc/59710513/datalogic-memor-k-handheld-computer-pos%D1%96bnik-koristuvacha (дата звернення: 10.11.2023).
17. 10 способів віртуалізації може покращити безпеку [Electronic resource]. – URL: https://uk.theastrologypage.com/10-ways-virtualization-can-improve-security (дата звернення: 12.11.2023).
18. Абонентське обслуговування комп'ютерної техніки організацій [Electronic resource]. – URL: https://lvivservice.com.ua/sysadmin/ (дата звернення: 13.11.2023).
19. Сучасні форми конкурентної взаємодії суб’єктів господарювання: монографія / Ж.В.Поплавська, Н.Л.Михальчишин, М.Л.Данилович-Кропивницька, О.В.Гошовська, С.О.Комаринець; за заг. ред.

Ж.В.Поплавської. – Львів: ТОВ «Галицька видавнича спілка», 2019. 201 с. ISBN 978–617–7809–09–7 [Electronic resource]. – URL: https://lpnu.ua/sites/default/files/2020/pages/187/monografiyazaredprofpoplavskoyizhv.pdf (дата звернення: 14.11.2023).

20. Операційні системи, їхні різновиди [Electronic resource]. – URL: https://ua5.org/opersys/2117-operaczijni-systemy-yihni-riznovydy.html (дата звернення: 15.11.2023).
21. Нові можливості Windows Server 2022 [Electronic resource]. – URL: https://learn.microsoft.com/ru-ru/windows-server/get-started/whats-new-in-windows-server-2022 (дата звернення: 16.11.2023).
22. Настройка DHCP-сервера на Windows Server 2022 [Electronic resource]. – URL: https://ru.a-d.site/?p=3861 (дата звернення: 17.11.2023).
23. Как настроить DHCP-сервер в Windows Server 2016 [Electronic resource]. – URL: https://serverspace.ru/support/help/how-to-configure-a-dhcp-server-in-windows-server-2016/ (дата звернення: 01.11.2023).
24. Install Remote Desktop Session Host role service in Windows Server without Connection Broker role service [Electronic resource]. – URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/install-rds-host-role-service-without-connection-broker (дата звернення: 02.11.2023).
25. Установка Active Directory Domain Services на Windows Server 2019 [Electronic resource]. – URL: https://www.heyvaldemar.net/ustanovka-active-directory-domain-services-na-windows-server-2019/ (дата звернення: 03.11.2023).
26. Полное руководство по Active Directory, от установки и настройки до аудита безопасности. Ч. 4: Установка Active Directory Domain Services в Windows Server 2022 [Electronic resource]. – URL: https://hackware.ru/?p=16428 (дата звернення: 04.11.2023).

27. Microsoft Windows Server Data Center 2022 [Electronic resource]. – URL: https://itpro.ua/catalog/catalogarticle/view/microsoft-windows-server-data-center-2022/?tab=description (дата звернення: 05.11.2023).
28. Microsoft оголосила про Windows Server 2022 [Electronic resource]. – URL: https://itpro.ua/post/microsoft_anonsirovala_os_windows_server_2022 (дата звернення: 07.11.2023).
29. Як встановити та налаштувати DHCP на Linux [Electronic resource]. – URL: https://ciksiti.com/uk/chapters/12439-how-to-install-and-configure-dhcp-on-linux (дата звернення: 18.11.2023).
30. Що нового у Windows Server 2022? Повний Огляд [Electronic resource]. – URL: https://www.hostzealot.com.ua/blog/about-servers/shho-novogo-u-windows-server-2022-povnii-oglyad (дата звернення: 19.11.2023).
31. Windows Server 2022 [Electronic resource]. – URL: https://qubstore.ru/rukovodstvo/7/windows-server-2022-chto-novogo-2 (дата звернення: 20.11.2023).
32. 31 січня 2023-KB5023321 оновлення для .NET Framework 4.8.1 для Windows Server 202 [Electronic resource]. – URL: https://support.microsoft.com/uk-ua/topic/31-%D1%81%D1%96%D1%87%D0%BD%D1%8F-2023-kb5023321-%D0%BE%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F-%D0%B4%D0%BB%D1%8F-net-framework-4-8-1-%D0%B4%D0%BB%D1%8F-windows-server-2022-7275ef1a-8f7d-4c7b-b437-20dab3670e1e (дата звернення: 21.11.2023).
33. Моделювання мережі [Electronic resource]. – URL: https://hmn.wiki/uk/Network_simulation#google_vignette (дата звернення: 22.11.2023).
34. Understanding corporate networks [Electronic resource]. – URL: https://medium.com/@opencorporates/understanding-corporate-networks-2b92b7088f64 (дата звернення: 23.11.2023).

35. Corporate Network [Electronic resource]. – URL: https://simple.wikipedia.org/wiki/Corporate_network (дата звернення: 24.11.2023).
36. Network Design and Best Practices [Electronic resource]. – URL: https://www.auvik.com/franklyit/blog/network-design-best-practices/ (дата звернення: 25.11.2023).
37. About Applications for FreeBSD [Electronic resource]. – URL: https://www.freebsd.org/applications/ (дата звернення: 26.11.2023).
38. Advanced Networking [Electronic resource]. – URL: https://docs.freebsd.org/en/books/handbook/advanced-networking/ (дата звернення: 27.11.2023).
39. The FreeBSD Corporate Networker's Guide [Electronic resource]. – URL:https://doc.lagout.org/operating%20system%20/bsd/FreeBSDDocumentationProject/books/TheFreeBSDCorporateNetworkersGuide.pdf (дата звернення: 28.11.2023).
40. Операційна система FreeBSD [Electronic resource]. – URL: https://www.trucoteca.com/uk/el-sistema-operativo-freebsd/ (дата звернення: 29.11.2023).
41. The 5 best Linux distros for the enterprise: Red Hat, Ubuntu, Linux Mint and more [Electronic resource]. – URL: https://www.computerworld.com/article/3245645/the-5-best-linux-distros-for-work-red-hat-suse-ubuntu-linux-mint-and-tens.html (дата звернення: 30.11.2023).
42. What is a Linux server and why does your business need one? [Electronic resource]. – URL: https://opensource.com/article/18/5/what-linux-server (дата звернення: 21.10.2023).
43. The 6 Best Linux Distros for Network Engineers [Electronic resource]. – URL: https://www.makeuseof.com/best-linux-distros-for-network-engineers/ (дата звернення: 22.10.2023).

44. Red Hat Enterprise Linux [Electronic resource]. – URL: https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux (дата звернення: 23.10.2023).
45. Windows Server management overview [Electronic resource]. – URL: https://learn.microsoft.com/en-us/windows-server/administration/overview (дата звернення: 24.10.2023).
46. Windows Server Admin Tools Pack: What It Is + Free Guide on How to Install and Best Practices [Electronic resource]. – URL: https://www.dnsstuff.com/windows-server-admin-tools (дата звернення: 25.10.2023).
47. Windows Server deployment, configuration, and administration [Electronic resource]. – URL: https://learn.microsoft.com/en-us/training/paths/windows-server-deployment-configuration-administration/ (дата звернення: 26.10.2023).
48. Windows Server Network Infrastructure [Electronic resource]. – URL: https://learn.microsoft.com/en-us/training/paths/windows-server-network-infrastructure/ (дата звернення: 27.10.2023).
49. Configure IIS Web Server on Windows Server 2019 [Electronic resource]. – URL: https://computingforgeeks.com/install-and-configure-iis-web-server-on-windows-server/ (дата звернення: 28.10.2023).
50. Routing and Remote Access Service (RRAS) [Electronic resource]. – URL: https://networkencyclopedia.com/routing-and-remote-access-service-rras/ (дата звернення: 29.10.2023).
51. Routing and Remote Access Service [Electronic resource]. – URL: https://en.wikipedia.org/wiki/Routing_and_Remote_Access_Service (дата звернення: 30.10.2023).
52. Server Operating System Explained [Electronic resource]. – URL: https://community.fs.com/article/server-operating-system-explained.html (дата звернення: 01.11.2023).

53. Network Scanning Tools [Electronic resource]. – URL: https://www.educba.com/network-scanning-tools/ (дата звернення: 02.11.2023).
54. The Top 10 LAN Monitoring Software Solutions [Electronic resource]. – URL: https://expertinsights.com/insights/the-top-10-lan-monitoring-software-solutions/ (дата звернення: 03.11.2023).
55. Introducing Cisco PPDIOO for Network Design [Electronic resource]. – URL: https://www.ictshore.com/network-design/cisco-ppdioo/ (дата звернення: 04.11.2023).
56. Как выбрать операционную систему для сервера [Electronic resource]. – URL: https://mixtelecom.ru/blog/servernie-os (дата звернення: 05.11.2023).
57. Windows Server 2022 [Electronic resource]. – URL: https://en.wikipedia.org/wiki/Windows_Server_2022 (дата звернення: 06.11.2023).
58. Computer Network Diagrams [Electronic resource]. – URL: https://www.conceptdraw.com/examples/draw-the-diagram-of-networking-hardware (дата звернення: 07.11.2023).
59. Top 10 Firewall Hardware Devices in 2022 [Electronic resource]. – URL: https://www.spiceworks.com/it-security/network-security/articles/top-10-firewall-hardware-devices/ (дата звернення: 08.11.2023).
60. Top 10 Best Antivirus Software for Business [Electronic resource]. – URL: https://cxoincmagazine.com/top-10-best-antivirus-software-for-business/ (дата звернення: 09.11.2023).
61. Windows Server 2022 [Electronic resource]. – URL: https://en.wikipedia.org/wiki/Windows_Server_2022 (дата звернення: 10.11.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

1

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ДИПЛОМНА РОБОТА
на ступінь вищої освіти магістр
із спеціальності 122 Комп'ютерні технології

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ WINDOWS SERVER 2022

Виконав: студент 6 курсу, групи КНДМ-61
Локойда Андрій Олегович
Керівник: д.т.н., доцент Катков Ю.І.

Київ - 2023

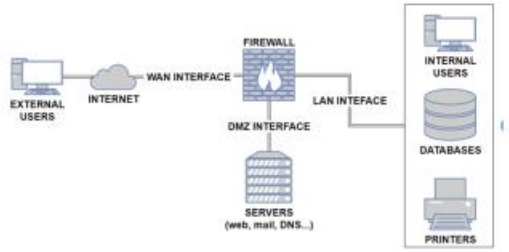
2

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ДИПЛОМНОЇ РОБОТИ

Тема	Дослідження можливостей адміністрування корпоративної мережі на основі Windows Server 2022
Мета дослідження	підвищити ефективність застосування можливостей Windows Server 2022 для адміністрування та управління корпоративними мережами
Наукове завдання	оцінити доцільність та ефективність використання Windows Server 2022 для адміністрування сучасної корпоративної мережі.
Об'єкт дослідження	процес використання Windows Server 2022 для корпоративного адміністрування мережі, що включає в себе застосування пропонованих функцій, які мають відношення до управління і забезпечення безпеки корпоративної мережі.
Предмет дослідження	потенціал Windows Server 2022 в управлінні корпоративними мережами

3

ОСНОВИ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ



Example of a Corporate Network Architecture.

Основи адміністрування корпоративної мережі складаються з таких етапів:

1. Планування та проектування мережі
2. Розгортання та налаштування мережі
3. Управління мережею
4. Безпека мережі

4

ПЛАНУВАННЯ ТА ПРОЕКТУВАННЯ МЕРЕЖІ

Корпоративна мережа - це група комп'ютерів, з'єднаних між собою в будівлі або в певній області, які всі належать одній компанії або установам. Вона не прив'язана до певного місця та може включати просторово віддалені частини організації, такі як філії, дочірні компанії та навіть офіси за кордоном. Ключові етапи планування та проектування: підготовка, планування, проектування, впровадження, експлуатація, оптимізація. Ці кроки є частиною популярної моделі життєвого циклу мережі, відомої як модель Cisco PPDIOO. У контексті адміністрування корпоративної мережі розуміння цих етапів є фундаментальним. Це допомагає забезпечити, щоб мережа відповідала потребам організації, зберігаючи продуктивність, безпеку, резервування та економічну ефективність.

5

РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ

Розгортання та налаштування мережі є важливим завданням адміністрування корпоративної мережі. Воно включає наступні етапи: закупівля обладнання та програмного забезпечення, встановлення обладнання та програмного забезпечення, налаштування обладнання та програмного забезпечення, тестування мережі. При покупці обладнання та програмного забезпечення необхідно враховувати такі фактори: гарантія, повернення і доставка. На етапі встановлення обладнання необхідно встановити обладнання відповідно до розробленої топології мережі та налаштувати його відповідно до вимог. При налаштуванні обладнання та програмного забезпечення необхідно виконати такі завдання: налаштування IP-адрес, налаштування мережевих масок, налаштування шлюзів, настроювання DNS-серверу, налаштування безпеки. На етапі тестування мережі потрібно перевірити працездатність мережі. При тестуванні мережі необхідно враховувати такі фактори: підключення пристроїв, обмін даними, безпека і продуктивність.

6

УПРАВЛІННЯ МЕРЕЖЕЮ

Управління мережею - це комплекс завдань, пов'язаних із підтриманням працездатності та ефективності корпоративної мережі. Воно включає наступні основні напрямки: обслуговування мережі, розширення мережі. На етапі обслуговування мережі здійснюється моніторинг мережі, виявлення та усунення несправностей, оновлення обладнання та програмного забезпечення. На етапі розширення мережі здійснюється додавання нових пристроїв та користувачів до мережі, розширення її пропускної спроможності та функціональності. До конкретних завдань управління корпоративною мережею належать: адміністрування обладнання та програмного забезпечення мережі, керування користувачами та доступом до ресурсів мережі, управління безпекою мережі і виправлення неполадок мережі.

Для управління корпоративною мережею використовуються різні інструменти, такі як: мережеві операційні системи, мережеві утиліти, мережеві сканери, мережеві монітори.

БЕЗПЕКА МЕРЕЖІ

7

Безпека мережі є одним із найважливіших аспектів адміністрування корпоративної мережі. Вона включає захист мережі від зовнішніх і внутрішніх загроз. Для забезпечення безпеки мережі необхідно виконувати такі завдання: розробка та впровадження політики безпеки, встановлення та налаштування засобів захисту, навчання працівників правилам безпеки.

Розробка та впровадження політики безпеки. Політика безпеки має визначати такі аспекти: права доступу до мережі та її ресурсів, регламентація використання мережі, заходи реагування на інциденти безпеки. Встановлення та налаштування засобів захисту. Необхідно регулярно оновлювати програмне забезпечення засобів захисту для забезпечення їхньої актуальності. Навчання працівників правилам безпеки. Необхідно регулярно проводити навчання співробітників, щоб вони були обізнані про існуючі загрози і могли вжити заходів для запобігання їм.

ОСНОВНІ ІНСТРУМЕНТИ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

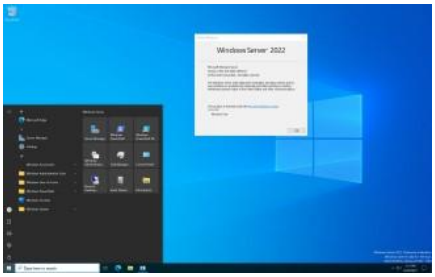
8

Windows Server - це потужна операційна система, яка може використовуватися для підтримки великих мереж, розроблена корпорацією Майкрософт. Це система забезпечує платформу для запуску різних серверних додатків, таких як файлові сервери, сервери друку, веб-сервери та сервери електронної пошти. Windows Server також використовується для управління мережами та забезпечення їх безпеки.

Linux є популярним вибором для корпоративних мереж завдяки своїй стабільності, безпеці та гнучкості. Ключові моменти про Linux в контексті корпоративних мереж: різноманітність дистрибутивів, серверні програми, рентабельність, безпека, сумісність, підтримка. В цілому, Linux пропонує переконливий набір переваг для корпоративних мереж.

FreeBSD - це надійна, гнучка та безпечна операційна система з відкритим кодом, яка добре підходить для корпоративних мережевих середовищ. Її поєднання стабільності, безпеки, продуктивності та гнучкості робить його переконливою альтернативою фірмовим рішенням, особливо для організацій, які шукають економічно ефективну та надійну платформу для своєї інфраструктури В цілому, FreeBSD є універсальною операційною системою, що добре підходить для корпоративних мереж.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ WINDOWS SERVER 2022 ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ 9



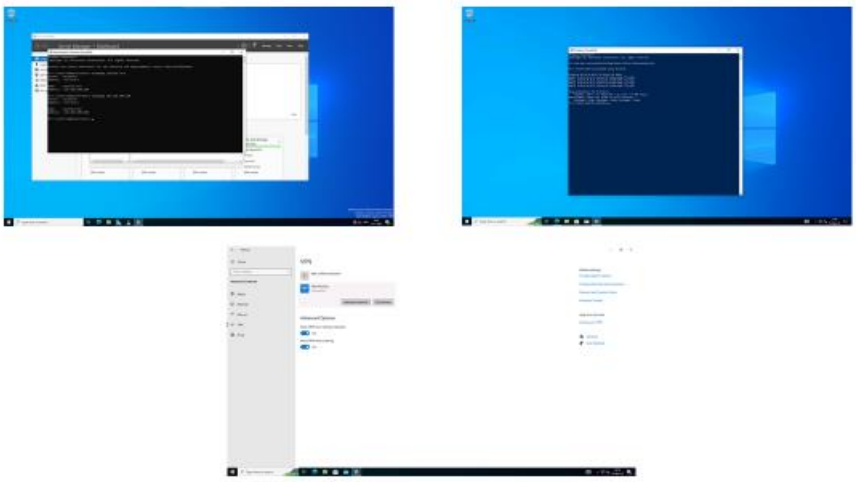
Windows Server 2022 - це остання версія флагманської серверної операційної системи Microsoft, що пропонує повний набір функцій і можливостей, призначених для задоволення вимог сучасних корпоративних мереж. Він забезпечує надійну і безпечну основу для широкого спектру робочих навантажень, від традиційного обміну файлами і друком до просунутих хмарних додатків. Windows Server 2022 пропонує повний набір функцій, які задовольняють широкий спектр корпоративних навантажень, включаючи: Active Directory, DNS-сервер, DHCP-сервер, служба маршрутизації та віддаленого доступу, спільний доступ до файлів і друку, віртуалізація Hyper-V, підтримка контейнеризації, віддалений робочий стіл. Windows Server 2022 пропонує привабливий набір функцій і можливостей, які роблять його ідеальним вибором для корпоративних мереж.

РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ DHCP- СЕРВЕРУ ТА AD 10

Першими кроками дослідження основних можливостей Windows Server 2022 було розгорнення та налаштування DHCP-серверу та AD. DHCP-сервер у Windows Server 2022 – це служба, яка дозволяє автоматично призначати IP-адреси та інші параметри мережі комп'ютерам та іншим пристроям у корпоративній мережі. Це дозволяє адміністраторам мережі уникнути необхідності вручну налаштовувати кожен пристрій зі статичною IP-адресою.

AD у Windows Server 2022 — це служба каталогів, яка надає централізовану базу даних для керування та організації облікових записів користувачів, комп'ютерів та інших ресурсів у мережі. AD — це ієрархічна база даних із доменами на верхньому рівні, за якими йдуть організаційні підрозділи (OU), а потім такі об'єкти, як користувачі, комп'ютери та групи.

РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ DNS-СЕРВЕРУ ТА RRAS 11



Останніми кроками було розгорнення і налаштування DNS-сервера і RRAS. DNS-сервер у Windows Server 2022 є критично важливим компонентом будь-якої корпоративної мережі, оскільки він забезпечує дозвіл імен у мережі. DNS-сервер дозволяє по доменному імені дізнатися IP адресу хоста і навпаки. RRAS – це служба, яка дозволяє Windows Server 2022 виконувати функції маршрутизатора та віддаленого доступу. Під час дослідження в RRAS було налаштовано NAT і VPN. NAT використовується для надання комп'ютерам у приватній мережі доступу до Інтернету. VPN використовується для забезпечення безпечного зв'язку між комп'ютерами через Інтернет.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ 12

Матеріали опубліковані в статті:

Локойда А. О., Катков Ю. І. Особливості адміністрування корпоративної мережі на основі Windows Server 2022 // Наукові записки Державного університету телекомунікацій №4, 2023, Подано до друку.
https://journals.dut.edu.ua/index.php/sciencenotes/issue/archive

В тезисах:

1. Катков Ю. І., Локойда А. О. ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК І ТЕРОРИСТИЧНИХ ЗАГРОЗ // Науково-практична конференція «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» Збірник тез. – К.: ДУІКТ, 2023. 27 жовтня 2023, С-180-182. https://duikt.edu.ua/uploads/p_2626_52007398.pdf

ВИСНОВКИ

Під час дослідження основних можливостей адміністрування корпоративної мережі на основі Windows Server 2022 було встановлено, що ця система надає широкий набір інструментів та можливостей для керування мережею. В рамках дослідження основних можливостей адміністрування корпоративної мережі на основі Windows Server 2022 було досліджено такий аспект як: управління мережею.

Windows Server 2022 надає такі основні можливості для керування мережею:

- Active Directory - централізована служба каталогів для управління користувачами, групами та ресурсами у мережі.
- DNS - служба доменних імен для дозволу імен в IP-адреси.
- DHCP - служба динамічного розподілу IP-адрес.
- NAT-мережевий метод, який дозволяє приватній мережі використовувати обмежену кількість публічних IP-адрес для зв'язку з Інтернетом.
- VPN – віртуальні приватні мережі для безпечного підключення віддалених користувачів до мережі.

В результаті дослідження було встановлено, що Windows Server 2022 надає широкі можливості адміністрування корпоративної мережі будь-якого розміру. Ця операційна система дозволяє централізовано керувати серверами, мережею та безпекою, що спрощує та підвищує ефективність адміністрування.